2024

Cyber Attacks and Counter Measures: User Perspective

POST GRADUATION DIPLOMA IN CYBER SECURITY

Madhya Pradesh Bhoj
Open University, Bhopal

Cyber Attacks and Counter Measures: User Perspective

Block-1:

Block-2:

Block-3:

Block-4:

Block-1

Unit 1: Cyber Attacks, Types of Attacks Motivation

1

Unit Structure

1.1 LEARNING OBJECTIVES

This unit purports at making you understand:

- What constitutes a cyber-attack,
- Types of cyber-attacks, and
- What motivates attacker(s) to do carry out attack(s).

1.2 INTRODUCTION

Everyone among us has one time or another has come across some form of attack. It could be physical or emotional or of some other kind. The intent is to cause some sort of harm – though sometimes it turn into a blessing in disguise. However, cyber attacks always aim at causing harm. They can be varied in their nature of approach and type of harm they inflict, depending on the motive, but the purpose is certainly malicious.

All of you must have encountered a situation when some unwanted changes, like installing some software or change your search engine, are made to your system or seen unwanted advertisements popping up while surfing Internet. These are examples of cyber attacks. These can range from being minor nuisance, like occasional popups, to creating havoc, like formatting hard disk.

1.3 CYBER ATTACK

Farhat et al[1] on 'What is a cyber attack' state as below:

A cyber attack is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it.

According to Anonymous[2], "Cyber-attack is any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous

[1] http://www.hklaw.com/files/Publication/bd9553c5-284f-4175-87d2849aa07920d3/Presentation/PublicationAttachment/1880b6d6-eae2-4b57-8a97 9f4fb1f58b36/CyberAttacksPreventionand ProactiveResponses.pdf

[2] https://en.wikipedia.org/wiki/Cyber-attack

source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can be labeled as either a Cyber campaign, cyber warfare or cyber terrorism in different context. Cyber-attacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nations."

In a nutshell, use of a device/system against another system/device with a malicious intent constitutes a cyber-attack.

1.4 TYPES OF CYBER ATTACK OR THREATS

Anonymous[3] gives a comprehensive list of cyber-attacks/threats which is reproduced below:

1. Backdoors – Backdoors[4] is bypassing normal authentication. Backdoor is a type of cyber threat in which the attacker uses a back door to install a key logging software, thereby allowing an illegal access to your system. This threat can turn out to be potentially serious as it allows for modification of the files, stealing information, installing unwanted software or even taking control of the entire computer.

   Default passwords can function as backdoors if they are not changed by the user. Some debugging features can also act as backdoors if they are not removed in the release version.

   Many computer worms, such as Sobig and Mydoom, install a backdoor on the affected computer (generally a PC on broadband running Microsoft Windows and Microsoft Outlook). Such backdoors appear to be installed so that spammers can send junk e-mail from the infected machines. Others, such as the Sony/BMG rootkit distributed silently on millions of music CDs through late 2005, are intended as DRM measures—and, in that case, as data gathering agents, since both surreptitious programs they installed routinely contacted central servers.

   A sophisticated attempt to plant a backdoor in the Linux kernel, exposed in November 2003, added a small and subtle code change by subverting the revision

[3] http://www.cybersecuritycrimes.com/types-of-cyber-attacks/

[4] https://en.wikipedia.org/wiki/Backdoor_(computing)

control system. In this case, a two-line change appeared to check root access permissions of a caller to the sys_wait4 function, but because it used assignment = instead of equality checking ==, it actually granted permissions to the system. This difference is easily overlooked, and could even be interpreted as an accidental typographical error, rather than an intentional attack.

In January 2014, a backdoor was discovered in certain Samsung Android products, like the Galaxy devices. The Samsung proprietary Android versions are fitted with a backdoor that provides remote access to the data stored on the device. In particular, the Samsung Android software that is in charge of handling the communications with the modem, using the Samsung IPC protocol, implements a class of requests known as remote file server (RFS) commands, that allows the backdoor operator to perform via modem remote I/O operations on the device hard disk or other storage. As the modem is running Samsung proprietary Android software, it is likely that it offers over-the-air remote control that could then be used to issue the RFS commands and thus to access the file system on the device.

2. Denial-of-Service Attack – A denial-of-service (DoS) attack is attacking the network to bring it down completely with useless traffic by affecting the host device which is connected to the Internet. DoS attack targets websites or services which are hosted on the servers. This type of attack can aim bank servers and credit card payment gateways.
3. Direct-access Attack – A direct-access attack simply means gaining physical access to the computer or its part and performing various functions or installing various types of devices to compromise security. The attacker can install software loaded with worms or download important data, using portable devices.
4. Eavesdropping – As the name suggests, eavesdropping means secretly listening to a conversation between the hosts on a network. There are various programs such as Carnivore and Narus Insight that can be used to eavesdrop.
5. Spoofing – Spoofing is a cyber attack where a person or a program impersonate another by creating false data in order to gain illegal access to a system. Such threats are commonly found in emails where the sender's address is spoofed.
6. Tampering – Tampering is a web based attack where certain parameters in the

URL are changed without the customer's knowledge; and when the customer keys in that URL, it looks and appears exactly the same. Tampering is basically done by hackers and criminals to steal the identity and obtain illegal access to information.

7. Repudiation Attack – A repudiation attack occurs when the user denies the fact that he or she has performed a certain action or has initiated a transaction. A user can simply deny having knowledge of the transaction or communication and later claim that such transaction or communication never took place.
8. Information Disclosure – Information disclosure breach means that the information which is thought to be secured is released to unscrupulous elements who are not trustworthy.
9. Privilege Escalation Attack – A privilege escalation attack is a type of network intrusion which allows the user to have an elevated access to the network which was primarily not allowed. The attacker takes the advantage of the programming errors and permits an elevated access to the network.
10. Exploits – An exploit attack is basically a software designed to take advantage of a flaw in the system. The attacker plans to gain easy access to a computer system and gain control, allows privilege escalation or creates a DOS attack.
11. Social Engineering – An attack by a known or a malicious person is known as social engineering. They have knowledge about the programs used and the firewall security and thus it becomes easier to take advantage of trusted people and deceive them to gain passwords or other necessary information for a large social engineering attack.
12. Indirect Attack – Indirect attack means an attack launched from a third party computer as it becomes more difficult to track the origin of the attack.
13. Computer Crime – A crime undertaken with the use of a computer and a network is called as a computer crime.
14. Malware – Malware refers to malicious software that are being designed to damage or perform unwanted actions into the system. Malware is of many types like viruses, worms, Trojan horses, etc., which can cause havoc on a computer's hard drive. They can either delete some files or a directory or simply gather data

without the actual knowledge of the user.

15. Adware – Adware is a software that supports advertisements which renders ads to its author. It has advertisements embedded in the application. So when the program is running, it shows the advertisement. Basically, adware is similar to malware as it uses ads to inflict computers with deadly viruses.
16. Bots – Bots is a software application that runs automated tasks which are simple and repetitive in nature. Bots may or may not be malicious, but they are usually found to initiate a DoS attack or a click fraud while using the internet.
17. Ransomware – Ransomware is a type of cyber security threat which will restrict access to your computer system at first and will ask for a ransom in order for the restriction to be removed. This ransom is to be paid through online payment methods only which the user can be granted an access to their system.
18. Rootkits – A rootkit is a malicious software designed in such a way that hides certain process or programs from normal anti-virus scan detection and continues to enjoy a privilege access to your system. It is that software which runs and gets activated each time you boot your system and are difficult to detect and can install various files and processes in the system.
19. Spyware – Spyware, as the name suggests, is a software which typically spies and gathers information from the system through a user's internet connection without the user's knowledge. A spyware software is majorly a hidden component of a freeware program which can be downloaded from the internet.
20. Scareware – Scareware is a type of threat which acts as a genuine system message and guides you to download and purchase useless and potentially dangerous software. Such scareware pop-ups seem to be similar to any system messages, but actually aren't. The main purpose of the scareware is to create anxiety among the users and use that anxiety to coax them to download irrelevant softwares.
21. Trojan Horses – Trojan Horses are a form of threat that are malicious or harmful codes hidden behind genuine programs or data which can allow complete access to the system and can cause damage to the system or data corruption or loss/theft of data. It acts as a backdoor and hence it is not easily detectable.

22. Virus – A computer virus is a self replicating program which, when executed, replicates or even modifies by inserting copies of itself into another computer file and infects the affected areas once the virus succeeds in replicating. This virus can be harmful as it spreads like wildfire and can infect majority of the system in no time.

23. Worm – Just like a virus, worm is a self replicating program which relies on computer network and performs malicious actions and spreads itself onto other computer networks. Worms primarily rely on security failures to access the infected system.

24. Phishing – Phishing is a cyber threat which makes an attempt to gain sensitive information like passwords, usernames and other details for malicious reasons. It is basically an email fraud where the perpetrator sends a legitimate looking email and attempts to gain personal information.

25. Identity Theft – Identity theft is a crime wherein your personal details are stolen and these details are used to commit a fraud. An identity theft is committed when a criminal impersonates individuals and use the information for some financial gain.

26. Intellectual Property Theft – Intellectual Property theft is a theft of copyrighted material where it violates the copyrights and the patents. It is a cybercrime to get hands onto some trade secrets and patented documents and research. It is basically a theft of an idea, plan and the methodology being used.

27. Password Attacks – Password attack is a form of a threat to your system security where attackers usually try ways to gain access to your system password. They either simply guess the password or use an automated program to find the correct password and gain an entry into the system.

28. Bluesnarfing – Bluesnarfing is a threat of information through unauthorized means. The hackers can gain access to the information and data on a Bluetooth enabled phone using the wireless technology of the Bluetooth without alerting the user of the phone.

29. Bluejacking – Bluejacking is simply sending of texts, images or sounds, to another Bluetooth enabled device and is a harmless way of marketing. However, there is a thin line between bluejacking and bluesnarfing and if crossed it results

into an act of threat.

30. DDoS – DDoS basically means a Distributed Denial of Service. It is an attempt to make any online service temporarily unavailable by generating overwhelming traffic from multiple sources or suspend services of a host connected to the internet.

31. Keylogger – A keylogger is a spyware that has the capability to spy on the happenings on the computer system. It has the capability to record every stroke on the keyboard, web sites visited and every information available on the system. This recorded log is then sent to a specified receiver.

1.5 MOTIVATION

Depending on the motivation, according to Ray[5], Verisign iDefense Security Intelligence Services classifies cyber-attacks into three categories: hacktivism, cyber crime and cyber- espionage.

Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially or ideologically motivated purpose. It is basically used as a means to promote an agenda. Hacktivists are responsible for denial-of-service (DoS), distributed denial of service (DDoS), information theft, data breaches, web site defacement, typosquatting(URL hijacking relying on typographical errors in URL spelling) and many other acts of digital sabotage.

Cyber crime, though, in a broad sense, covers any illegal activity that is committed through a digital means, here it refers to an activity with the monetary gain in mind. Such an activity can be a direct one, e.g., fraudulent bank transaction, or an indirect one, e.g., selling stolen

information in black market. Frequently used cyber crime tools are ATM and point-of-sale (PoS) skimming, RAM scrapping, code injection, key logging and phishing to extract confidential personal information.

Cyber espionage is unauthorized spying by computer[6]. However, a more

[5]http://www.circleid.com/posts/understanding_the_threat_landscape_cyber_attack_actors_and_motivations
[6]http://www.pcmag.com/encyclopedia/term/64376/cyber-espionage

comprehensive definition, and the associated tools, is given by Anonymous[7] which is as below:

Cyber spying, or cyber espionage, is the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware. It may wholly be perpetrated online from computer desks of professionals on bases in far away countries or may involve infiltration at home by computer trained conventional spies and moles or in other cases may be the criminal handiwork of amateur malicious hackers and software programmers.

John Arquilla (a US expert on national security affairs and defense analysis) added to new dimension to motivation behind cyber attacks by coining the term cyber warfare or cyber war. Cyber warfare has been defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption," but other definitions also include non-state actors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists, and transnational criminal organizations[8].

The above definition of cyber espionage is very likely to raise some confusion as to whether it does not cover cyber war. It does not, which has been made clear by Anonymous[8] as below:

‘Cyber "war" is simply the act of fighting on an electronic battlefield with digital weapons. To attack an adversary’s capabilities in an effort to disable or destroy their ability to get things done. This may be completely digital in nature (such as communication and information systems) or the electronics that monitor and manage physical infrastructure, like power and water systems. Hostile code like StuxNet is an example of such weapons for cyber warfare.

Cyber "espionage" on the other hand is the act of obtaining information that is held in secrecy by the adversary. This in itself is not the end game - this information is

[7]https://en.wikipedia.org/wiki/Cyber_spying
[8]https://en.wikipedia.org/wiki/Cyberwarfare

then used for some sort of gain or strategic advantage. It must have an intrinsic value to the adversary, or its useless. In many cases, this may be to gain financial / competitive advantage in the business world, or strategic advantage over political communities of conflict.

Now here is where it gets complicated and is the source of much of the confusion. Cyber espionage is routinely used as a precursor to a cyber warfare strike. This allows an adversary to do reconnaissance in aid of an attack. In the movies, this would be sending in the recon patrol in the military to disable an enemy's capabilities before a major attack, or sending a spy into the enemy territory to gather intel before the strike. And this happens in the real world too.

Typically though cyber espionage is a covert operation that takes months or years to commit. It usually comes with signs of exfiltration and with the right tools can be tracked back to the source, with some level of certainty. Cyber warfare is different. The attack is usually pretty fast, striking in seconds and causing damage for use with other objectives.'

It must be noted that a perpetrator may belong to more than category of attack. For example, politically motivated cyber attacks may be carried out by members of extremist groups who use cyberspace to spread propaganda, attack websites, and steal money to fund their activities or to plan and coordinate physical-world crime[9].

The figure below shows worldwide motivation statistics, typically for April 2015. It clearly shows that most attacks (> 50%) fall under category 'cyber crime' whereas about one third belong to hacktivism. This is obvious from the fact that these two categories consist of mainly individuals and groups and require less resources whereas 'cyber espionage' and 'cyber warfare' usually require greater resources and, in many cases, government backing.

[9]https://en.wikipedia.org/wiki/Cyberwarfare

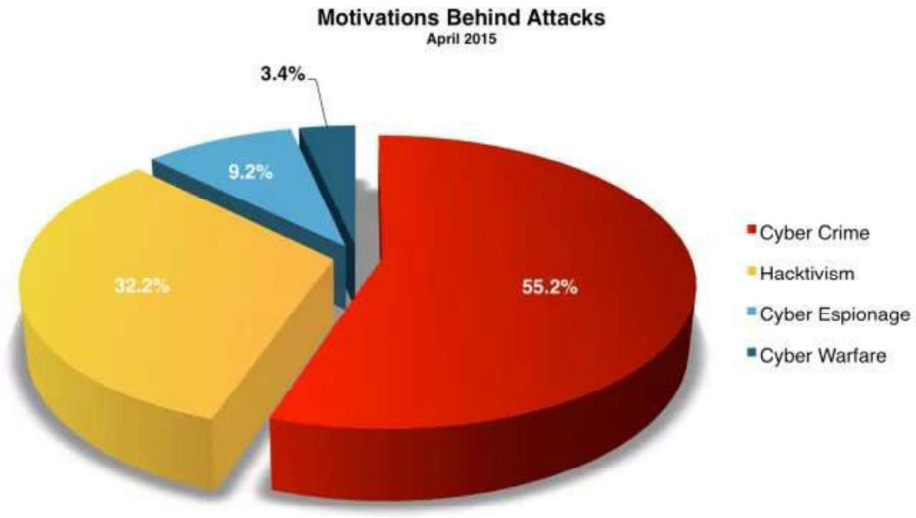


Figure 1: Motivation behind attacks[10]

1.6 LET US SUM UP

1 A **cyber attack** is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it.

2 **Hacktivism** is the act of hacking, or breaking into a computer system, for a politically or socially or ideologically motivated purpose.

3 **Cyber crime,** though, in a broad sense, covers any illegal activity that is committed through a digital means, here it refers to an activity with the monetary gain in mind.

4 **Cyber espionage** is unauthorized spying by computer.

5 **Cyber war** is simply the act of fighting on an electronic battlefield with digital weapons

[10]http://www.hackmageddon.com/category/security/cyber-attacks-statistics/

1.7 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Fill in the blanks:**

a. _____ is an attack initiated from a computer against a website, computer system or individual computer.

b. A_____is a spyware that has the capability to spy on the happenings on the computer system.

c. _____ is the act or practice of obtaining secrets without the permission of the holder of the information

d. _____is a threat of information through the hackers can gain access to the information and data on a Bluetooth enabled phone.

e. _____is a type of cyber security threat which will restrict access to your computer system at first and will ask for a ransom in order for the restriction to be removed.

Answers

a. Cyber attack
b. Keylogger
c. Cyber spying, or cyber espionage
d. Bluesnarfing
e. Ransomware

2. **State True or False:**

a. Hostile code like StuxNet is an example of weapons for cyber warfare.

b. Phishing is basically an email fraud where the perpetrator sends a legitimate looking email and attempts to gain personal information.

c. The ransom in Ransomware attack is to be paid through online payment methods.

d. In a privilege escalation attack URL are changed without the customer's knowledge.

e. Hacktivists are responsible for denial-of-service (DoS).

Answers

a. True
b. True
c. True

d. False
e. True

1.8 ASSIGNMENTS

1. What is Cyber Attack? How it is different from electronic authentication?
2. What are the different types of cyber attack?
3. Explain different types of Cyber Attacks in details.
4. What is Hacktivism?
5. Write a short note on Cyber War.
6. What is Cyber espionage?

1.9 ACTIVITIES

- Study about cyber-attacks happened during last five year globally.

Unit 2: Asset, Threat and Risk Management

2

Unit Structure

2.1 LEARNING OBJECTIVES

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

- Know Assets, classification of assets and protection of assets.
- Understand Vulnerability and Threat management
- Define Risk Management, Risk assessment, Risk treatment, Risk Mitigation

2.2 INTRODUCTION

Information security core objective is to secure the information asset of the organization. Loss of information can have severe impact over the economic condition of the organization along with the reputation loss in the market. It is a well-known fact that you cannot secure what you do not know exist in your environment. Asset management is all about discovery, ownership, value, acceptable use, protection, disposal of information related assets. Assets can be tangible and intangible. Examples of tangible assets are software and data while server is an example of tangible asset

The task of identifying assets that need to be secure is a less glamorous aspect of information security. But unless we know these assets, their locations and value, how are we going to choose the amount of time, effort or money that we should spend on safeguarding the assets? The major steps required for asset classification and controls are:

- Identification of the assets
- Accountability of assets
- Preparing a schema for information classification
- Implementing the classification schema

2.2.1 Identification of assets

What are the critical assets? Suppose your corporate office was devastated in a major fire. Surviving with this level of adversity will depend on what critical information you previously backed up at a remote location. Another terrifying scene is that a hacker hacked into your network and copied your entire customer

database. What impact will this have on your business?

Identifying the critical assets is important for many reasons. You will come to know what is critical and crucial for the business. You will be able to take suitable decisions regarding the level of security that should be provided to safeguard the assets. You will also be able to decide about the level of redundancy that is necessary by keeping an extra copy of the data or an extra server that you should procure and keep as a hot standby.

We should now focus on what is "Information Asset"? Is it hardware, software, program or database? We can broadly classify assets in the following categories:

2.2.1.1 Information assets

Every piece of information about your organization falls in this category. This information has been collected, classified, organized and stored in various forms.

i. Databases: Information about customer, production, finances and other different areas which are critical to the business. Confidentiality, Integrity and availability depends upon the classification by the data owner. Operational and support procedures: These have been developed over the years and provide detailed instructions on how to perform various activities.
ii. Archived information: Information of previous months or business cycles to maintain because of the law.

Continuity plans, fall-back arrangements: These plans are created to overcome any incident which can impact the business. Absence of these could result into the discontinuity of the business for a shorter or longer period depends upon the severity of the incident.

2.2.1.2. Software assets

These can be divided into two categories:

i. Application software: Application software implements business rules of the organization. Creation of application software is a time consuming

task. Integrity of application software is very important. Any flaw in the application software could impact the business adversely.

ii. System software: An organization would invest in various packaged software programs like operating systems, DBMS, development tools and utilities, software packages, office productivity suites etc.

Most of the software under this category would be available off the shelf, unless the software is obsolete or non-standard.

2.2.1.3 Physical assets

These are the visible and tangible equipment and could comprise of:

i. Computer equipment: Mainframe computers, servers, desktops and notebook computers.
ii. Communication equipment: Modems, routers, EPABXs and fax machines.
iii. Storage media: Magnetic tapes, disks, CDs and DATs.
iv. Technical equipment: Power supplies, air conditioners.
v. Furniture and fixtures

2.2.1.4 Services

Services that organization has outsourced to third party.

2.2.2 Accountability of assets

The next step is to create accountability of assets. This can be done easily for the tangible asset. A more difficult task is creating ownership for the information assets. There will be a number of users for these assets. But the prime responsibility for accuracy will lie with the asset owner. Any addition or modification to the information asset will only be done with the consent of the asset owner. For example, any changes to customer information will be done with the knowledge and consent of the marketing head. Information technology staff will probably make the changes, physically. But ownership clearly lies with the business head who has the prime responsibility for the content in the customer database.

Using these criteria, we have to identify the actual owners of each of the

information assets. This is also an important step for one more reason. Only an owner of the asset will be able to decide the business value of the asset. Unless the correct business value of the asset is known, we cannot identify the security requirement of the asset.

The next step is identifying owners of the application software. Application software implements the business rules. As such the business process owner should be the owner of application software. But the responsibility of maintaining application software to accurately reflect business rules will be vested with the application developers. As such, the accountability for application software should be with the application development manager.

System software ownership could be with the appropriate persons within the IT team. The owner of these assets will be responsible for maintaining all the system software including protecting the organization against software piracy.

2.2.2.1 Assets valuation

Another important task is to identify the value of the asset. Asset owner is the right person to verify the value of the asset. But the valuation of the information is a tedious task and depends on many factors which needs to be consider while evaluating them. We need to also consider the fact if in case information is not available how much it will going to impact our business. Also in case this information is leaked in market how it will going to impact the organization reputation in the market.

2.2.3 Preparing a schema for classification

The next important task is to create classification levels. The criteria for the classification of assets could be:

1. Confidentiality: Information comes under this criteria is highly important to the organization and only privileged employees should have access to it. Proper control should be put in place to control the access to this information.
2. Value: What is the asset value? Is it a high value item, costly to replace or a low value item?
3. Time: Is the information time sensitive? Will its confidentiality status change

after some time?

4. Access rights: Who will have access to the asset?
5. Destruction: How long the information will be stored? How can it be destroyed, if necessary?

Each asset needs to be evaluated against the above criteria and classified for easy identification. Let us look at each category for classification.

Confidentiality could be defined in terms of:

a. **Confidential**: Where the access is restricted to a specific list of people. These could be company plans, secret manufacturing processes, formulas, etc.
b. **Company only**: Where the access is restricted to internal employees only. These could be customer databases, manufacturing procedures, etc.
c. **Shared**: Where the resources are shared within groups or with people outside of the organization. This could be operational information and contact information like the internal telephone book to be shared with business partners and agents.
d. **Unclassified**: Where the resources are publicly accessible. For example, the company sales brochure and other publicity material.

Classification based on values could be high, medium or low value. Business justifications should be needed to support this classification. Criticality of the assets depends upon the impact it will create on the business. For example, a server who might not be very expensive but it can have the data which is very critical to the organization.

Access rights need to be defined for individuals by the owners. It depends on who is allowed to access the confidential information in the organization. Also who will approve to access those data in the organization?

Destruction of the information is a controlled activity. The information that is not required by the company any longer should be used by the competitor in the same business, that information should be destroyed by the pre-decided schedule and method depends on the confidentiality classification.

Classification schema should lead to an implementable structure. It should be simple to understand and identify.

2.2.4 Implementation of the classification schema

The real test of classification schema is when it is implemented. Information is a fluid resource. It keeps changing its form. The implementation should lead to a uniform way of identifying the information so that a uniform protection could be provided.

Let us take an example. A company's business plan is a confidential document. Let us trace its journey in the corporate world. The plan will be discussed behind closed doors, known to only a few senior members. In the next step the final plan will be prepared and stored on the MD's computer or that of his secretary. A soft copy of this plan would be sent by email to all executives who need to refer to it. The hard disk of every computer where the plan is stored will also have a backup copy on floppy or other media. Each member will no doubt print it and keep a hard copy folder for reference. An extra copy will also be prepared using the copying machine. If the email is not available, the plan would be sent by fax, post or courier.

So the 'confidential' plan is now distributed across the organization, available on the hard disks of computers belonging to each secretary and each senior executive. You get the general idea. If this can happen to confidential information, imagine how easy it is to get hold of other types of information. The information explosion has given rise to proliferation of information in every nook and corner of the organization.

A practical implementation of classification schema thus becomes very important. The classification label should not give an easy way of identification, which could be misused. It should provide the right amount of protection. In the example given above, each and every asset where the confidential information is residing or transiting through will have to be given the same classification level as that of the information itself. It may be desirable to altogether avoid transmission of confidential documents in soft copy format, for example as an attachment to email. Only a restricted number of hard copies should be circulated. If it is necessary to carry the soft copies, everyone should be

instructed to encrypt information for transmission and storage, and to memorize their passwords and keep them secret.

These frame works are used as plans or blueprints to design the security of an information security program to mitigate risk and bring down the impact of the risks under the acceptance criteria. Frameworks are often customized as per the requirement of the organizations. Framework assists enterprise to achieve their objectives and deliver values through effective governance and management.

2.3 VULNERABILITY AND THREATS

Information security vulnerabilities are weaknesses that expose an organization to risk. Vulnerability is a weakness in a system that could allow an attacker to compromise the security of the organization.

Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. Vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

Threats can exploit the vulnerabilities to impact the performance of the systems. A threat, in the context of information security, refers to anything that has the potential to cause serious harm to a system. Threats can include everything from viruses, Trojans, and back doors to outright attacks from hackers. A threat is something that may or may not happen, but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more.

The lack of access control in an office can be an example of vulnerability but unauthorized person who intentionally or unintentionally want to access the office premises will act as a threat which can exploit the absence of access control in the premises.

2.3.1 Types of threat

- **Physical damage**
  - fire
  - water
  - pollution
- **Natural events**
  - climatic
  - seismic
  - volcanic
- **Loss of essential services**
  - electrical power
  - air conditioning
  - telecommunication
- **Compromise of information**
  - eavesdropping,
  - theft of media
  - retrieval of discarded materials
- **Technical failures**
  - equipment
  - software
  - capacity saturation
- **Compromise of functions**
  - error in use
  - abuse of rights
  - denial of actions
- **Accidental**
  - equipment failure
  - software failure
- **Environmental**
  - natural event
  - loss of power supply

2.4 RISK MANAGEMENT

Risk management is an activity to manage the assessment, mitigation and monitoring of the risk in an organization. Information Security Risk Management is subset of the enterprise risk management. Information Security risk management access the risk which can impact the 'Confidentiality', 'Integrity' and 'Availability' of the organizational information. It also helps to identify the appropriate management actions and defined the priorities for implementing controls to protect those risks.

The risk management process help to create the organizational priorities and help organization to identify risk appetite for them. Top level management is authorized to make decisions about risk acceptance criteria.

Information security decisions should be managed by the top management. Only leadership of the organization should be able to decide the risk acceptance criteria because they are the stakeholders.

This process can be broadly divided into two components:

- Risk assessment
- Risk Mitigation

Risk assessment identifies, quantifies, and prioritizes risks against both criteria for risk acceptance and intents related to the organization. The assessment will result into the proper priorities of security risks and implementation of controls for securing those risks. The assessment result into determining of appropriate management actions and priorities for managing information security risks and for implementation of controls against them. The assessment helps to identify the impact of the risk. It also helps to identify the amount of resources needs to protect the assets. The scope of a risk assessment can be either whole organization, parts of the organization, and individual information system, or even specific system components or services. Performing risk assessment in a company infrastructure includes vulnerability assessment to help quantify risks. This process of assessing risks and helps to quantify them. This will also ensure that constantly evolving changes in security requirements and/or significant changes are assessed. For example, IT will be implementing new products or

service each year and new additional risk may be introduced due to vulnerabilities that can be exploited.

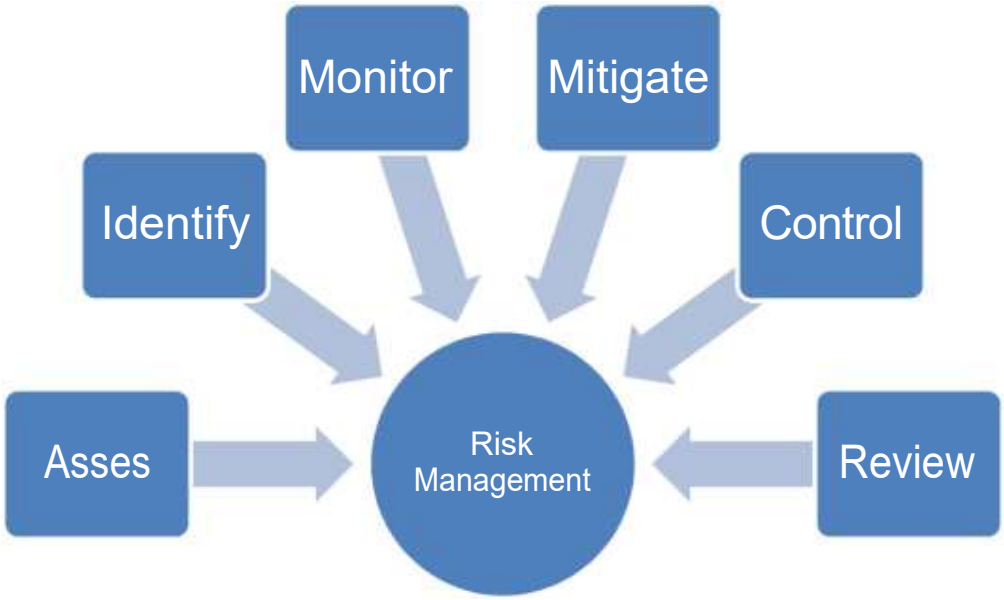


Figure 2: Risk management

Once a risk assessment is finished, risk treatment/risk mitigation is the next step in the process. For each of the risks identified during an assessment there should be a risk mitigation needs to be made. Risk mitigation is a systematic methodology used by senior management to reduce impact of the risk.

Risk mitigation can be completed through any of the following risk mitigation options:

- Risk Assumption: To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level.
- Risk Avoidance: To avoid the risk by eliminating the cause or root cause of the system.
- Risk Limitation: To avoid the risk by eliminating the risk cause and/or consequence (e.g., for certain functions of the system or shut down the system when risks are identified)

Once a risk assessment is finished, risk treatment/risk mitigation is the next step in the process. For each of the risks identified during an assessment there should be a risk mitigation needs to be made. Risk mitigation is a systematic methodology used by senior management to reduce impact of the risk. Risk mitigation can be completed through any of the following risk mitigation options:

- Risk Assumption: To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level.
- Risk Avoidance: To avoid the risk by eliminating the cause or root cause of the system.
- Risk Limitation: To avoid the risk by eliminating the risk cause and/or consequence (e.g., for certain functions of the system or shut down the system when risks are identified)
- Risk Planning: To manage risk by developing risk mitigation plan that prioritizes, implements, and maintains controls.
- Risk Transfer: To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

There are a variety of risk assessment tools and methodologies that can be used, but all are basically divided into quantitative and qualitative risk assessments.

2.4.1 Quantitative Risk Assessment

Quantitative risk assessments attempt to allocate a monetary value to the assets being measured, a monetary cost to the influence of an adverse event, and percentages to the frequency of threats and the likelihood of events. The monetary values and costs mentioned above are used to determine three elements needed to complete a quantitative risk assessment:

1. **Single Loss Expectancy (SLE):** What is the predictable loss from a single event? Consider physical destruction or theft of assets, loss of data, stopped or delayed processing, and interruption of business processes. Single-loss expectancy (SLE) is the monetary value predictable from the occurrence of a risk on an asset.

SLE = Asset Value x Impact (percent of asset loss incurred after an event)

2. **Annualized Rate of Occurrence (ARO):** How many times is an event expected to happen in a year?

For example, if insurance data suggests that a serious fire is likely to occur once in 25 years, then the annualized rate of occurrence is 1/25 = 0.04.

3. **Annual Loss Expectancy (ALO):** The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE).

ALO = SLE * ARO.

2.4.1.1 Advantages of Quantitative Risk Assessments

- Allows for a description and communication of consequences of event occurrence in monetary terms.
- It facilitates costs and benefits analysis for the selection of controls for the mitigation.

2.4.1.2 Disadvantages of Quantitative Risk Assessments

- It is very difficult in some cases to assign a dollar value to assets under the scope of the risk assessment. Especially in case information is under the scope of risk assessment as it is very difficult to identify the exact value of the information.
- Requires extensive time and staff resources.
- Values and costs are only as good and meaningful as the scope and accuracy of the amounts used to calculate them.
- Results of the assessment may be not exact and may be confusing.

2.4.2 Qualitative Risk Assessment

Qualitative risk assessments do not assign a financial value to the assets being measured, or to the impact of an adverse event. They measure the criticality of the assets and impact in range of high, low and medium. This ranking most parts comes under subjective:

- Low – Minor inconvenience tolerated for a short period of time.
- Medium — can result in destruction to the organization's assets which will require a moderate amount of time, effort, and money to repair.
- High— can result in loss of organization status. It will also result in a legal action or fine.

2.4.2.1 Advantages of Qualitative Risk Assessments

- Allows for ordering risks according to priority.
- Does not require extensive time and staff resources.
- It can recognize areas of greater risk in a short time and without significant expense.

2.4.2.2 Disadvantages of Qualitative Risk Assessments

- Results are estimates and subjective.
- Cost-benefit analysis during selection of mitigating controls is subjective.

2.5 LET US SUM UP

1. Asset management is all about discovery, ownership, value, acceptable use, protection, disposal of information related assets.
2. Information security vulnerabilities are weaknesses that expose an organization to risk. A vulnerability is a weakness in a system that could allow an attacker to compromise the security of the organization.
3. Threats can exploit the vulnerabilities to impact the performance of the systems. A threat, in the context of information security, refers to anything that has the potential to cause serious harm to a system.
4. Risk management is an activity to manage the assessment, mitigation and monitoring of the risk in an organization
5. The risk management process help to create the organizational priorities and help organization to identify risk appetite for them. Top level management is authorized to make decisions about risk acceptance criteria.
6. Risk assessment identifies, quantifies, and prioritizes risks against both criteria for risk acceptance and intents related to the organization.

7. Quantitative risk assessments attempt to allocate a monetary value to the assets being measured, a monetary cost to the influence of an adverse event, and percentages to the frequency of threats and the likelihood of events.
8. Qualitative risk assessments do not assign a financial value to the assets being measured, or to the impact of an adverse event.

2.6 ASSIGNMENTS

1. What is information asset?
2. How compromise of information asset impact the organization?
3. Explain the relation between threat and vulnerability?
4. Explain risk management?
5. Explain difference between qualitative and quantitative risk assessment?
6. Explain difference between ALO, ARO and SLE?
7. Explain the activities in risk assessment process?

Unit 3: Organization Security & Frameworks

3

Unit Structure

3.1 LEARNING OBJECTIVES

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

1. Information Security Frameworks
2. Types of framework and their advantage.
3. Organization structure, roles and responsibilities.
4. Overview of Policy, Procedures and Guidelines.

3.2 INTRODUCTION

Information security framework is a collection of documented procedures that are used to describe policies, procedures and guidelines around the implementation and management of Information security controls as per the security requirements of the enterprise requirements. These frame works are used as plans or blueprints to design the security of an information security program to mitigate risk and bring down the impact of the risks under the acceptance criteria. Frameworks are often customized as per the requirement of the organizations. Framework assist enterprise to achieve their objectives and deliver values through effective governance and management.

3.2.1 Advantage of Information Security framework

Framework helps in achieving organizational objective in a systematic and uniformed manner. Few main advantages of using information security framework is given below:

- Maintaining of processed information to support business decision.
- Achieving strategic objectives and provide benefit through effective use of resources.
- Maintain risk at acceptance level.
- Optimize the cost of IT services and technology.
- Supporting compliance with relevant laws, regulation, contractual agreement and policies.

3.2.2 Many Standards, Best Practices and Frameworks

In the coming section, we will see many profitable and non-profitable

organizations have made their own methodologies to security management, security control objectives, process management and enterprise management

Basic break of these standards, frameworks are given below:

Security Program Development

- **ISO/IEC 27000 series** developed by ISO and IEC for the development and management of ISMS.

Enterprise Architecture Development

- **Zachman framework** is developed by ZohnZazhman for the development of enterprise architectures.
- **TOGAF Model** developed by the open group for the enterprise architectures development.
- **MODAF Architecture** framework used mainly in military support missions developed by the British Ministry of Defense.

Security Enterprise Architecture Development

- **SABSA model**, Model and methodology for the development of information security enterprise architectures.
-

Security Controls Development

- **COBIT** Set of control objectives for IT management developed by Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI)
- **SP 800-53Set** of controls to protect U.S. federal systems developed by the National Institute of Standards and Technology (NIST).

Corporate Governance

- **COSO** is a set of internal corporate controls to help decrease the risk of financial fraud developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.

Process Management

- **ITIL** Processes to permit for IT service management developed by the United Kingdom's Office of Government Commerce.
- **Six Sigma Business** management strategy that can be used to carry out process improvement.
- **Capability Maturity Model Integration (CMMI)** Organizational development for process improvement developed by Carnegie Mellon.

3.2.2.1 ISO 27001:2013

ISO 27001:2013, is an information security standard that was published in September'2013.It is revised version of ISO 27001: 2005, and is published by ISO (International Organization of Standards) and IEC(International Electrotechnical commission). This standard is specifically target to develop and maintain Information Security Management System in the organization. ISO 27001 gives the requirement for the implementation of ISMS (Information Security Management System).

Information Security Management System (ISMS) defines the control that need to be placed (configuration management, physical security management, data protection, auditing etc.) and explains how these should be treated during their whole lifecycle. ISMS provide a complete picture of the security by aligning and placing controls strategically in the organization. ISMS components should be integrated within the whole organization is should not be practiced in certain departments of the organization.

ISO 27001:2013 has 14 domains and 114 controls. Refer to ISO 27001:2013 to understand exactly the control structure. Due to intellectual property right we could list exact controls of ISO 27001:2013 but control structure and their purposes are given below:

1. **A.5 Information security policies –** It defines the control on how policies are documented and reviewed.
2. **A.6 Organization of information security –** It defines the control on the responsibilities given to different individuals.
3. **A.7 Human resources security –** It defines the control before the employment, during the employment and after employee left the organization.

4. **A.8 Asset management –** It defines the controls on information classification, media handling and inventory of assets.
5. **A.9 Access control –** It defines controls on accessing user access management, application, server and user responsibilities along with them.
6. **A.10 Cryptography –** It defines control related to encryption and decryption.
7. **A.11 Physical and environmental security –** It defines controls mentioning secure areas, access control for entrance and exit, equipment security, protection against threats, secure disposal, clear desk and clear screen.
8. **A.12 Operational security–** It defines controls related to change management, capacity management, backup, logging, monitoring, installation, vulnerabilities etc.
9. **A.13 Communications security–** It defines control related to network security, network services, transfer of information.
10. **A.14 System acquisition, development and maintenance –** It defines control for mentioning security requirement and development and support process.
11. **A.15 Supplier relationships –** It defines control on agreements controls on what to include in agreements, and how to monitor the suppliers
12. **A.16 Information security incident management –** It defines controls for reporting incidents, defining weakness, response procedure and collection of evidence.
13. **A.17 Information security aspects of business continuity management –** It defines the controls related to the plan of business continuity, procedures, verification and reviewing.
14. **A.18 Compliance –** It defines controls requiring the identifying applicable laws and regulation on intellectual property protection of personal data etc.

Table 1: Comparison of ISO 27001:2005 to ISO 27001:2013

Context	ISO 27001:2005	ISO 27001:2013
Process	The standard clearly states that it follows PDCA (Plan-Do-Check-Act) model.	The Standard does not mention any specific process model.
Risk Assessment	In ISO 27001:2005 asset owner determines how to treat the risk, accepting residual risk.	The Risk assessment and risk treatment plan process are aligned to ISO 31000.
Controls	There are 133 controls across 11 domains	There are 114 controls across 14 domains.
Documentation	Standard used records and documentation to cover all the requirements. Document include policies, procedure and guidelines. Records include audit, schedules etc.	There is no such distinction between control and records.

3.2.2.2 COSO

COBIT was derived from COSO framework which was developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). In 1985, to deal with enterprise risk management, fraudulent activities, internal control and financial reporting. The COSO internal control framework comprises of five interconnected components derived from the way management manages a business. COSO assures that these components provide an effective framework for describing and evaluating According to COSO, these components provide an effective framework for describing and analyzing internal control system integrated in an organization. The five components are the following:

1. **Control environment:** The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.
2. **Risk assessment:** Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives and thus risk assessment is the identification and analysis of relevant risks to the achievement of assigned objectives. Risk

assessment is a prerequisite for determining how the risks should be managed.

3 **Control activities:** Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address the risks that may hinder the achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

4 **Information and communication:** Information systems play a key role in internal control systems as they produce reports, including operational, financial and compliance-related information that make it possible to run and control the business. In a broader sense, effective communication must ensure information flows down, across and up the organization. For example, formalized procedures exist for people to report suspected fraud. Effective communication should also be ensured with external parties, such as customers, suppliers, regulators and shareholders about related policy positions.

5 **Monitoring**: Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities or separate evaluations. Internal control deficiencies detected through these monitoring activities should be reported upstream and corrective actions should be taken to ensure continuous improvement of the system.

The framework mentioned 17 principles associated with each components.

Table 2: COSO framework

Internal Control Component	**Principles**
Control environment	1. Demonstrate commitment to integrity and ethical values 2. Ensure that board exercises oversight responsibility 3. Establish structures, reporting lines, authorities and responsibilities 4. Demonstrate commitment to a competent workforce 5. Hold people accountable
Risk assessment	6. Specify appropriate objectives 7. Identify and analyze risks 8. Evaluate fraud risks 9. Identify and analyze changes that could significantly affect internal controls
Control activities	10. Select and develop control activities that mitigate risks 11. Select and develop technology controls 12. Deploy control activities through policies and procedures
Information and communication	13. Use relevant, quality information to support the internal control function 14. Communicate internal control information internally 15. Communicate internal control information externally
Monitoring	16. Perform ongoing or periodic evaluations of internal controls (or a combination of the two) 17. Communicate internal control deficiencies

There are certain limitation as Framework recognize that as internal control provide assurance of achieving the organizations objective, but limitation do exist as internal control do not overcome bad judgments, external events etc. which can cause failing of achieving its operational goal. Organization can face the failure from multiple factors:

- Breakdown due to human failures.
- Cases in which management override internal control.
- External event beyond the organizations control.
- Mistakes due to human intervention.

3.2.2.3 COBIT (IT Governance Framework)

Before understand the COBIT framework we need to understand use and motive of IT governance frameworks. IT governance is a management initiative to develop a structured framework which allow organization to align the IT with

the business goals while reducing risk and improving continually. IT governance is a top down approach which require strong management support to be successful in the organization. IT Governance focuses majorly on five areas given below:

1 Strategic alignment emphases on guaranteeing the linkage of business and IT plans; describing, maintaining and validating the IT value; and aligning IT operations with enterprise goals.

2 Value delivery is about accomplishing the value proposition throughout the delivery cycle, confirming that IT delivers the promised benefits against the strategy, focused on optimizing costs and proving the value of IT.

3 Resource management is about the optimum investment in, and the appropriate management of, critical IT resources: applications, information, infrastructure and people.

4 Risk management needs risk awareness by senior officers, a clear picture of the enterprise's acceptance of the risk, understanding of compliance and technical requirements.

5 Performance measurement monitors strategy implementation, project completion, resource usage, process performance and service delivery, using balanced scorecards that translate strategyinto action to achieve goals.

COBIT (Control objective for information and related technology) is a framework for developing, implementing, monitoring and improving Information technology governance and management practices. The COBIT framework is published by ISACA in 1996. The framework support organization governance by aligning IT goals with business goals. It helps enterprise to drive optimal value from IT by maintaining balance between resources use, benefits and optimizing risk levels. Adoption of COBIT will allow the organization to achieve the following goals:

- Alignment of IT with the business goals.
- Increased the importance of IT to business.
- Risk reduction.
- Continual improvement of IT.
- Development of goals and scorecards for measurement of IT in a structured

way.

COBIT has 5 key principles:

- Principle 1: Meeting Stakeholders Needs.
- Principle 2: Covering the enterprise end to end.
- Principle 3: Applying a single, integrated framework.
- Principle 4: enabling a Holistic approach.
- Principle 5: Separating governance from management.

Table 3: Differences between COSO and COBIT

COSO	COBIT
COSO is a model for cooperate governance.	COBIT is a model for IT governance.
COSO deals more at strategic level.	COBIT focuses more at operational level.

3.3 POLICIES, STANDARDS, BASELINES, GUIDELINES AND PROCEDURES

3.3.1 Security Policy

A Security policy is a statement given by the top management that reflects the role of security in the organization. It can be organizational policy, issue related policy or specific system related policy. Organization Security policy defines how the organization security program will be executed, program goals, roles and responsibilities and outlines how enforcement should be carried out. The organization security policy outlines how all security related activities will be carried out in the organization.

Organization security policy should have several important characteristic that should be understood and implemented:

- Policy should be aligned with the business objective, business should not be aligned with the policy.
- It should be easily understood document that is used as a reference point for all employee and management.
- It should be used to induce security into the business functions.
- It should be changed with any business function such as merger with the new company, adoption of new technology or change of

management/ownership.

- It should be tracked through version control.
- It should have clear and declarative statements.
- It should be reviewed on regular basis.

The Types of policies are given below:

1 **Regulatory** This type of policy ensures that the organization is following standards set by specific industry regulations (HIPAA, GLBA, SOX, PCI-DSS, etc.). It is very detailed and specific to a type of industry. It is used in financial institutions, healthcare facilities, public utilities, and other government-regulated industries.

2 **Advisory** This type of policy strongly advises employees as to which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if Employees do not comply with the established behaviors and activities. This policy type can be used, for example, to describe how to handle medical or financial information.

3 **Informative** This type of policy informs employees of certain topics. It is not an enforceable policy, but rather one that teaches individuals about specific issues relevant to the company. It could explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations.

A common hierarchy of security policies is outlined here:

- Organizational policy
- Acceptable use policy
- Risk management policy
- Vulnerability management policy
- Data protection policy
- Access control policy
- Business continuity policy
- Log aggregation and auditing policy
- Personnel security policy
- Physical security policy
- Secure application development policy

- Change control policy
- E-mail policy
- Incident response policy

3.3.2 Guidelines

Guidelines are recommended actions and operational instructions to users, IT staffs, where specific standard does not apply. A guideline is used to determine the course of action according to a set routine. Guidelines are the best practices used to achieve the goals mentioned in the security policy.

3.3.3 Procedure

Procedure are detailed step-by-step that should be accomplished to reach a certain goal. This apply to IT staff, Information security group members and others who need to carry out specific tasks. Procedures are at the lower level where in the documentation series because they are near to the computers and users. They provide detailed steps for configuration.

Procedure practically shows how policy, procedure and guidelines are actually implemented in the practical scenario. If policy states that password should be alpha numeric then procedure specifically explains how to configure the same on the systems.

3.4 LET US SUM UP

1. ISO 27001:2013 is a standard which explain the requirement to implement Information Security Management System.
2. Information security framework is a collection of documented procedures that are used to describe policies, procedures and guidelines around the implementation and management of Information security controls as per the security requirements of the enterprise requirements.
3. Frameworks are used to provide a structural approach to implement security in a systematic approach.
4. IT governance is a management initiative to develop a structured framework which allow organization to align the IT with the business goals while

reducing risk and improving continually.

5. COBIT is derived from the COSO framework
6. COSO deal with enterprise risk management, fraudulent activities, internal control and financial reporting.
7. A Security policy is a statement given by the top management that reflects the role of security in the organization. It can be organizational policy, issue related policy or specific system related policy.
8. Procedure are detailed step-by-step that should be accomplished to reach a certain goal. This apply to IT staff, Information security group members and others who need to carry out specific tasks.
9. Guidelines are recommended actions and operational instructions to users, IT staffs, where specific standard does not apply. A guideline is used to determine the course of action according to a set routine.
10. The survival and integrity of any given network infrastructure of any company or organization strongly depends on the application of computer forensics.

3.5 ASSIGNMENTS

1. What is Information Security Management System?
2. What is difference between ISO 27001:2005 and ISO 27001:2013?
3. Explain 5 components of COSO framework?
4. What is major difference between COSO and COBIT?
5. Explain the 5 focus areas on which IT governance focuses?
6. Explain difference between policy, procedure and guidelines

Block-2

Unit 1: Security Controls 1

Unit Structure

1.1. LEARNING OBJECTIVES

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

- Know security basics
- Implement physical controls
- Define access control models
- Understand desktop security
- Implement password security

1.2. INTRODUCTION

Securing the modern business network and IT infrastructure demands an end-to-end approach and a firm grasp of vulnerabilities and associated protective measures. While such knowledge cannot thwart all attempts at network incursion or system attack, it can empower network engineers to eliminate certain general problems, greatly reduce potential damages, and quickly detect breaches. With the ever-increasing number and complexity of attacks, vigilant approaches to security in both large and small enterprises are a must. Prior to discussing Procedural / People security controls we will start by defining security controls in general.

Security Controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

People are truly the weakest link in any security schema. Most people are not careful about keeping secrets such as passwords and access codes that form the basis for most secure systems. All security systems rely on a set of measures employed to control access, verify identity and protect disclosure of sensitive information. These measures usually involve one or more “secrets”. Should a secret be revealed or stolen then the systems that are protected by these secrets can be compromised. It may seem like a terribly obvious statement, but most systems are compromised in very basic ways. Leaving a

Post-It note with a system password stuck to the side of a computer monitor may seem foolish, but many people in fact do such things. Another example, which is only slightly less obvious, is the tendency to leave factory default passwords in certain network devices. One such device might be a network management interface to a UPS. UPS systems, whether small in capacity or large enough to power 100 servers, are often overlooked in a security scheme. If such devices are left with default usernames and passwords, it could just be a matter of time before someone gains access knowing nothing more than the device type and its published default credentials. Imagine a server bank with rock solid security protocols on each web and mail server crashed by a simple power cycle on an unprotected UPS!

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; and the way management assigns authority and organizes and develops its people.

1.3. SECURITY BASICS

It is not possible to protect anything unless one clearly understands WHAT one wants to protect. Organizations of any size should have a set of documented resources, assets and systems. Each of these elements should have a relative value assigned in some manner as to their importance to the organization. Examples of things that should be considered are servers, workstations, storage systems, routers, switches, hubs, network and Telco links, and any other network elements such as printers, UPS systems and HVAC systems. Other important aspects of this task include documenting equipment location and any notes on dependencies. For instance most computers will rely on power backup systems such as UPSs which themselves may be part of the network if they are managed. Environmental equipment such as HVAC units and air purifiers may also be present.

The next step is to identify the potential "threats". Threats can come from both

internal and external sources. They may be human based, automated or even non-intentional natural phenomenon. The latter might more appropriately be categorized under system health threats as opposed to security threats, but one issue can lead to the other. One example is a power outage to a burglar alarm. The power outage could be intentional or through some natural event such as a lightning strike. In either case security is diminished.

To help review or design security controls, they can be classified by several criteria, for example according to the time that they act, relative to a security incident:

a. **Preventive Controls** are intended to prevent an incident from occurring i.e. these controls are implemented before the event takes place. They exist to prevent the threat from coming in contact with the weakness, e.g. by locking out unauthorized intruders.
b. **Detective Controls** are applied during the event and are intended to identify and characterize an incident in progress. These exist to identify that the threat has landed in our systems, e.g. by sounding the intruder alarm and alerting the security guards or police.
c. **Corrective Controls** are executed after the event and are intended to limit the extent of any damage caused by the incident. In other word they exist to mitigate or lessen the effects of the threat being manifested, e.g. by recovering the organization to normal working status as efficiently as possible.

Computer security is often divided into three distinct master categories, commonly referred to as *controls*:

a. Physical
b. Technical
c. Administrative

These three broad categories define the main objectives of proper security implementation. Within these controls are sub-categories that further detail the controls and how to implement them.

1.3.1 Physical Controls

The Physical control is the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material. Examples of physical controls are:

i. Closed-circuit surveillance cameras

ii. Motion or thermal alarm systems

iii. Security guards

iv. Picture IDs

v. Locked and dead-bolted steel doors

1.3.2 Technical Controls

The Technical control uses technology as a basis for controlling the access and usage of sensitive data throughout a physical structure and over a network. Technical controls are far- reaching in scope and encompass such technologies as:

i. Encryption

ii. Smart cards

iii. Network authentication

iv. User Access control

v. File integrity auditing software

1.3.3 Administrative Controls

Administrative controls define the human factors of security. It involves all levels of personnel within an organization and determines which users have access to what resources and information by such means as:

i. Training and awareness

ii. Disaster preparedness and recovery plans

iii. Personnel recruitment and separation strategies

iv. Personnel registration and accounting

1.3.4 Physical security, protection on the inside

Most experts would agree that all security starts with physical security. Controlling physical access to machines and network attach points is perhaps more critical than any other aspect of security. Any type of physical access to an internal site creates a major exposure of the site. Secure files, passwords, certificates and all sorts of other data can usually be obtained if physical access is possible. Fortunately there are all sorts of access control devices and secure cabinets that can help with this problem.

1.3.5 Partitioning and protecting network boundaries with firewalls

Besides the basic physical security of a site, the next most important aspect is controlling digital access into and out of the organization's network. In most cases this means controlling the points of connectivity to the outside world, typically the Internet. Almost every medium and large-scale company has a presence on the Internet and has an organizational network connected to it. In fact there is a large increase in the number of smaller companies and homes getting full time Internet connectivity. Partitioning the boundary between the outside Internet and the internal intranet is a critical security piece. Sometimes the inside is referred to as the "trusted" side and the external Internet as the "un-trusted" side. As a generality this is all right, however, as will be described, this is not specific enough.

A firewall is a mechanism by which a controlled barrier is used to control network traffic into AND out of an organizational intranet. Firewalls are basically application specific routers. They run on dedicated embedded systems such as an internet appliance or they can be software programs running on a general server platform. In most cases these systems will have two network interfaces, one for the external network such as the Internet and one for the internal intranet side. The firewall process can tightly control what is allowed to traverse from one side to the other. Firewalls can range from being fairly simple to very complex. As with most aspects of security, deciding what type of firewall to use will depend upon factors such as traffic levels, services needing protection and

the complexity of rules required. The greater the number of services that must be able to traverse the firewall the more complex the requirement becomes. The difficulty for firewalls is distinguishing between legitimate and illegitimate traffic.

What do firewalls protect against and what protection do they not provide? Firewalls are like a lot of things; if configured correctly they can be a reasonable form of protection from external threats including some denial of service (DOS) attacks. If not configured correctly they can be major security holes in an organization. The most basic protection a firewall provides is the ability to block network traffic to certain destinations. This includes both IP addresses and particular network service ports. A site that wishes to provide external access to a web server can restrict all traffic to port 80 (the standard http port). Usually this restriction will only be applied for traffic originating from the un-trusted side. Traffic from the trusted side is not restricted. All other traffic such as mail traffic, ftp, snmp, etc. would not be allowed across the firewall and into the intranet.

An even simpler case is a firewall often used by people with home or small business cable or DSL routers. Typically these firewalls are setup to restrict ALL external access and only allow services originating from the inside. A careful reader might realize that in neither of these cases is the firewall actually blocking all traffic from the outside. If that were the case how could one surf the web and retrieve web pages? What the firewall is doing is restricting connection requests from the outside. In the first case all connection requests from the inside are passed to the outside as well as all subsequent data transfer on that connection. From the exterior, only a connection request to the web server is allowed to complete and pass data, all others are blocked. The second case is more stringent as connections can only be made from the interior to the exterior.

More complex firewall rules can utilize what is called “stateful inspection” techniques. This approach adds to the basic port blocking approach by looking at traffic behaviors and sequences to detect spoof attacks and denial of service attacks. The more complex the rules, the greater the computing power of the

firewall required.

One problem most organizations face is how to enable legitimate access to "public" services such as web, ftp and e-mail while maintaining tight security of the intranet. The typical approach is to form what is known as a DMZ (demilitarized zone), a euphemism from the cold war applied to the network. In this architecture there are two firewalls: one between the external network and the DMZ, and another between the DMZ and the internal network. All public servers are placed in the DMZ. With this setup, it is possible to have firewall rules which allow public access to the public servers but the interior firewall can restrict all incoming connections. By having the DMZ, the public servers are still provided more protection than if they were just placed outside a single firewall site.

1.4. USER ACCESS CONTROLS

What is an access control? We can say it's a way to manage access to enterprise resources. It we go with the word definition, access control is a mechanism to control the flow of information between subject and object where subject is always as active entity while object is a passive entity. In its broadest meaning, access control is a three-step process that includes identification, authentication. In this white paper, the term authentication is generally used to represent both identification and authentication, and access control is used for authorization.

The section discusses the importance of selecting an access control model that fits with your security needs to provide a lower total cost of ownership and enable strong identification. It also discusses the various authentication solutions and weights their need to your organization.

1.4.1 Why Access Controls are required

As the business of an enterprise increases, so does the demand for access control since it is the first line of defense to protect the organization's resources. When you try to access a certain resource and you are asked to provide your identification – that is access control. Access control solutions provide protection, integrity, availability and auditing capability to the organization.

1.4.2 What are Access Control Models

Access control model is a framework that dictates access control using various access- control technologies. There are standard access control models which are highly domain and implementation independent. Each access control model has its own merits and demerits, and the specific business objectives they serve depend on the organization's need, culture, nature of business, etc. We will discuss these models and examine their fitness with respect to an organization's security policy and business goals.

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Role Based Access Control (RBAC)

1.4.3.1 Discretionary Access Control (DAC)

Discretionary Access Control is based on ownership and delegation. In a DAC Model, access is governed by the access rights granted to the user groups. An organization/administrator/creator can identify a set of operations and assign them to an object and to set of users and to a set of users (belonging to user group).

The DAC model is flexible but complex. It creates a paradox in some complex situations. For example, A is owner of resource R of organization O and he has delegated permission P1 and P2 to B who, in turn, has delegated permission P1 to C. Now, it A chooses to revoke permission to B what will happen to the permission that B granted to C?

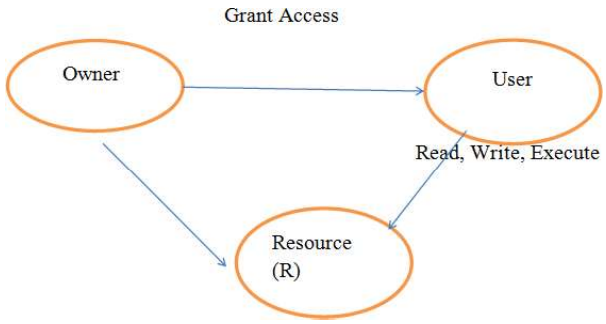


Figure 3: Discretionary Access Control

While the model above is complex, it is still flexible enough to handle various access control needs, and therefore is used in various network management applications.

1.4.3.2 Mandatory Access Control (MAC)

In MAC, the data owner has limited freedom to decide on access control. Information is classified into different categories and each category is assigned a particular security level. For example, resource R is a very confidential resource to the organisation and so has been assigned a “Very Confidential” security level. When a user, who has been assigned security level “Confidential”, tries to access this resource, he is denied access because the security level assigned to him doesn’t match. This model is appropriate when securing confidential of data is critical, as in—for example—military operation systems.

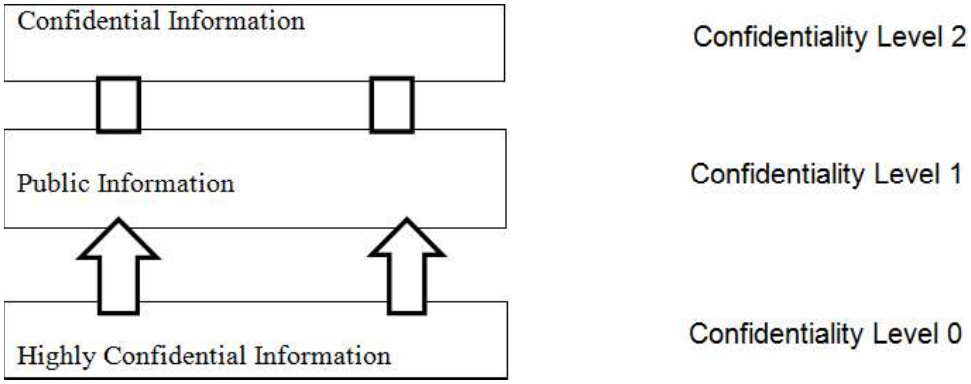


Figure 4: Mandatory Access Control

1.4.3.3 Role Based Access Control (RBAC)

RBAC is a widely used- and dominant- access control model, and most access control security products available in the market today are based on this model because its objectives are architectural. Entrust Get Access is one such product. The model allows access to a resource, based on the role the user holds in the organization. It is based on the concept of “separation of duties”. The privileges to the particular role are decided and thereafter mapped to the user. If the environment does not require a high level of security, the choices are usually discretionary and role based. The discretionary model gives data owners the ability to allow users to access resources, enabling choices to be

made with full knowledge of what it entails. If the organization has a high turnover rate, the role based model is more appropriate. If the environment requires higher level of security and it is desired that only administrator should grant the access control, then MAC is the best choice.

1.4.4 Authentication

Authentication or identification is the first step in any access solution. It is the process of identifying the user to verify whether he/she is what he/she claims to be. Normally, identification is done with the help of information that is known to everyone (i.e., user name or user ID) and some personal information known only to the subject (i.e. password). Faced with the threat of identity theft and increasing consequences associated with failing to secure information, enterprises are increasingly looking for stronger forms of authentication to enhance their overall security capabilities. At the same time, enterprises and governments need to take into account other important considerations such as usability, total cost of deployment and maintenance, and integration with existing security solution offerings. Usernames and passwords are the most common authentication techniques. But most organizations do not depend on user name authentication alone since username and passwords are an authentication solution for low-value transactions and for accessing non-sensitive information over the network. Also, experience has shown that usernames and passwords provide relatively weak authentication because they can often be guessed or stolen. They are often difficult to deploy because each application may implement its own scheme, adding to both development cost and user complexity. Also, it is very difficult to maintain and reset the password.. Determining the appropriate level of authentication that meets your budget requirements is essential when implementing your secure identity management solution. It is very crucial to identify the appropriate authentication technique depending upon the nature of the business and sensitivity of the information. One has to consider various authentication methods and their pros and cons. The means of authentication are often discussed in terms of “factors” of proof, such as:

- Something your know to prove your identity (e.g.a PIN)
- Something you have to prove your identity (e.g. a smart card)
- Something you have to prove your identity (e.g. a fingerprint)

A good authentication technique contains at least two of the above methods. In a client server environment, strong authentication is a combination of server and client authentication:

- Server authentication is when the server proves its identity to the client.
- Client authentications are when clients prove their identity to the server.

1.4.4.1 User password Authentication

It is the most common form of providing identification. When user accesses the resource, access control framework asks for the user name password provided to the user. The credentials are validat3d against the one stored in the system's repository.

1.4.4.2 Windows user based authentication

Usually, organizations have a list of users stored in the windows active directory. Access control framework should be able to provide authentication for the user of the Primary Domain Controller (PDC).

1.4.4.3 Directory based authentication

With the rising volume of business over the web, millions of user's often try to access the resource simultaneously. In such a scenario, the authentication framework should be able to provide for faster authentication. One such technique is Directory Based Authentication where user credentials are validated against the one which is stored in the LADAP Directory.

1.4.4.4 Certificate based authentication

This is probably one of the strongest authentication techniques where the user is asked to provide his/her digital ID. This digital ID, known as digital certificate, is validated against the trusted authority that issued the digital ID. There are various other parameters that ate checked to ensure the identification of the user.

1.4.4.5 Smart card based authentication

This is also used as a second factor authentication. Smart cards are small devices containing co-processors to process cryptographic data.

1.4.4.6 Biometrics

This is the strongest authentication. Known as third factor authentication, it is based on something the user is. It works after the users have provided something the know (User name password) and something they own (either a gird or token) or something they are (retina- scan, thumbprint or thermal scan). It is required in cases where data is top confidential, such as in Military/Defense.

1.4.4.7 Grid based Authentication

This is used as a second factor authentication. It authenticates the user based on something he knows (User name password authentication) and then asks for something he owns (gird card information). Entrust Identity Guard provides such an authentication.

1.4.4.8 Knowledge-based authentication

One of the simplest mechanisms for gaining additional confidence in a user's identity is to challenge the user to provide information that an attacker is unlikely to be able to provide. Based on "shared secrets", this allows for the organization to question the user, when appropriate, to confirm information that is already known about the user through a registration process, or from previous transactions.

1.4.4.9 Machine Authentication

Machine authentication provides validation of the user's computer in a way that secures against a variety of threats in a zero touch fashion, reducing user impact. This is an especially effective method of user authentication where users typically access their accounts from a regular set of machines, allowing for stronger authentication to be performed without any significant impact on the user experience.

1.4.4.10 One time Password (OTP)

A one-time password is dynamically generated and it is valid only for once. The advantage of one time password is that if an intruder hacks it, he cannot reuse it. These are two types of OTP token generators: synchronous and asynchronous. A synchronous token device synchronizes with the authentication service by using time or an event as the core piece of the authentication process. A token device, which is using as asynchronous token generating method, uses a challenge response scheme to authenticate the user.

1.4.5 Access Control Framework (ACF)

The access control framework (ACF), presented in this paper, is like an umbrella that covers both authentication and authorization. Whenever the user accesses any enterprise resource, ACF can come up with one or more authentication techniques depending on the need of the enterprise. Once the authentication is done, ACF can authorize the request, following any model, depending on the need of the organization.

1.4.6 Access Control Techniques and Technologies

Once an organization decides on the type of access control model to be employed, the next step would be to decide on the techniques and technology to be used. Here are some techniques and technologies:

1.4.6.1 Rule Based Access control

Rule based access control is based on rules defined on the object, as defined by the administrator who decides on the operations that can be performed by subject. A rule can be as simple as defining the day of the week on which the resource can be accessible.

1.4.6.2 Menu Based Access Control

In a menu based control, the user interface given to the user controls the operations that can be performed on the object, i.e., If A and B operations can be performed on object O, then the user interface pertaining to A and B options is enabled and the rest of the user interface is disabled.

1.4.6.3 Access Control List

Access control list is the list of subjects that are authorized to access a particular object. It also defines the level of authorization.

1.4.6.4 Content Based Access Control

In content based access control (CBAC), the access to the object is determined by the content within the object. For example, a manager can access the payroll database but only for employees reporting to him.

1.4.6.5 Access control Markup Language (XACML)

XACML is the access control markup language that is used to express the rules that are necessary for authentication and authorization. The vocabulary to express these rules is given by the access control markup language. These rules are used to make decisions regarding the authentication. eXtensible Access Control Markup Language – or XAVML – provides a Mechanism to create policies and rules for controlling access to information.

A typical access control and authorization scenario includes three main entities - a subject, a resource, and an action - - and their attributes. A subject makes a request for permission to perform an action on a resource. For example, in the access request, “Allow the Sys-admin to create files in the root folder of the production server” the subject is the “Sys-admin”, the target resource is the “root folder of the production server”, and the action is “create files”.

1.4.6.6 Security Assertion Markup Language (SAML)

SAML is an XML standard for exchanging authentication and authorization data between security domains, that is, between an identify provider (a producer of assertions) and a service provider (a consumer of assertions). SAML is a product of the OASIS Security Services Technical Committee.

The single most important problem that SAML is trying to solve is the Web Browser single sign-on (SSO) problem. Single sign-on solutions are abundant at the intranet level (using cookies, for example) but extending these solutions beyond the intranet has been problematic and has led to the proliferation of non-interoperable proprietary technologies. SAML has become the definitive

standard underlying many web single sign-on solutions in the enterprise problem space.

The whole thrust of access control is to restrict unauthorized users from accessing organization resources. The authentication techniques and access controls described in this white paper can be chosen based on an organization's need. The authentication and access control framework should be flexible enough to serve all the authentication techniques and future evolution in the area such as Biometrics. The access control framework should be able to handle an organization's authentication and authorization (access control) needs. Entrust Get Access and Identify Guard is the products with such features.

1.5. TRAINING AND AWARENESS

One of the greatest threats to information security could actually come from within your company or organization. Inside 'attacks' have been noted to be some of the most dangerous since these people are already quite familiar with the infrastructure. It is not always disgruntled workers and corporate spies who are a threat. Often, it is the non-malicious, uninformed employee.

The focus will be on uninformed users who can do harm to your network by visiting websites infected with malware, responding to phishing e-mails, storing their login information in an unsecured location, or even giving out sensitive information over the phone when exposed to social engineering.

One of the best ways to make sure company employees will not make costly errors in regard to information security is to institute company-wide security-awareness training initiatives that include, but are not limited to classroom style training sessions, security awareness website(s), helpful hints via e-mail, or even posters. These methods can help ensure employees have a solid understanding of company security policy, procedure and best practices. Some of the more important items to cover in your security awareness training are your organization's security policy, data classification and handling, workspace and desktop security, wireless networks, password security, phishing, hoaxes,

malware, file sharing and copyright.

1.5.1 Types of Training

Organizations are starting to realize there really is a need for security awareness training. According to a study conducted, the following statistics revealed a rather startling necessity:

- "One in five workers (21%) let family and friends use company laptops and PCs to access the Internet".
- "More than half (51%) connect their own devices or gadgets to their work PC... a quarter of who do so every day".
- "One in ten confessed to downloading content at work they should not".
- "Two thirds (62%) admitted they have a very limited knowledge of IT Security".
- "More than half (51%) had no idea how to update the anti-virus protection on their company PC".
- "Five percent say they have accessed areas of their IT system they should not have".

Security awareness training can be performed in a variety of ways that can be utilized alone or in conjunction with each other. Those mediums can consist of a more thorough classroom style training, creation of a security-awareness website, pushing helpful hints onto computers when they start up and/or e-mailing helpful hints on a weekly or monthly basis, and utilizing visual aids like posters.

1.5.1.1 Classroom-Style Training

Utilizing a classroom setting for security-awareness training can offer the benefit of lecture- based and interactive learning as well as the availability of someone to answer questions in real time. There can also be a Q&A period after the materials are presented as well as contact information distributed for questions that might pop up afterward.

Some companies offer both live and web-based training and utilize a variety of methods such as role-playing and simulation games so the interaction is more two-way than one-way. Other companies offer videos, web-based training, and live trainers. The method you use is by no means limited.

This type of training can vary in the amount of time it can take. The security

awareness training I have implemented at Washtenaw Community College takes about two hours, but it has no real interactivity such as role-playing or simulations; just PowerPoint and Q&A. Training time can depend on the effectiveness and the extent of the material discussed. Training sessions could possibly take a full day if need be.

1.5.1.2 Security Awareness Website

Another way of implementing a security awareness program is through the creation of a security awareness website. This website could consist of different sections with the different areas that need to be covered (e.g. Malware, hoaxes, file sharing and copyright, etc). The University of Tennessee implemented a very impressive security awareness website complete with videos, examples, and helpful external links.

Another implementation of the security awareness website could be a self-paced tutorial where users can log in and go through it, taking mini quizzes at the end of each section to make sure the material is actually being read and absorbed. Utilizing logins can also be a means of keeping track of who has (and more importantly who has not) taken the training. An FAQ section could be implemented as well as contact information for users to ask questions that are not addressed in the FAQ.

1.5.2 Helpful Hints

Utilizing helpful hints and tips is more of a supplement to the training, be it via classroom style or online, and should not be used as a means of security awareness training on its own. Helpful hints can consist of tips and reminders that are pushed to user screens when they log in. These tips and reminders can consist of key points emphasized in the training (e.g. “Never keep your password in a place that can be accessed or viewed by anyone besides yourself”). Reminders can be as simple as reminding someone to change their password or run their virus scan.

1.5.2.1 Visual Aids

Visual aids are another item that should not be used as the lone source of security awareness training, but more as a supplement. The University of Michigan recently created a series of catchy password security posters that compare passwords to underwear. One says to change them often, another

says to not leave passwords lying around, and another one says to not share them with friends.

1.5.2.2 Promotions

Security tips can appear on flyers distributed across the user base and one could even go so far as to hand out pencils and/or key chains with a catchy security-related phrase or reminder (e.g. “Unexpected attachments can mean unexpected chaos: Please do not open them”). Now that we have addressed possible methods in implementing security awareness training, what should be covered in the training will be addressed.

1.5.2.3 Training Topics

Topics addressed by the security awareness training should consist of a combination of existing organizational policies and procedures (how they tie in with each aspect, if they do), physical security, desktop security, password security, phishing, hoaxes, malware (viruses, worms, Trojans, spyware, and adware), and copyright with regard to file sharing. These topics will help employees understand why security awareness is important and guide them in knowing how to prevent incidents from happening and what to do if one occurs.

1.5.2.4 Physical Security

When addressing physical security, locking your doors and desk/file cabinet drawers should be the main focus. A helpful item to include could be the crime statistics, more specifically thefts, from the organization. Another item to lightly touch upon (but go into greater detail in Desktop Security) is the fact that if a potential attacker has access to a user’s computer, they could install a key logger or actually get into a machine that has not been locked.

1.5.2.5 Desktop Security

The desktop security section should go into detail as to why it is important to either have a password-protected screen saver or, even better, to get into the habit of locking computers when users walk away from them. A screensaver timeout should be utilized so if a user walks away from their computer, the password-protected screensaver would come up. Personally, I have mine set to 5 minutes, but upon doing a Google search regarding typical screensaver timeouts, the average response was 10 minutes. This information can and should be supplemented with information on how to do this. Tactics a potential attacker could utilize (e.g. Shoulder surfing, key loggers, etc) also need to be

addressed. The pill of having to take extra measures to make sure your desktop is secured can be swallowed more easily if users understand WHY they should be taking them.

Another item that could be addressed is to make sure users understand that it is important that they shut down their computers at the end of the day. Sometimes this allows for valuable updates to be applied and doing your own part for a greener environment. If somehow a potential attacker gains access to a computer that is turned off, they will be less likely to utilize it than one that is already turned on and unlocked.

1.5.2.6 Wireless Networks and Security

The wireless networks and security section should address the unsecure nature of wireless networks as well as tips and tricks to exercise caution and harden laptops against the dangers of 'sniffing'. Emphasis should also be placed on not storing any kind of sensitive information on laptops that will be accessing a wireless network. Another area that should be covered is the importance of firewalls. Windows Firewalls by themselves are not enough. Most times companies will provide a purchased firewall on company-supplied laptops and computers but personal laptops that may utilize the company wireless network need to have a firewall on them. For small office environments as well as those who remotely access their workstation from home, it is always helpful to provide information on free firewall options like ZoneAlarm and Comodo as well as relatively inexpensive firewall options like McAfee and Norton. The free firewalls are more for the personal user, though and not for commercial use. It may also be a benefit to the training to compare the price of a laptop to the price of a breach.

1.5.2.7 Password Security

The password security section should include what constitutes a strong, secure password or passphrase, with an emphasis on passphrases since they are harder to guess and to crack. This section should also outline the minimum password requirements of the organization.

Sharing passwords as well as leaving them out where anyone but the user could access them should be strongly discouraged. Making this part of organization-wide policy could be very helpful in this arena. If this is

incorporated into policy, this should be addressed in the training. Users need to be aware a policy is in place and general “rules of thumb” to make sure these policies are followed. Statistics could also be a good supplement. For example, a delegated individual could go around to all of the offices and see if they can uncover any unsecured passwords. They could even take this a step further and see how many computers are left on as well as without password-protected screensavers. No specific individuals would be singled out; just a number of instances out of the total number of computers would suffice.

Helpful hints and rules of thumb should also be a part of this section. For example, passwords should not contain the username or any part of the user’s full name. Passwords also should not be based on personal information such as a spouse name, favourite team, or pet. Another important point is to stress that the default password given to users should always be changed immediately. Instructions on how to change passwords should also be included.

To round out the password security section, it can be very beneficial to define what constitutes a poor choice of password as well as a listing of the most common passwords used.

1.5.2.8 Phishing

When discussing phishing, the term as well as the purpose should always be defined. Examples are key to this portion of security awareness training. Things to avoid (e.g. clicking on links provided in e-mail, submitting banking and password information via email, etc.) should be highly emphasized so people know what to look for. It could also be beneficial to have users take a Phishing IQ Test. This way the bits and pieces that can identify a phishing e-mail can be explained and displayed. Another item that should be addressed is how to actually fight phishing attacks. A couple of web sites actually encourage the reporting and tracking of phishing web sites and e-mails: PhishTank (www.phishtank.com) and The Anti- Abuse Project (www.antiabuse.org), which address these issues.

1.5.2.9 Hoaxes

Hoaxes should be addressed in the training because a lot of time and resources can be spent reading and forwarding hoax emails. The types of hoaxes as well as examples should be the meat of this section. Using familiar hoaxes is the

best option so it will be easier to grasp. It could also be beneficial to compare hoaxes to viruses in that they are spread by continually forwarding them. The dangers of hoaxes should also be addressed because some hoaxes warn of a virus and tell users to delete valid and sometimes important system files.

Preventing the spread of hoaxes should also be covered. Hoaxes can be prevented by checking a number of hoax sites on the Web and following a few rules of thumb. It is important to point out that if something sounds too good to be true, it probably is and if something seems suspicious it can be checked on one of the hoax sites

1.5.2.10 Malware

When addressing malware, it should always be defined and then broken down into its categories: viruses, worms, Trojans, spyware, and adware. After each category is broken down, address how they end up on systems.

1.5.2.11 Viruses

Start out by outlining what makes a virus a virus. It is important for users to be able to identify a potential virus when they see one or to identify characteristics of a virus that has already infiltrated the user's system. What a virus is capable of is also something that should supplement the defining of what makes a virus what it is.

Defining what a virus is and how to identify one must be complemented with the important of antivirus software. Most organizations will have this installed on all organization-wide computers, but this might not be installed on laptops used by employees. Users also need to learn the importance of not only performing regular scans of their computers, but also of any file they download from a web site, e-mail, or thumb drive.

Another important tip to include is how vital it is to keep systems and applications up-to-date. Never assume that a system or application is always going to update itself. Users should proactively see if the systems and applications they are using need updated.

Finally, it is important to let users know what to do if their system does become infected. Make sure not to incite a sense of panic that would steer employees toward hiding the infection until it has gotten out of control or their machine is

beyond repair. The main procedure to address is what to do if and when a virus infects a work machine, since it would differ considerably to what to do at home.

When your work machine becomes infected, do not do anything to the computer aside from performing a scan with the anti-virus software on the machine. Phone the I.T. Department of your business to come evaluate your machine and hopefully get rid of the virus.

If your machine at home (especially if you work from home) becomes infected, it is important to follow the following steps outlined on Viruslist.com:

- Do not panic
- Disconnect from the Internet and any Local Area Network it may be connected to.
- If computer cannot boot, try starting in Safe Mode or boot from the Windows boot disk.
- Back up any important data you cannot afford to lose to an external drive (scan the file with your anti-virus software first) (floppy, CD, jump drive, etc).
- If you do not have anti-virus software installed (which SHOULD not be the case), install it and then update it.
- Perform a full scan of your system.

1.5.2.12 Worms

The worms section can be handled much the same way the virus section is handled: Definition, how to spot, what it is capable of, how to prevent, what to do if one invades the system.

1.5.2.13 Trojans

Like the previous 2 sections, the Trojans portion should define what they are, what they can do, what can be done to prevent them, and what to do in the event of one making it onto the system. One item that should be emphasized is that Trojans are different from viruses and why they are two different things.

1.5.2.14 Spyware and Adware

Again, spyware and adware should be defined, what they can do should be outlined, prevention tips and tricks, and then what to do if it is found on the

system. Spyware and adware identification and removal programs should also be addressed, most of which are free (e.g. Ad Aware, Spy Sweeper, etc).

1.6. LET US SUM UP

- Security Controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.
- All security systems rely on a set of measures employed to control access, verify identity and protect disclosure of sensitive information.
- The control environment sets the tone of an organization, influencing the control consciousness of its people.
- Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style.
- Controlling physical access to machines and network attach points is perhaps more critical than any other aspect of security.
- Besides the basic physical security of a site, the next most important aspect is controlling digital access into and out of the organization's network.
- Partitioning the boundary between the outside Internet and the internal intranet is a critical security piece.
- A firewall is a mechanism by which a controlled barrier is used to control network traffic into and out of an organizational intranet.
- The most basic protection a firewall provides is the ability to block network traffic to certain destinations.
- Authentication or identification is the first step in any access solution.

1.7. CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. Controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an__.
2. _____are truly the weakest link in any security schema.
3. Organizations of any size should have a set of documented___, _____and_____.

4. _____ controls are intended to prevent an incident from occurring.
5. _____controls define the human factors of security.
6. _____are basically application specific routers.
7. _____ is the process of identifying the user to verify whether he/she is what he/she claims to be.
8. _____is known as third factor authentication.

Answers:

1. Asset
2. People
3. Resources, assets and systems
4. Preventive
5. Administrative
6. Firewalls
7. Authentication
8. Biometrics

1.8. ASSIGNMENTS

1. What are security controls?
2. What is threat? What are the possible sources of threats?
3. What are Detective Controls? Explain.
4. What are the three distinct master categories into which Computer security is categorized?
5. What is a firewall?
6. What are stateful inspection techniques?
7. What is demilitarized zone in a network?
8. What is access control? Why access controls are required?
9. What are the different access control models?
10. What is access control framework?
11. Why training and awareness is an import aspect of security controls?

Unit 2: Security Control Design 2

Unit Structure

2.1 LEARNING OBJECTIVES

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

- Understand technical security controls
- Know preventive controls
- Protect your system from malicious attacks
- Understand Networks and Communication
- Know the concept of cloud computing

2.2 INTRODUCTION

Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset. To help review or design security controls, they can be classified by several criteria. The salient criteria are listed below:

a. Categorizing according to the time that they act, relative to a security incident.
   i. **Preventive controls** are intended to prevent an incident from occurring e.g. by locking out unauthorized intruders.
   ii. **Detective controls** are intended to identify and characterize an incident in progress
   e.g. by sounding the intruder alarm and alerting the security guards or police.
   iii. **Corrective controls** are intended to limit the extent of any damage caused by the incident e.g. by recovering the organization to normal working status as efficiently as possible.

b. Security controls can also be categorized according to their nature.
   i. **Physical controls e.g. fences, doors, locks and fire extinguishers**

ii. **Procedural controls e.g. incident response processes, management oversight, security awareness and training**

iii. **Technical controls e.g. user authentication (login) and logical access controls, antivirus software, firewalls**

iv. **Legal and regulatory or compliance controls e.g. privacy laws, policies and clauses**

In other words Security controls are technical or administrative safeguards to minimize loss or unavailability due to threats acting on their matching vulnerability, i.e., security risk. However, this unit restricts our scope to Technical Security Controls.

2.3 TECHNICAL SECURITY CONTROL

Technical security involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices. Technical controls are also referred to as logical controls.

2.3.1 Preventive Technical Controls

Preventive technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources. Examples of these controls include:

- Access control software.
- Antivirus software.
- Library control systems.
- Passwords.
- Smart cards.
- Encryption.
- Dial-up access control and callback systems.

2.3.1.1 Access Control Software

The purpose of access control software is to control sharing of data and programs between users. In many computer systems, access to data and programs is implemented by access control lists that designate which users are allowed access. Access control software provides the ability to control access to the system by

establishing that only registered users with an authorized log-on ID and password can gain access to the computer system. After access to the system has been granted, the next step is to control access to the data and programs residing in the system. The data or program owner can establish rules that designate who is authorized to use the data or program.

2.3.1.2 Antivirus Software

Viruses have reached epidemic proportions throughout the microcomputing world and can cause processing disruptions and loss of data as well as significant loss of productivity while clean-up is conducted. In addition, new viruses are emerging at an ever-increasing rate — currently about one every 48 hours. It is recommended that antivirus software be installed on all microcomputers to detect, identify, isolate, and eradicate viruses. This software must be updated frequently to help fight new viruses. In addition, to help ensure that viruses are intercepted as early as possible, antivirus software should be kept active on a system, not used intermittently at the discretion of users.

2.3.1.3 Library Control Systems

These systems require that all changes to production programs be implemented by library control personnel instead of the programmers who created the changes. This practice ensures separation of duties, which helps prevent unauthorized changes to production programs.

2.3.1.4 Passwords

Passwords are used to verify that the user of an ID is the owner of the ID. The ID-password combination is unique to each user and therefore provides a means of holding users accountable for their activity on the system. Fixed passwords that are used for a defined period of time are often easy for hackers to compromise; therefore, great care must be exercised to ensure that these passwords do not appear in any dictionary. Fixed passwords are often used to control access to specific data bases. In this use, however, all persons who have authorized access to the data base use the same password; therefore, no accountability can be achieved. Currently, dynamic or one-time passwords, which are different for each log-on, are preferred over fixed passwords. Dynamic passwords are created by a token that is programmed to generate passwords randomly.

2.3.1.5 Smart Cards

Smart cards are usually about the size of a credit card and contain a chip with logic functions and information that can be read at a remote terminal to identify a specific user's privileges. Smart cards now carry pre-recorded, usually encrypted access control information that is compared with data that the user provides (e.g., a personal ID number or biometric data) to verify authorization to access the computer or network.

2.3.1.6 Encryption

Encryption is defined as the transformation of plaintext (i.e., readable data) into cipher text (i.e., unreadable data) by cryptographic techniques. Encryption is currently considered to be the only sure way of protecting data from disclosure during network transmissions. Encryption can be implemented with either hardware or software. Software-based encryption is the least expensive method and is suitable for applications involving low-volume transmissions; the use of software for large volumes of data results in an unacceptable increase in processing costs. Because there is no overhead associated with hardware encryption, this method is preferred when large volumes of data are involved.

2.3.1.7 Dial-Up Access Control and Callback Systems

Dial-up access to a computer system increases the risk of intrusion by hackers. In networks that contain personal computers or are connected to other networks, it is difficult to determine whether dial-up access is available or not because of the ease with which a modem can be added to a personal computer to turn it into a dial-up access point. Known dial-up access points should be controlled so that only authorized dial-up users can get through.

Currently, the best dial-up access controls use a microcomputer to intercept calls, verify the identity of the caller (using a dynamic password mechanism), and switch the user to authorized computing resources as requested. Previously, call-back systems intercepted dial- up callers, verified their authorization and called them back at their registered number, which at first proved effective; however, sophisticated hackers have learned how to defeat this control using call-forwarding techniques.

2.3.2 Detective Technical Controls

Detective technical controls warn personnel of violations or attempted violations of preventive technical controls. Examples of these include audit trails and intrusion detection expert systems, which are discussed in the following sections.

2.3.2.1 Audit Trails

An audit trail is a record of system activities that enables the reconstruction and examination of the sequence of events of a transaction, from its inception to output of final results. Violation reports present significant, security-oriented events that may indicate either actual or attempted policy transgressions reflected in the audit trail. Violation reports should be frequently and regularly reviewed by security officers and data base owners to identify and investigate successful or unsuccessful unauthorized accesses.

2.3.2.2 Intrusion Detection Systems

These expert systems track users (on the basis of their personal profiles) while they are using the system to determine whether their current activities are consistent with an established norm. If not, the user's session can be terminated or a security officer can be called to investigate. Intrusion detection can be especially effective in cases in which intruders are pretending to be authorized users or when authorized users are involved in unauthorized activities.

2.3.3 Corrective Technical Controls

Corrective controls exist to mitigate or lessen the effects of the threat being manifested. Examples of these include OS upgrades, Backup Data restoral and Vulnerability Mitigation which are discussed in the following sections.

2.3.3.1 OS Upgrade

Keep any and all original software media from which to restore the system. The latest upgrades of operating system should be maintained for system integrity.

2.3.3.2 Backup Data restoral

A good backup methodology should be in place to back up data. Commercial third party products may be used for the same. A back up will allow an organisation to restore critical data once a system has been rebuilt.

2.3.3.3 Vulnerability Mitigation

To mitigate the damage caused due to the vulnerability in the security system, the periodic testing of the backups for data integrity of the archived data.

2.4 PROTECTION FROM MALICIOUS ATTACKS

Although the technology behind the development of protection methods continues to improve in leaps and bounds, the threats against computers and the data, they contain, still remain. Keeping your defensive mechanism regularly updated is a critical aspect of your online security. Always keep in mind that hackers don't stick to the same threat tactics. They are also constantly looking for ways to bypass and counter the protective programs that people install in their computers. Whatever operating system you use, always see to it that you have at least two anti-virus software programs installed. The logic is simple - if the first line of defense didn't catch and contain the threat then the second program should do the trick. In fact, a lot of people make use of more than two security programs to protect their computers and data from malicious attacks.

In trying to find the best protection for your computer, there are several factors that you need to consider. For instance, what kind of data do you store in your computer? And what's the scope of this data? We need to understand that individuals with malicious intent usually make use of different types of attacks when sabotaging different types of data. Consequently, the methodology to be chosen should have the capability to protect whatever type of data you store in your computer. Fortunately, there's no shortage of software companies that focus on developing security programs. These defense systems are also constantly updated to ensure that they can hinder new threats.

Here are some practical tips on how you can efficiently prevent malicious code from wreaking havoc to your computer data.

a. Choose reliable anti-virus programs
b. Install real-time anti-spyware protection
c. Keep anti-malware applications current
d. Disable auto-run
e. Perform daily scans

f. Block suspicious files sent to your organization via email

g. Surf smart

h. Use a hardware-based firewall

i. Deploy DNS protection

Discussing each of the methods we can be more aware of the attacks and the mitigating techniques that can be adopted for the safety of our systems.

1 **Choose reliable anti-virus programs:** Many computer users believe free antivirus applications, such as those included with an Internet service provider's bundled service offering, are sufficient to protect a computer from virus or spyware infection. However, such free anti-malware programs typically don't provide adequate protection from the ever-growing list of threats. Instead, all users should install professional, business-grade antivirus software on their PCs. Pro-grade antivirus programs update more frequently throughout the day (thereby providing timely protection against fast-emerging vulnerabilities), protect against a wider range of threats (such as rootkits), and enable additional protective features (such as custom scans).

2 **Install real-time anti-spyware protection:** Many computer users mistakenly believe that a single antivirus program with integrated spyware protection provides sufficient safeguards from adware and spyware. Others think free anti-spyware applications, combined with an antivirus utility, deliver capable protection from the skyrocketing number of spyware threats. Unfortunately, that's just not the case. Most free anti- spyware programs do not provide real-time, or active, protection from adware, Trojan, and other spyware infections. While many free programs can detect spyware threats once they've infected a system, typically professional (or fully paid and licensed) anti- spyware programs are required to prevent infections and fully remove those infections already present.

3 **Keep anti-malware applications current:** Antivirus and anti-spyware programs require regular signature and database updates. Without these critical updates, anti- malware programs are unable to protect systems from the latest threats. Statistics reveal that a lot of serious computer threats are secretive and fast-moving. Many of these infections are short-lived, but

they're estimated to infect as many as 100,000 to 300,000 new Web sites a day. Computer users must keep their antivirus and anti- spyware applications up to date. All users must take measures to prevent license expiration, thereby ensuring that their anti-malware programs stay current and continue providing protection against the most recent threats.

4 **Perform daily scans:** Occasionally, virus and spyware threats escape a system's active protective engines and infect a system. The sheer number and volume of potential and new threats make it inevitable that particularly inventive infections will outsmart security software. In other cases, users may inadvertently instruct anti-malware software to allow a virus or spyware program to run. Regardless of the infection source, enabling complete, daily scans of a system's entire hard drive adds another layer of protection. These daily scans can be invaluable in detecting, isolating, and removing infections that initially escape security software's attention.

5 **Disable auto run:** Many viruses work by attaching themselves to a drive and automatically installing themselves on any other media connected to the system. As a result, connecting any network drives, external hard disks, or even thumb drives to a system can result in the automatic propagation of such threats. Computer users can disable the autorun feature by following the providers recommendations, which differ by operating system.

6 **Block suspicious files sent to your organization via email:** It's a mantra most users have heard repeatedly: Don't click on email links or attachments. Yet users frequently fail to heed the warning. Whether distracted, trustful of friends or colleagues they know, or simply fooled by a crafty email message, many users forget to be wary of links and attachments included within email messages, regardless of the source. Simply clicking on an email link or attachment can, within minutes, corrupt Windows, infect other machines, and destroy critical data. Users should never click on email attachments without at least first scanning them for viruses using a business- class anti-malware application. As for clicking on links, users should access Web sites by opening a browser and manually navigating to the sites in question.

7 **Surf smart:** Many business-class anti-malware applications include browser

plug-ins that help protect against drive-by infections, phishing attacks (in which pages purport to serve one function when in fact they try to steal personal, financial, or other sensitive information), and similar exploits. Still others provide "link protection," in which Web links are checked against databases of known-bad pages. Whenever possible, these preventive features should be deployed and enabled. Unless the plug- ins interferes with normal Web browsing, users should leave them enabled. The same is true for automatic pop-up blockers, included in browser toolbars. Regardless, users should never enter user account, personal, financial, or other sensitive information on any Web page at which they haven't manually arrived. They should instead open a Web browser, enter the address of the page they need to reach, and enter their information that way, instead of clicking on a hyperlink and assuming the link has directed them to the proper URL. Hyperlinks contained within an e-mail message often redirect users to fraudulent, fake, or unauthorized Web sites. By entering Web addresses manually, users can help ensure that they arrive at the actual page they intend which is also not fool proof.

8 **Use a hardware-based firewall:** Technology professionals and others argue the benefits of software- versus hardware-based firewalls. Often, users encounter trouble trying to share printers, access network resources, and perform other tasks when deploying third-party software-based firewalls. As a result, users in many cases simply disable firewalls altogether. But a reliable firewall is indispensable, as it protects computers from a wide variety of exploits, malicious network traffic, viruses, worms, and other vulnerabilities. Unfortunately, by itself, the software-based firewall included with operating system isn't sufficient to protect systems from the myriad robotic attacks affecting all Internet-connected systems. For this reason, all systems connected to the Internet should be secured behind a capable hardware-based firewall.

9 **Deploy DNS protection:** Internet access introduces a wide variety of security risks. Among the most disconcerting may be drive-by infections, in which users only need to visit a compromised Web page to infect their own PCs (and potentially begin infecting those of customers, colleagues, and

other staff). Another worry is Web sites that distribute infected programs, applications, and Trojan files. Still another threat exists in the form of poisoned DNS attacks, whereby a compromised DNS server directs you to an unauthorized Web server. These compromised DNS servers are typically your ISP's systems. Users can protect themselves from all these threats by changing the way their computers process DNS services. While a computer professional may be required to implement the switch, OpenDNS offers free DNS services to protect users against common phishing, spyware, and other Web-based hazards.

2.5 NETWORKS AND COMMUNICATION

Data refers to the raw facts that are collected while information refers to processed data that enables us to take decisions e.g. When result of a particular test is declared it contains data of all students, when you find the marks you have scored you have the information that lets you know whether you have passed or failed. The word data refers to any information which is presented in a form that is agreed and accepted upon is creators and users.

2.5.1 Data Communication

Data Communication is a process of exchanging data or information In case of computer networks this exchange is done between two devices over a transmission medium. This process involves a communication system which is made up of hardware and software. The hardware part involves the sender and receiver devices and the intermediate devices through which the data passes. The software part involves certain rules which specify what is to be communicated, how it is to be communicated and when. It is also called as a Protocol. The following sections describe the fundamental characteristics that are important for the effective working of data communication process and are followed by the components that make up a data communications system.

2.5.2 Characteristics of Data Communication

The effectiveness of any data communications system depends upon the following four fundamental characteristics:-

a. **Delivery:** The data should be delivered to the correct destination and correct user.

b. **Accuracy:** The communication system should deliver the data accurately, without introducing any errors. The data may get corrupted during transmission affecting the accuracy of the delivered data.

c. **Timeliness:** Audio and Video data has to be delivered in a timely manner without any delay; such a data delivery is called real time transmission of data.

d. **Jitter:** It is the variation in the packet arrival time. Uneven Jitter may affect the timeliness of data being transmitted.

2.5.3 Components of Data Communication

A Data Communication system has five components as shown in the diagram below:-

a. **Message:** Message is the information to be communicated by the sender to the receiver.
b. **Sender:** The sender is any device that is capable of sending the data (message).
c. **Receiver:** The receiver is a device that the sender wants to communicate the data (message).
d. **Transmission Medium:** It is the path by which the message travels from sender to receiver. It can be wired or wireless and many subtypes in both.
e. **Protocol:** It is an agreed upon set or rules used by the sender and receiver to communicate data. A protocol is a set of rules that governs data communication without which the communicating entities are like two persons trying to talk to each other in a different language without know the other language.

2.5.4 Data Representation

Data is collection of raw facts which is processed to deduce information. There may be different forms in which data may be represented. Some of the forms of data used in communications are as follows:-

a. **Text:** Text includes combination of alphabets in small case as well as upper case. It is stored as a pattern of bits. Prevalent encoding system: ASCII, Unicode etc.

b. **Numbers:** Numbers include combination of digits from 0 to 9. It is stored as a pattern of bits. Prevalent encoding system: ASCII, Unicode etc.
c. **Images:** In computers images are digitally stored. A Pixel is the smallest element of an image. To put it in simple terms, a picture or image is a matrix of pixel elements. The pixels are represented in the form of bits. Depending upon the type of image (black n white or color) each pixel would require different number of bits to represent the value of a pixel. The size of an image depends upon the number of pixels (also called resolution) and the bit pattern used to indicate the value of each pixel. Commonly used Image formats: jpg, png, bmp, etc.
d. **Audio Data:** Audio Data can also be in the form of sound which can be recorded and broadcasted. Example: What we hear on the radio is a source of data or information. Audio data is continuous, not discrete. Commonly used audio formats: mp3 etc.
e. **Video:** Video refers to broadcasting of data in form of picture or movie. Commonly used audio formats: mp4, mkv etc.

2.5.5 Data Flow

Devices on a network communicate with each other by sending and receiving data. The data can flow between the two devices in the following ways.

a. Simplex
b. Half Duplex
c. Full Duplex

2.5.5.1 Simplex

In Simplex, communication is unidirectional only one of the devices sends the data and the other one only receives the data. Example: a CPU sends data while a monitor only receives data.

2.5.5.2 Half Duplex

In half duplex both the stations can transmit as well as receive but not at the same time. When one device is sending other can only receive and vice- versa Example: A walkie-talkie.

2.5.5.3 Full Duplex

In Full duplex mode, both stations can transmit and receive at the same time.

Example: mobile phones

2.6 COMPUTER NETWORK

A computer network can be defined as a collection of nodes which is used for data communications. A node can be any device capable of transmitting or receiving data. The communicating nodes have to be connected by communication links. A Compute network should ensure:

a. Reliability of the data communication process
b. Security of the data
c. Performance by achieving higher throughput and smaller delay times

2.6.1 Categories of Network

Networks are categorized on the basis of their size. The three basic categories of computer networks are:-

a. **Local Area Network (LAN)** is usually limited to a few kilometers of area. It may be privately owned and could be a network inside an office on one of the floor of a building or a LAN could be a network consisting of the computers in an entire building.
b. **Wide Area Network (WAN)** is made of all the networks in a (geographically) large area. The network in an entire state could be termed as a WAN.
c. **Metropolitan Area Network (MAN)** is of size between LAN & WAN. It is larger than LAN but smaller than WAN. It may comprise the entire network in a city.

2.6.2 Protocol

A Protocol is one of the components of a data communications system which specifies the rules for communication between two or more parties. Without protocol communication cannot occur. The sending device cannot just send the data and expect the receiving device to receive and further interpret it correctly. When the sender sends a message it may consist of text, number, images, etc. which are converted into bits and grouped into blocks to be transmitted and often certain additional information called control information is also added to help the receiver interpret the data. For successful communication to occur, the sender and receiver must agree upon certain rules called protocol. A Protocol is

defined as a set of rules that governs data communications. A protocol defines what is to be communicated, how it is to be communicated and when it is to be communicated.

2.6.2.1 Elements of a Protocol

There are three key elements of a protocol:

a. **Syntax**: It means the structure or format of the data. It is the arrangement of data in a particular order.
b. **Semantics**: It tells the meaning of each section of bits and indicates the interpretation of each section. It also tells what action/decision is to be taken based on the interpretation.
c. **Timing:** It tells the sender about the readiness of the receiver to receive the data and also intimates the sender at what rate the data should be sent to the receiver to avoid overwhelming the receiver.

2.6.3 External Services

Any service that is not sourced from a particular organisations network may be termed as an External Service. Such services are provided by an **external service provider** (ESP). Examples of this are: Consumer email **services** such as Yahoo, live.com, or Google mail etc.

2.6.3.1 Policy on Use of External Services

Sensitive data should neither be stored on nor sent to, from or through any external service provider (ESP) unless one of the two following conditions has been met:

The organization has a contract with the ESP that specifically addresses such use of sensitive data.

Encryption methods that meet the requirements of the organization are implemented to protect this data.

The idea of cloud computing is based on a very fundamental principal of „reusability of IT capabilities'. The difference that cloud computing brings compared to traditional concepts of “grid computing”, “distributed computing”, “utility computing”, or “autonomic computing” is to broaden horizons across organizational boundaries.

2.7 CLOUD COMPUTING

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data centre from a capital-intensive set up to a variable priced environment.

The idea of cloud computing is based on a very fundamental principal of „reusability of IT capabilities'. The difference that cloud computing brings compared to traditional concepts of “grid computing”, “distributed computing”, “utility computing”, or “autonomic computing” is to broaden horizons across organizational boundaries.

2.7.1 Cloud Computing Models

Cloud Providers offer services that can be grouped into three categories viz.

a. **Software as a Service (SaaS):** In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customers‟ side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc.

b. **Platform as a Service (Paas):** Here, a layer of software, or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider’s infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE, Ruby etc. Google‟s App Engine, Force.com, etc are some of the popular PaaS examples.

c. **Infrastructure as a Service (Iaas):** IaaS provides basic storage and computing capabilities as standardized services over the network. Servers,

storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, GoGrid, 3 Tera, etc.

2.7.2 Understanding Public and Private Clouds

Enterprises can choose to deploy applications on Public, Private or Hybrid clouds. Cloud Integrators can play a vital part in determining the right cloud path for each organization.

2.7.2.1 Public Cloud

Public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, “Pay-as-you-go” model. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider. One of the advantages of a Public cloud is that they may be larger than an enterprises cloud, thus providing the ability to scale seamlessly, on demand.

2.7.2.2 Private Cloud

Private clouds are built exclusively for a single enterprise. They aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variations to a private cloud: - On-premise Private Cloud: On-premise private clouds, also known as internal clouds are hosted within one’s own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications which require complete control and configurability of the infrastructure and security. - Externally hosted Private Cloud: This type of private cloud is hosted externally with a cloud provider, where the provider facilitates an exclusive cloud environment with full guarantee of privacy. This is best suited for enterprises that don’t prefer a public cloud due to sharing of physical resources.

2.7.2.3 Hybrid Cloud

Hybrid Clouds combine both public and private cloud models. With a Hybrid Cloud, service providers can utilize 3rd party Cloud Providers in a full or partial

manner thus increasing the flexibility of computing. The Hybrid cloud environment is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

2.7.3 Cloud Computing Benefits

Enterprises would need to align their applications, so as to exploit the architecture models that Cloud Computing offers. Some of the typical benefits are listed below:

a. **Reduced Cost:** There are a number of reasons to attribute Cloud technology with lower costs. The billing model is pay as per usage; the infrastructure is not purchased thus lowering maintenance. Initial expense and recurring expenses are much lower than traditional computing.

b. **Increased Storage**: With the massive Infrastructure that is offered by Cloud providers today, storage & maintenance of large volumes of data is a reality. Sudden workload spikes are also managed effectively & efficiently, since the cloud can scale dynamically.

c. **Flexibility**: This is an extremely important characteristic. With enterprises having to adapt, even more rapidly, to changing business conditions, speed to deliver is critical. Cloud computing stresses on getting applications to market very quickly, by using the most appropriate building blocks necessary for deployment.

2.7.4 Cloud Computing Challenges

Despite its growing influence, concerns regarding cloud computing still remain. In our opinion, the benefits outweigh the drawbacks and the model is worth exploring. Some common challenges are:

a. **Data Protection**: Data Security is a crucial element that warrants scrutiny. Enterprises are reluctant to buy an assurance of business data security from vendors. They fear losing data to competition and the data confidentiality of consumers. In many instances, the actual storage location is not disclosed, adding onto the security concerns of enterprises. In the existing models, firewalls across data centres (owned by enterprises) protect this sensitive information. In the cloud model, Service providers are responsible for maintaining data security and enterprises would have to rely on them.

b. **Data Recovery and Availability**: All business applications have Service level agreements that are stringently followed. Operational teams play a key role in management of service level agreements and runtime governance of applications. In production environments, operational teams support.

   i. Appropriate clustering and Fail over
   ii. Data Replication
   iii. System monitoring (Transactions monitoring, logs monitoring and others)
   iv. Maintenance (Runtime Governance)
   v. Disaster recovery
   vi. Capacity and performance management

If, any of the above mentioned services is under-served by a cloud provider, the damage & impact could be severe.

c. **Management Capabilities**: Despite there being multiple cloud providers, the management of platform and infrastructure is still in its infancy. Features like „Auto- scaling" for example, are a crucial requirement for many enterprises. There is huge potential to improve on the scalability and load balancing features provided today.

d. **Regulatory and Compliance Restrictions**: In some of the European countries, Government regulations do not allow customer's personal information and other sensitive information to be physically located outside the state or country. In order to meet such requirements, cloud providers need to setup a data center or a storage site exclusively within the country to comply with regulations. Having such an infrastructure may not always be feasible and is a big challenge for cloud providers.

With cloud computing, the action moves to the interface — that is, to the interface between service suppliers and multiple groups of service consumers. Cloud services will demand expertise in distributed services, procurement, risk assessment and service negotiation — areas that many enterprises are only modestly equipped to handle.

2.7.5 IT Infrastructure

IT infrastructure refers to the composite hardware, software, network resources

and services required for the existence, operation and management of an enterprise IT environment. It allows an organization to deliver IT solutions and services to its employees, partners and/or customers and is usually internal to an organization and deployed within owned facilities. In other words, IT infrastructure consists of all components that somehow play a role in overall IT and IT-enabled operations. It can be used for internal business operations or developing customer IT or business solutions. Typically, a standard IT infrastructure consists of the following components:

a. **Hardware**: Servers, computers, data centres, switches, hubs and routers, etc.
b. **Software:** Enterprise resource planning (ERP), customer relationship management (CRM), productivity applications and more.
c. **Network:** Network enablement, Internet connectivity, firewall and security.
d. **Meatware:** Human users, such as network administrators (NA), developers, designers and generic end users with access to any IT appliance or service are also part of an IT infrastructure, specifically with the advent of user-centric IT service development.

2.8 LET US SUM UP

1 Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

2 Technical security involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices.

3 The purpose of access control software is to control sharing of data and programs between users.

4 After access to the system has been granted, the next step is to control access to the data and programs residing in the system.

5 Passwords are used to verify that the user of an ID is the owner of the ID.

6 Dial-up access to a computer system increases the risk of intrusion by hackers.

7 In networks that contain personal computers or are connected to other

networks, it is difficult to determine whether dial-up access is available or not because of the ease with which a modem can be added to a personal computer to turn it into a dial-up access point.

8 An audit trail is a record of system activities that enables the reconstruction and examination of the sequence of events of a transaction, from its inception to output of final results.

9 Although the technology behind the development of protection methods continues to improve in leaps and bounds, the threats against computers and the data, they contain, still remain.

10 The word data refers to any information which is presented in a form that is agreed and accepted upon is creators and users.

11 Data Communication is a process of exchanging data or information In case of computer networks this exchange is done between two devices over a transmission medium.

12 IT infrastructure refers to the composite hardware, software, network resources and services required for the existence, operation and management of an enterprise IT environment.

2.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1 _____ help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

2 _____controls are technical or administrative safeguards to minimize loss or unavailability due to threats acting on their matching vulnerability.

3 Technical controls are also referred to as_____controls.

4 _____technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources.

5 In many computer systems, access to data and programs is implemented that designate which users are allowed access.

6 _____ control systems require that all changes to production programs be implemented by library control personnel instead of the programmers who created the changes.

7 _____are usually about the size of a credit card and contain a chip with logic functions and information that can be read at a remote terminal to

identify a specific user's privileges.

8 Currently, the best dial-up access controls use a _____ to intercept calls, verify the identity of the caller (using a dynamic password mechanism), and switch the user to authorized computing resources as requested.

9 _____ technical controls warn personnel of violations or attempted violations of preventive technical controls.

10 _____ reports should be frequently and regularly reviewed by security officers and data base owners to identify and investigate successful or unsuccessful unauthorized accesses.

11 _____ controls exist to mitigate or lessen the effects of the threat being manifested.

12 A computer__ can be defined as a collection of nodes which is used for data communications.

13 _____ is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage.

14 In_____ model, a complete application is offered to the customer, as a service on demand.

Answers:

1. Controls
2. Security
3. Logical
4. Preventive
5. By access control lists
6. Library
7. Smart cards
8. Microcomputer
9. Detective
10. Violation
11. Corrective
12. Network
13. Cloud computing
14. Software as a service

2.10 ASSIGNMENTS

1. What are security controls? What are the basic criteria based on which security controls are classified?
2. What are preventive security controls? Give examples.
3. What are smart cards? Why they are used?
4. What is encryption?
5. What is an audit trial?
6. What is an Intrusion Detection Systems?
7. What are the methods to safeguard your system from malicious attacks?
8. What is the difference between data and information? Explain with the help of an example.
9. What is data communication? What are its characteristics?
10. What is the difference between simplex, half duplex and full duplex communication?
11. What is a protocol? What are its elements?

Unit 3:Software Development Life Cycle (SDLC) 3

Unit Structure

3.1 LEARNING OBJECTIVES

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

- Know the basics of Software Development Lifecycle (SDLC)
- Know the various stages involved in the SDLC
- Study the various models of SDLC

3.2 INTRODUCTION

We will initially start by briefly studying the concept of Software Development Life Cycle (SDLC). SDLC is a process used by the industry to design, develop and test high quality software. The process of SDLC aims to produce high quality software that meets or exceeds customer experience and expectations while meeting the financial and time constraints. This is also known as the Software Development Process for which tasks are pre – defined in the Software Development Life Cycle (SDLC). ISO/IEC 12207 is the international standard for software lifecycle processes. It aims to be the standard that defines all the tasks required for developing and maintaining software.

3.3 SOFTWARE DEVELOPMENT LIFE CYCLE(SDLC)

3.3.1 Definition

SDLC is a process that an organisation follows for the development of a software project. It consists of a detailed plan describing how to develop, maintain, replace and alter or enhance specific software. The life cycle defines a methodology for improving the quality of software and the overall development process.

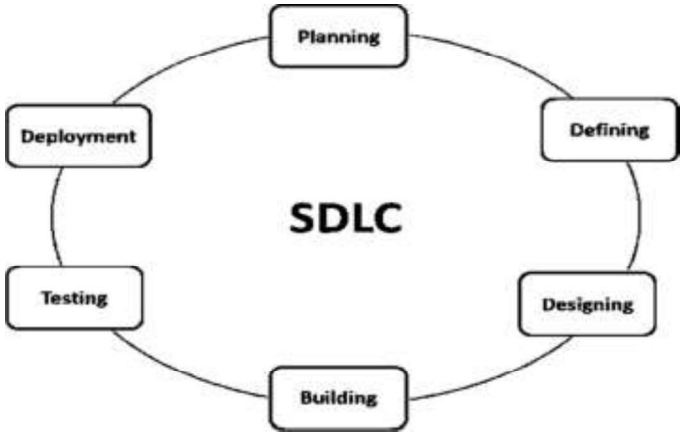


Figure 5: Stages of Software Development Life Cycle

3.3.2 Stages in SDLC

The various steps of Software Development Life Cycle are briefly described below:

1. **Stage 1: Planning and Requirement Analysis:** The most important and fundamental stage in SDLC is Planning, which may also be referred to as Requirement Analysis. It is performed by a team, generally having adequate seniority and experience, with inputs from the customer, the sales department, market surveys and domain experts in the industry. This information is then used to plan the basic project approach and to conduct product feasibility study in the operational, technical and economical areas. Planning for the quality assurance requirements and identification of the risks associated with the project is also done in the planning stage. The outcome of the technical feasibility study is to define the various technical approaches that can be followed to implement the project successfully with minimum risks.
2. **Stage 2: Defining Requirements:** After the requirement analysis, the next step is to clearly define and document the product requirements. This documentation is then discussed with and is approved after incorporation of suggestions/variations by the customer/analyst. This is done through SRS – Software Requirement Specification document which consists of all the product requirements to be designed and developed during the project life cycle.
3. **Stage 3: Designing the product architecture:** Software Requirement Specification (SRS) document forms the basis for best product architecture of the product to be developed. Based on the requirements specified in SRS, usually more than one design approach for the product architecture is proposed and documented in Detailed Design Document which may also be referred to as a DDS - Design Document Specification. This DDS is reviewed by all the important stakeholders and based on various parameters as risk assessment, product robustness, design modularity , budget and time constraints , the best design approach is selected for the product. A design approach clearly defines all the architectural modules of the product along with its communication and data flow representation with the external and third

party modules if any. The internal design of all the modules of the proposed architecture should be clearly defined with the minutest of the details in DDS.

4. **Stage 4: Building or Developing the Product:** During this stage of SDLC the actual development starts based on the DDS and the process for building of the product is initiated. The programming code is written as per DDS during this stage. If the designing is accomplished in a detailed and structured manner, error free code generation can be achieved within short time frames. Developers have to follow the coding guidelines defined by their organization and programming tools like compilers, interpreters, debuggers etc. are used to generate the code. Different high level programming languages such as C, C++, Pascal, Java, and PHP are used for coding. The programming language is chosen with respect to the type of software being developed.
5. **Stage 5: Testing the Product:** This stage is usually a subset of all the stages as in the modern SDLC models, the testing activities are mostly involved in all the stages of SDLC. However this stage refers to the testing only stage of the product where products defects are reported, tracked, fixed and retested, until the product reaches the quality standards defined in the SRS.
6. **Stage 6: Deployment in the Market and Maintenance:** After the product is tested and ready it is released formally deployed in the appropriate market based on the Business strategy of the organization. The product at this stage may be subjected to Site Acceptance Trials (SAT) in a limited segment and later, tested in the real business environment with the User testing the product in the real world scenario. Then based on the feedback, the product may be released as it is or with suggested enhancements in the targeting market segment. After the product is released in the market, its maintenance is done for the existing customer base.

3.4 SDLC MODELS

There are various software development life cycle models defined and designed which are followed during software development process. These models are also referred as "Software Development Process Models". Each process model follows a Series of steps unique to its type, in order to ensure success in

process of software development. Following are the most important and popular SDLC models followed in the industry:

- Waterfall Model
- Iterative Model
- Spiral Model
- V-Model
- Big Bang Model
- Agile Model
- Rapid Application Development Model
- Software Prototyping Model

In the further chapters we would consider the detailed description of the various SDLC Models.

3.5 WATERFALL MODEL

The waterfall model is a popular version of the systems development life cycle model for software engineering. It is often considered as the classic approach to the systems development life cycle. The waterfall model describes a development method that is linear and sequential. Waterfall development has distinct goals for each phase of development. In a waterfall model, each phase must be completed before the next phase can begin and there is no overlapping in the phases. Once a phase of development is completed, the development proceeds to the next phase and there is no turning back. Waterfall model is the earliest SDLC approach that was used for software development.

3.5.1 Waterfall Model Design

Waterfall approach was one of the earliest of SDLC Models to be used widely in Software Engineering and considering its linearity it ensured success of the project. In "The Waterfall" approach, the whole process of software development is divided into separate phases which neither overlap nor are retractable. In waterfall model the outcome of one phase acts as the input for the next phase sequentially.

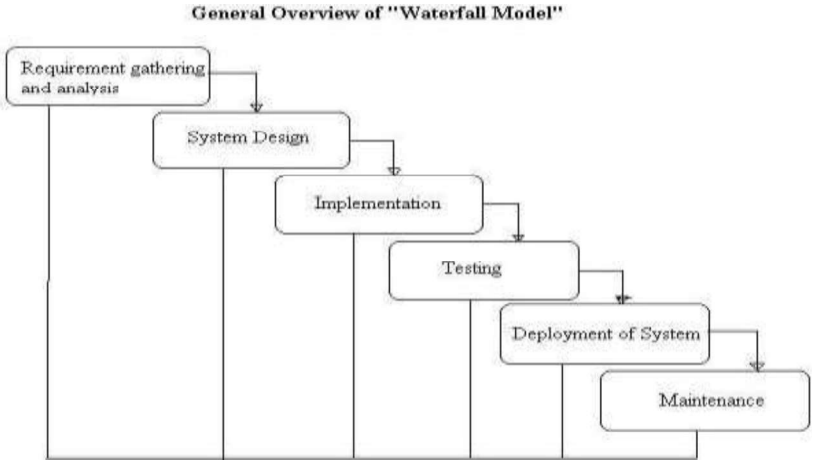


Figure 6 : Waterfall model

3.5.2 Stages of the Waterfall model

The various stages of the Waterfall model are:

1. **Requirement Gathering and analysis:** All possible requirements of the system to be developed are captured in this phase and documented in a Software Requirement Specification document. In order to understand the requirements, various brainstorming and walkthrough sessions are organized. During this stage the requirements feasibility test is also carried out to ensure that the requirements are testable.
2. **System Design:** The requirement specifications from first phase are studied in this phase and system design is prepared. System Design helps in specifying hardware and system requirements and also helps in defining overall system architecture.
3. **Implementation:** With inputs from system design, the system is first developed in small programs/codes called units, which are integrated in the next phase. Each unit is developed and tested for its functionality which is referred to as Unit Testing.
4. **Integration and Testing:** All the units developed in the implementation phase are integrated into a system after testing of each unit to ensure that it works as expected. The progress on testing is tracked through tools like traceability matrices etc. Post integration the entire system is tested for any faults and failures.

5. **Deployment of system:** Once the functional and non-functional testing is done, the product is deployed in the customer environment or released into the market and a sanity check is performed in the environment after the application is deployed to ensure the application does not break.
6. **Maintenance:** There are some issues which come up in the client environment. To fix those issues patches are released. Also to enhance the product some better versions are released. Maintenance is done to deliver these changes in the customer environment.

All these phases are cascaded to each other in which progress is seen as flowing steadily downwards like a waterfall through the phases. The next phase is started only after the defined set of goals are achieved for previous phase and it is signed off, so the name "Waterfall Model". In this model phases do not overlap.

3.5.3 Application

Every software developed is different and requires a suitable SDLC approach to be followed based on the internal and external factors. Some situations where the use of Waterfall model is most appropriate are:

a. Requirements are very well documented, clear and fixed.
b. Product definition is stable.
c. Technology is understood and is not dynamic.
d. There are no ambiguous requirements.
e. Ample resources with required expertise are available to support the product.
f. The project is short.

3.5.4 Advantages and Disadvantages of Waterfall Model

3.5.4.1 Advantages

The advantage of waterfall development is that it allows for departmentalization and control. A schedule can be set with deadlines for each stage of development and a product can proceed through the development process model phases one by one.

Development moves from concept, through design, implementation, testing, installation, troubleshooting, and ends up at operation and maintenance. Each

phase of development proceeds in strict order.

3.5.4.2 Disadvantages

The disadvantage of waterfall development is that it does not allow for much reflection or revision. Once an application is in the testing stage, it is very difficult to go back and change something that was not well-documented or thought upon in the concept stage.

3.6 ITERATIVE MODEL

In Iterative model, iterative process starts with a simple implementation of a small set of the software requirements and iteratively enhances the evolving versions until the complete system is implemented and ready to be deployed. An iterative life cycle model does not attempt to start with a full specification of requirements. Instead, development begins by specifying and implementing just part of the software, which is then reviewed in order to identify further requirements. This process is then repeated, producing a new version of the software at the end of each iteration of the model.

3.6.1 Iterative Model design

Iterative process starts with a simple implementation of a subset of the software requirements and iteratively enhances the evolving versions until the full system is implemented. At each iteration, design modifications are made and new functional capabilities are added. The basic idea behind this method is to develop a system through repeated cycles iterative and in smaller portions at a time incremental.

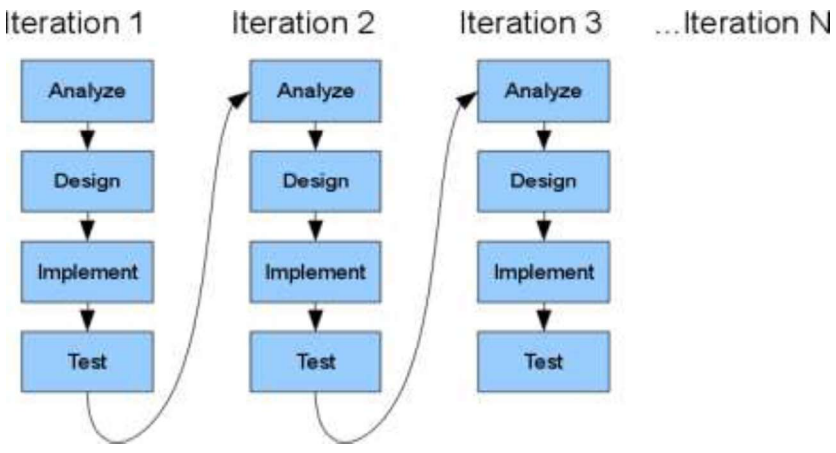


Figure 7: Iterative Model

Iterative and Incremental development is a combination of both iterative design

or iterative method and incremental build model for development. "During software development, more than one iteration of the software development cycle may be in progress at the same time." and "This process may be described as an "evolutionary acquisition" or "incremental build" approach.

In incremental model the whole requirement is divided into various builds. During each iteration, the development module goes through the requirements, design, implementation and testing phases. Each subsequent release of the module adds function to the previous release. The process continues till the complete system is ready as per the requirement.

The key to successful use of an iterative software development lifecycle is rigorous validation of requirements, and verification & testing of each version of the software against those requirements within each cycle of the model. As the software evolves through successive cycles, tests have to be repeated and extended to verify each version of the software.

3.6.2 Application

Like other SDLC models, Iterative and incremental development has some specific applications in the software industry. This model is most often used in the following scenarios:

a. Requirements of the complete system are clearly defined and understood.
b. Major requirements must be defined; however, some functionalities or requested enhancements may evolve with time.
c. There is a time to the market constraint.
d. A new technology is being used and is being learnt by the development team while working on the project.
e. Resources with needed skill set are not available and are planned to be used on contract basis for specific iterations.
f. There are some high risk features and goals which may change in the future.

3.6.3 Advantages and Disadvantages of Iterative Model

3.6.3.1 Advantages

The advantage of this model is that there is a working model of the system at a very early stage of development which makes it easier to find functional or design flaws. Finding issues at an early stage of development enables to take corrective measures in a limited budget.

3.6.3.2 Disadvantages

The disadvantage with this SDLC model is that it is applicable only to large and bulky software development projects. This is because it is hard to break a small software system into further small serviceable increments/modules.

3.7 SPIRAL MODEL

The spiral model combines the idea of iterative development with the systematic, controlled aspects of the waterfall model. The spiral model is a risk-driven process model generator for software projects. Based on the unique risk patterns of a given project, the spiral model guides a team to adopt elements of one or more process models, such as incremental, waterfall, or evolutionary prototyping.

Spiral model is a combination of iterative development process model and sequential linear development model i.e. waterfall model with very high emphasis on risk analysis. It allows for incremental releases of the product, or incremental refinement through each iteration around the spiral.

3.7.1 Spiral Model design

The spiral model has four distinct phases. A software project repeatedly passes through these phases in iterations called Spirals.

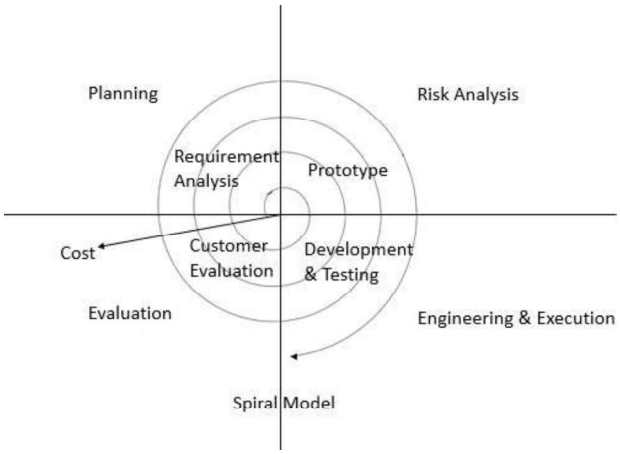


Figure 8: Spiral Model

1. **Planning (Determine Objectives):** This phase starts with gathering and analyzing the business requirements in the baseline spiral. In the subsequent spirals as the product matures, identification of system requirements, subsystem requirements and unit requirements are all done in this phase.
   This also includes understanding the system requirements by continuous communication between the customer and the system analyst. At the end of the spiral the product is deployed in the identified market.
2. **Design:** Design phase starts with the conceptual design in the baseline spiral and involves architectural design, logical design of modules, physical product design, which may be referred to as a prototype, and final design in the subsequent spirals.
3. **Construct or Build:** Construct phase refers to production of the actual software product at every spiral. In the baseline spiral when the product is just thought of and the design is being developed a Proof of Concept (POC) is developed in this phase to get customer feedback. Then in the subsequent spirals with higher clarity on requirements and design details a working model of the software called build is produced with a version number. These builds are sent to customer for feedback.
4. **Evaluation and Risk Analysis:** Risk Analysis includes identifying, estimating, and monitoring technical feasibility and management risks, such as schedule slippage and cost overrun. After testing the build, at the end of first iteration, the customer evaluates the software and provides feedback.

3.7.2 Application

Spiral Model is very widely used in the software industry as it is in sync with the natural development process of any product i.e. learning with maturity and also involves minimum risk for the customer as well as the development firms. Following are the typical uses of Spiral model:

a. When there is a budget constraint and risk evaluation is important.
b. For medium to high-risk projects.
c. Long-term project commitment because of potential changes to economic priorities as the requirements change with time.
d. Customer is not sure of their requirement which is usually the case.
e. Requirements are complex and need evaluation to get clarity.
f. New product line which is released in phases to get enough customer feedback.
g. Significant changes are expected in the product during the development cycle.

3.7.3 Advantages and Disadvantages of Spiral Model

3.7.3.1 Advantages

The advantage of spiral lifecycle model is that it allows for elements of the product to be added in when they become available or known. This assures that there is no conflict with previous requirements and design. This method is consistent with approaches that have multiple software builds and releases and allows for making an orderly transition to a maintenance activity. Another positive aspect is that the spiral model forces early user involvement in the system development effort.

3.7.3.2 Disadvantages

On the other side, it takes very strict management to complete such products and there is a risk of running the spiral in indefinite loop. So the discipline of change and the extent of taking change requests is very important to develop and deploy the product successfully.

3.8 V – MODEL

The V - model is SDLC model where execution of processes happens in a sequential manner in V shape. It is also known as Verification and Validation model. V - Model is an extension of the waterfall model and is based on association of a testing phase for each corresponding development stage. This means that for every single phase in the development cycle there is a directly associated testing phase. This is a highly disciplined model and next phase starts only after completion of the previous phase.

3.8.1 V- Model design

Under V-Model, the corresponding testing phase of the development phase is planned in parallel. So there are Verification phases on one side of the V and Validation phases on the other side (Please see Figure 5 below). Coding phase joins the two sides of the V-Model.

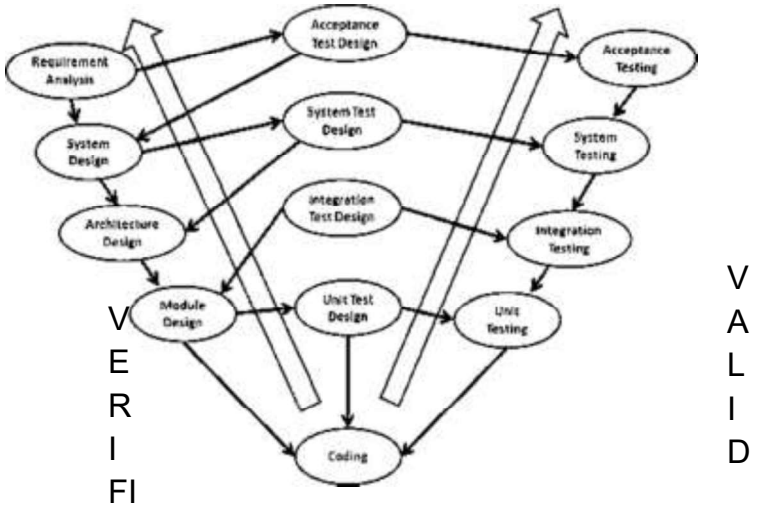


Figure 9:V

3.8.2 Verification Phases

Following are the Verification phases in V-Model:

1. **Business Requirement Analysis:** This is the first phase in the development cycle where the product requirements are understood from the customer perspective. This phase involves detailed communication with the customer to understand his expectations and exact requirement. This is a very important activity and need to be managed well, as most of the customers are not sure about what exactly they need. The acceptance test design planning is done at

this stage as business requirements can be used as an input for acceptance testing.

2. **System Design:** Once you have the clear and detailed product requirements, it's time to design the complete system. System design would comprise of understanding and detailing the complete hardware and communication setup for the product under development. System test plan is developed based on the system design. Doing this at an earlier stage leaves more time for actual test execution later.
3. **Architectural Design:** Architectural specifications are understood and designed in this phase. Usually more than one technical approach is proposed and based on the technical and financial feasibility the final decision is taken. System design is broken down further into modules taking up different functionality. This is also referred to as High Level Design (HLD). The data transfer and communication between the internal modules and with the other systems is clearly understood and defined in this stage. With this information, integration tests can be designed and documented during this stage.
4. **Module Design:** In this phase the detailed internal design for all the system modules is specified, referred to as Low Level Design (LLD). It is important that the design is compatible with the other modules in the system architecture and the other external systems. Unit tests are an essential part of any development process and helps eliminate the maximum faults and errors at a very early stage. Unit tests can be designed at this stage based on the internal module designs.

3.8.3 Coding Phase

The actual coding of the system modules designed in the design phase is taken up in the Coding phase. The best suitable programming language is decided based on the system and architectural requirements. The coding is performed based on the coding guidelines and standards. The code goes through numerous code reviews and is optimized for best performance before the final build is checked into the repository.

3.8.4 Validation Phases

Following are the Validation phases in V-Model:

1. **Unit Testing:** Unit tests designed in the module design phase are executed on the code during this validation phase. Unit testing is the testing at code level and helps eliminate bugs at an early stage, though all defects cannot be uncovered by unit testing.
2. **Integration Testing:** Integration testing is associated with the architectural design phase. Integration tests are performed to test the coexistence and communication of the internal modules within the system.
3. **System Testing:** System testing is directly associated with the System design phase. System tests check the entire system functionality and the communication of the system under development with external systems. Most of the software and hardware compatibility issues can be uncovered during system test execution.
4. **Acceptance Testing:** Acceptance testing is associated with the business requirement analysis phase and involves testing the product in user environment. Acceptance tests uncover the compatibility issues with the other systems available in the user environment. It also discovers the non-functional issues such as load and performance defects in the actual user environment.

3.8.5 Application

V-Model application is almost same as waterfall model, as both the models are of sequential type. Requirements have to be very clear before the project starts, because it is usually expensive to go back and make changes. This model is used in the medical development field, as it is strictly disciplined domain. Following are the suitable scenarios to use V-Model:

a. Requirements are well defined, clearly documented and fixed.
b. Product definition is stable.
c. Technology is not dynamic and is well understood by the project team.
d. There are no ambiguous or undefined requirements.
e. The project is short.

3.8.6 Advantages and Disadvantages of Software Prototyping V-Model

3.8.6.1 Advantage

The advantage of V-Model is that it's very easy to understand and apply. The simplicity of this model also makes it easier to manage.

3.8.6.2 Disadvantage

The disadvantage is that the model is not flexible to changes and just in case there is a requirement change, which is very common in today's dynamic world, it becomes very expensive to make the change.

3.9 BIG BANG MODEL

The Big Bang model is SDLC model where we do not follow any specific process. The development just starts with the required money and efforts as the input, and the output is the software developed which may or may not be as per customer requirement. Big Bang Model is SDLC model where there is no formal development followed and very little planning is required. Even the customer is not sure about what exactly he wants and the requirements are implemented on the fly without much analysis. Usually this model is followed for small projects where the development teams are very small.

3.9.1 Big Bang Model design and Application

Big bang model comprises of focusing all the possible resources in software development and coding, with very little or no planning. The requirements are understood and implemented as they come. Any changes required may or may not need to revamp the complete software.

This model is ideal for small projects with one or two developers working together and is also useful for academic or practice projects. It's an ideal model for the product where requirements are not well understood and the final release date is not given.

3.9.2 Advantages and Disadvantages of Waterfall Model

3.9.2.1 Advantages

The advantage of Big Bang is that it is very simple and requires very little or no planning. It is easy to manage and no formal procedures are required.

3.9.2.2 Disadvantage

The Big Bang model is a very high risk model and changes in the requirements or misunderstood requirements may even lead to complete reversal or scraping of the project. It is ideal for repetitive or small projects with minimum risks.

3.10 AGILE MODEL

Agile SDLC model is a combination of iterative and incremental process models with focus on process adaptability and customer satisfaction by rapid delivery of working software product. Agile Methods break the product into small incremental builds. These builds are provided in iterations. Each iteration typically lasts from about one to three weeks. Every iteration involves cross functional teams working simultaneously on various areas like planning, requirements analysis, design, coding, unit testing, and acceptance testing.

At the end of the iteration a working product is displayed to the customer and important stakeholders.

3.10.1 Concept of Agility

Agile model believes that every project needs to be handled differently and the existing methods need to be tailored to best suit the project requirements. In agile the tasks are divided to time boxes (small time frames) to deliver specific features for a release.

Iterative approach is taken and working software build is delivered at the end of each iteration. Each build is incremental in terms of features; the final build holds all the features required by the customer.

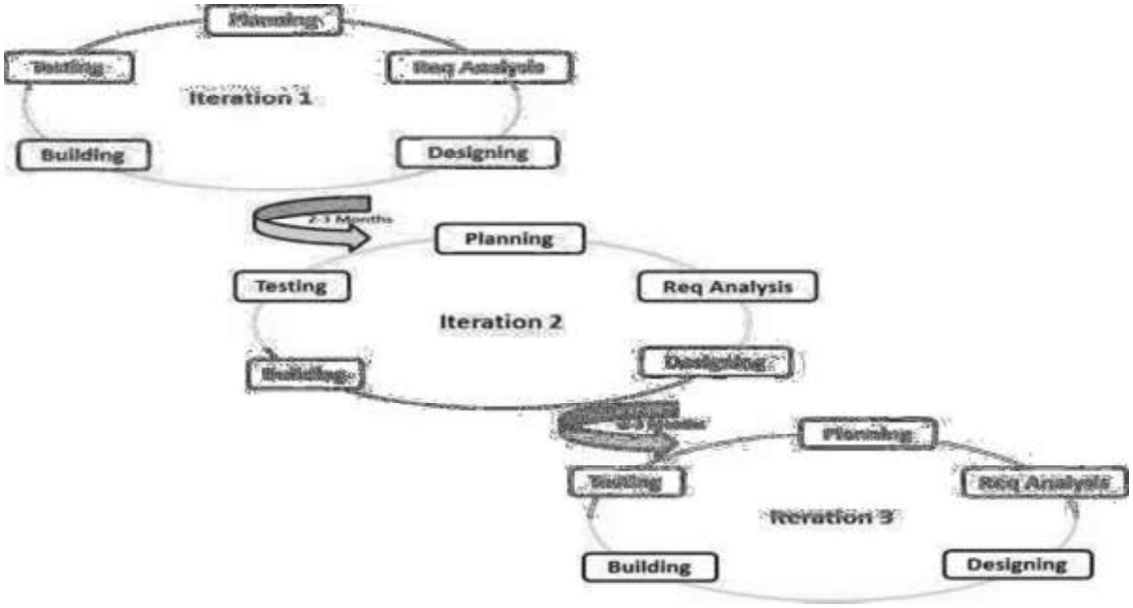


Figure 10: Agile Model

Agile thought process had started early in the software development and started becoming popular with time due to its flexibility and adaptability. The most popular agile methods include Rational Unified Process 1994, Scrum 1995, Crystal Clear, Extreme Programming 1996, Adaptive Software Development, Feature Driven Development, and Dynamic Systems Development Method DSDM 1995. These are now collectively referred to as agile methodologies, after the Agile Manifesto was published in 2001.

Agile Manifesto principles are as follows:

1. **Individuals and interactions** - in Agile development, the factors that gain importance are self-organization, motivation, interactions, co-location and pair programming.
2. **Working software** - Demonstration working software is considered the best means of communication with the customer to understand their requirement, instead of just depending on documentation.
3. **Customer collaboration** - As the requirements cannot be gathered completely in the beginning of the project due to various factors, continuous customer interaction is very important to get proper product requirements.
4. **Responding to change** - Agile development is focused on quick responses

to change and continuous development.

3.11 RAPID APPLICATION DEVELOPMENT MODEL

The Rapid Application Development (RAD) model is based on prototyping and iterative development with no specific planning involved. The process of writing the software itself involves the planning required for developing the product. Rapid Application development focuses on gathering customer requirements through workshops or focus groups, early testing of the prototypes by the customer using iterative concept, reuse of the existing prototypes components, continuous integration and rapid delivery.

3.11.1 RAD Concept

Rapid application development RAD is a software development methodology that uses minimal planning in favor of rapid prototyping. A prototype is a working model that is functionally equivalent to a component of the product. In RAD model the functional modules are developed in parallel as prototypes and are integrated to make the complete product for faster product delivery. Since there is no detailed preplanning, it makes it easier to incorporate the changes within the development process. RAD projects follow iterative and incremental model and have small teams comprising of developers, domain experts, customer representatives and other IT resources working progressively on their component or prototype. The most important aspect for this model to be successful is to make sure that the prototypes developed are reusable.

3.11.2 RAD Model Design

RAD model distributes the analysis, design, build, and test phases into a series of short, iterative development cycles. Following are the phases of RAD Model:

1. **Business Modeling:** The business model for the product under development is designed in terms of flow of information and the distribution of information between various business channels. A complete business analysis is performed to find the vital information for business, how it can be obtained, how and when is the information processed and what are the factors driving successful flow of information.
2. **Data Modeling:** The information gathered in the Business Modeling phase is reviewed and analyzed to form sets of data objects vital for the business. The

attributes of all data sets is identified and defined. The relation between these data objects are established and defined in detail in relevance to the business model.

3. **Process Modeling:** The data object sets defined in the Data Modeling phase are converted to establish the business information flow needed to achieve specific business objectives as per the business model. The process model for any changes or enhancements to the data object sets is defined in this phase. Process descriptions for adding, deleting, retrieving or modifying a data object are given.
4. **Application Generation:** The actual system is built and coding is done by using automation tools to convert process and data models into actual prototypes.
5. **Testing and Turnover:** The overall testing time is reduced in RAD model as the prototypes are independently tested during iterations. However the data flow and the interfaces between all the components need to be thoroughly tested with complete test coverage. Since most of the programming components have already been tested, it reduces the risk of any major issues.

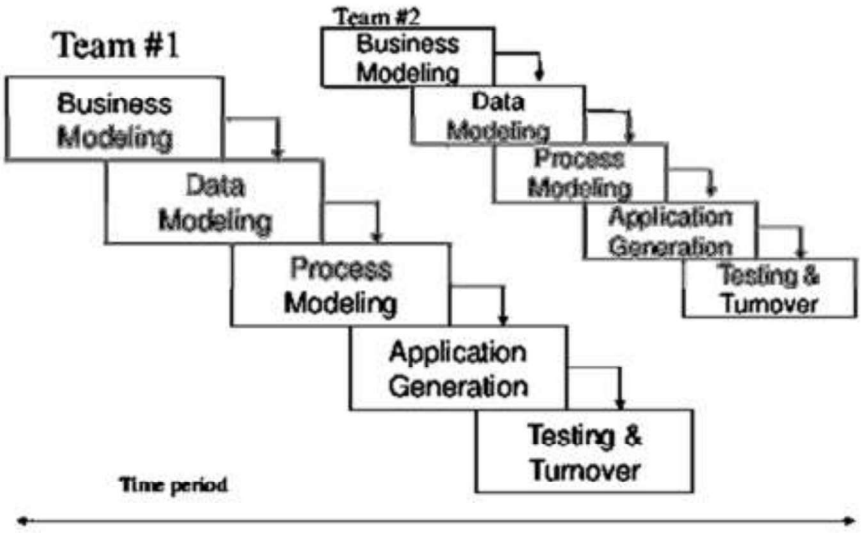


Figure 11: Rapid Application Development Model

3.11.3 RAD Model Applications

RAD model can be applied successfully to the projects in which clear modularization is possible. If the project cannot be broken into modules, RAD may fail. Following are the typical scenarios where RAD can be used:

a. RAD should be used only when a system can be modularized to be delivered in

incremental manner.

b. It should be used if there's high availability of designers for modeling.
c. It should be used only if the budget permits use of automated code generating tools.
d. RAD SDLC model should be chosen only if domain experts are available with relevant business knowledge.
e. Should be used where the requirements change during the course of the project and working prototypes are to be presented to customer in small iterations of 2-3 months.

3.11.4 Advantages and Disadvantages of RAD Model

3.11.4.1 Advantage

RAD model enables rapid delivery as it reduces the overall development time due to reusability of the components and parallel development.

3.11.4.2 Disadvantage

RAD works well only if high skilled engineers are available and the customer is also committed to achieve the targeted prototype in the given time frame. If there is commitment lacking on either side the model may fail.

3.12 SOFTWARE PROTOTYPING MODEL

The Software Prototyping refers to building software application prototypes which display the functionality of the product under development but may not actually hold the exact logic of the original software. Software prototyping is becoming very popular as a software development model, as it enables to understand customer requirements at an early stage of development. It helps get valuable feedback from the customer and helps software designers and developers understand about what exactly is expected from the product under development.

3.12.1 Software Prototyping Concept

- Prototype is a working model of software with some limited functionality.
- The prototype does not always hold the exact logic used in the actual software application and is an extra effort to be considered under effort estimation.
- Prototyping is used to allow the users evaluate developer proposals and try them out before implementation.
- It also helps understand the requirements which are user specific and may not have been considered by the developer during product design.

3.12.2 Steps involved in Software Prototyping

Stepwise approach to design a software prototype is as follows:

1. **Basic Requirement Identification:** This step involves understanding the very basics product requirements especially in terms of user interface. The more intricate details of the internal design and external aspects like performance and security can be ignored at this stage.
2. **Developing the initial Prototype:** The initial Prototype is developed in this stage, where the basic requirements are showcased and user interfaces are provided. These features may not exactly work in the same manner internally in the actual software developed and the workarounds are used to give the same look and feel to the customer in the prototype developed.
3. **Review of the Prototype:** The prototype developed is then presented to the customer and the other important stakeholders in the project. The feedback is collected in an organized manner and used for further enhancements in the product under development.
4. **Revise and enhance the Prototype:** The feedback and the review comments are discussed during this stage and some negotiations happen with the customer based on factors like, time and budget constraints and technical feasibility of actual implementation. The changes accepted are again incorporated in the new Prototype developed and the cycle repeats until customer expectations are met.

   Prototypes can have horizontal or vertical dimensions. Horizontal prototype displays the user interface for the product and gives a broader view of the entire system, without concentrating on internal functions. A vertical prototype

on the other side is a detailed elaboration of a specific function or a sub system in the product.

3.12.3 Software Prototyping Types

There are different types of software prototypes used in the industry. Following are the major software prototyping types used widely:

1. **Throwaway/Rapid Prototyping:** Throwaway prototyping is also called as rapid or close ended prototyping. This type of prototyping uses very little efforts with minimum requirement analysis to build a prototype. Once the actual requirements are understood, the prototype is discarded and the actual system is developed with a much clear understanding of user requirements.
2. **Evolutionary Prototyping:** Evolutionary prototyping also called as breadboard prototyping is based on building actual functional prototypes with minimal functionality in the beginning. The prototype developed forms the heart of the future prototypes on top of which the entire system is built. Using evolutionary prototyping only well understood requirements are included in the prototype and the requirements are added as and when they are understood.
3. **Incremental Prototyping:** Incremental prototyping refers to building multiple functional prototypes of the various sub systems and then integrating all the available prototypes to form a complete system.
4. **Extreme Prototyping:** Extreme prototyping is used in the web development domain. It consists of three sequential phases. First, a basic prototype with all the existing pages is presented in the html format. Then the data processing is simulated using a prototype services layer. Finally the services are implemented and integrated to the final prototype. This process is called Extreme Prototyping used to draw attention to the second phase of the process, where a fully functional UI is developed with very little regard to the actual services.

3.12.4 Software Prototyping Application

Software Prototyping is most useful in development of systems having high level of user interactions such as online systems. Systems which need users to fill out forms or go through various screens before data is processed can use prototyping very effectively to give the exact look and feel even before the actual software is developed. Software that involves too much of data processing and

most of the functionality is internal with very little user interface does not usually benefit from prototyping. Prototype development could be an extra overhead in such projects and may need lot of extra efforts. Software prototyping is used in typical cases and the decision should be taken very carefully so that the efforts spent in building the prototype add considerable value to the final software developed.

3.13 LET US SUM UP

1 This was about the various SDLC models available and the scenarios in which these SDLC models are used. The information in this tutorial will help the project managers decide what SDLC model would be suitable for their project and it would also help the developers and testers understand basics of the development model being used for their project.

2 We have discussed all the popular SDLC models in the industry, both traditional and Modern. This tutorial also gives you an insight into the applications, advantages and disadvantages of the SDLC models discussed.

3 Waterfall and V-model are traditional SDLC models and are of sequential type. Sequential means that the next phase can start only after the completion of first phase. Such models are suitable for projects with very clear product requirements and where the requirements will not change dynamically during the course of project completion.

4 Iterative and Spiral models are more accommodative in terms of change and are suitable for projects where the requirements are not so well defined, or the market requirements change quite frequently.

5 Big Bang model is a random approach to Software development and is suitable for small or academic projects.

6 Agile is the most popular model used in the industry. Agile introduces the concept of fast delivery to customers using prototype approach. Agile divides the project into small iterations with specific deliverable features. Customer interaction is the backbone of Agile methodology, and open communication with minimum documentation are the typical features of Agile development environment.

7 Rapid Application Development and Software Prototype are modern techniques to understand the requirements in a better way early in the project cycle. These techniques work on the concept of providing a working model to

the customer and stockholders to give the look and feel and collect the feedback. This feedback is used in an organized manner to improve the product.

3.14 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

i. The process of SDLC aims to produce high quality software that meets or exceeds customer experience and expectations while meeting the _____and _____constraints.

2 _____is the international standard for software lifecycle processes.

3 SRS Stands for_____.

4 A_____approach clearly defines all the architectural modules of the product along with its communication and data flow representation with the external and third party modules if any.

5 After the product is_____and ready it is released formally deployed in the appropriate market based on the Business strategy of the organization.

6 _____ model is often considered as the classic approach to the systems development life cycle.

7 The advantage of waterfall development is that it allows for _____ and_____.

8 The advantage of_____model is that there is a working model of the system at a very early stage of development which makes it easier to find functional or design flaws.

9 _____ model is also known as Verification and Validation model.

10 _____SDLC model is a combination of iterative and incremental process models with focus on process adaptability and customer satisfaction by rapid delivery of working software product.

11 _____is a working model of software with some limited functionality.

Answers:

1 Financial, time
2 ISO/IEC 12207
3 Software Requirement Specification

4 Design
5 Tested
6 Waterfall
7 Departmentalization, control
8 Iterative
9 V
10 Agile
11 Prototype

3.15 ASSIGNMENTS

1 Define SDLC. Explain different stages of SDLC with the help of a diagram.
2 Name the different SDLC models.
3 Discuss waterfall model. What are the applications of waterfall model. Discuss its advantages and disadvantages.
4 Discuss iterative model design.
5 Discuss spiral model.
6 Explain V-Model.
7 Explain Big Bang model.
8 What is the Concept of Agility?
9 Explain RAD Concept.
10 Explain the concept of Software Prototyping model.

Block-3

Unit 1: Authentication and Password Security

1

Unit Structure

1.1 LEARNING OBJECTIVES

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

- Know the basics authentication
- Differentiate identity, authentication and authorization
- Know types of authentication factors
- Study different types of authentication methods and protocols
- Study different types of authentication methods and protocols
- Set a strong passwords for your accounts
- Know the bad password combinations

1.2 INTRODUCTION

I hope all the readers are internet users! What is the first screen you encounter whenever you open your Gmail, Yahoomail or Rediffmail account? Yes you have guessed it right, you are landed to login page of the website.

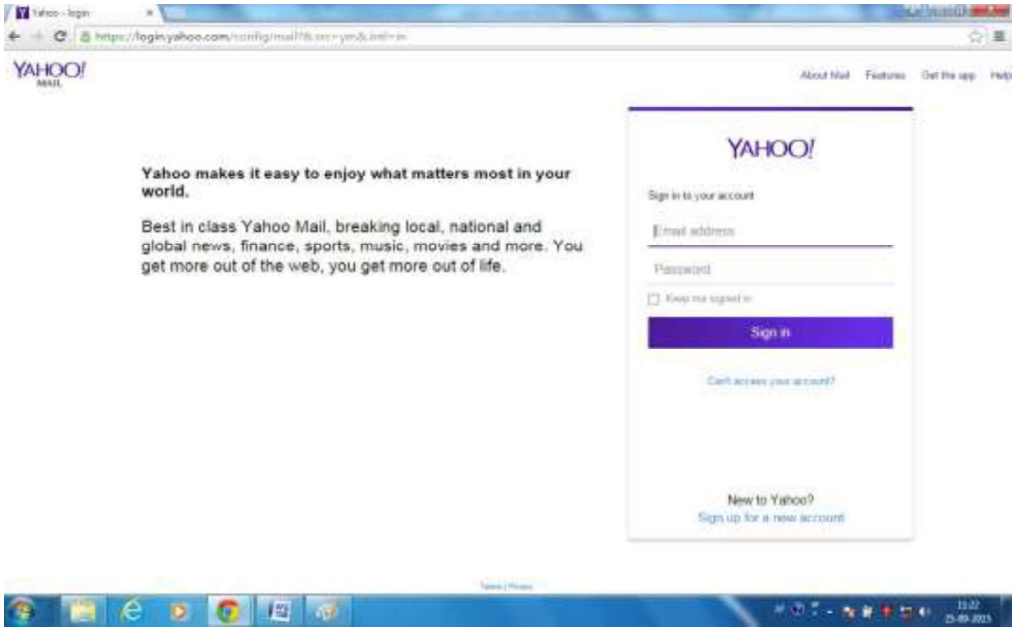


Figure 12: Login Screen of Yahoo

Have you ever thought why we require to login? Why we are not landed to our mailbox directly? You need to authenticate yourself before you are given access to your mailbox so that the unauthorized person does not have access to your communication. So login-password is the methods of authentication. Let us first discuss what authentication is!

1.3 AUTHENTICATION

1.3.1 Definition of Authentication

Authentication[11] is the act of confirming the truth of an attribute of a single piece of data (a datum) claimed true by an entity. In contrast with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a Website with a digital certificate, tracing the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification. In digital world, we perform electronic authentication. Let us now talk about e-authentication.

1.3.2 Definition of Electronic Authentication

Electronic authentication[12], also referred to as **e-authentication** is the process of establishing confidence in user identities electronically presented to an information system. In online environments, the username identifies the user, while the password authenticates that the user is who he claim to be. E-authentication presents a technical challenge when this process involves the remote authentication of individual people over a network, for the purpose of electronic government and commerce.

Authentication in the context of a user accessing an application tells an application who the current user is and whether or not they're present[13]. A full authentication protocol will probably also tell you a number of attributes about this user, such as a unique identifier, an email address, and what to call them when the application says "Good Morning". Authentication is all about the user and their presence with the application, and an internet- scale authentication protocol needs to be able to do this across network and security boundaries.

---

[11] https://en.wikipedia.org/wiki/Authentication

[12] https://en.wikipedia.org/wiki/Electronic_authentication

[13] http://oauth.net/articles/authentication/

1.3.3 Authentication vs. Authorization

The word authentication is often confused with authorization. Let us discuss the difference between the two. As stated in the above paragraph, authentication is process of verifying the claim of the person whom he claims to be by the use of some personal identifiers. Whereas authorization is the process of allocation of access rights to the used after the identity of the person is confirmed through authorization. Often the organizations have hierarchical structure. There are workers at the lower level, supervisors at the middle level and manager & higher management like General Manager at the top level. Different kinds of privileges are granted at different levels. For example, let us discuss an example of a School/College Management System. The hierarchical structure is as follows:

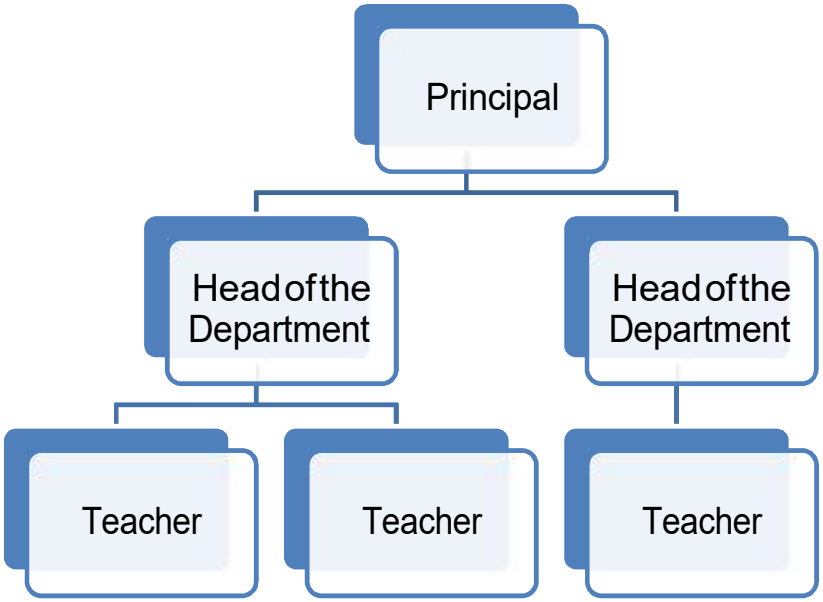


Figure 13: Organizational structure in a school

The teacher feeds the marks/attendance of the student in the School Management System. So the teacher is given the write permission to enter the marks/attendance of a particular subject and he can view/enter details pertaining to his subject only. The head of the department is one level-up in the hierarchy and is responsible for all the subjects, teachers and students of a particular department. So he may be given both read and write permission so that he can view/enter the subjects allocated to him as well as view the details of the subjects under his department.

Principal is the head of the school. He is responsible for all the subjects, teachers and students of the school. Some students may have short attendance and therefore are not allowed to sit in the final examination due to short attendance. He student may submit medical certificate or may produce an evidence of attending a school activity like sports, cultural festival etc. After approval, he may need to modify the existing attendance. Marks, etc. therefore, Principal may need all the three permissions like enter, view and modify.

Whenever a person login into the system, he may be asked for user login and password. Login is for verifying who the user is and the password is for verifying the user who he claims to be. Once it is verified that it's a teacher login, head login or principal log based on authorization, the user may be allowed to perform one/all of the activities from write, view or modify. After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change). This is called authorization.

1.3.4 Types of Authentication Factors

In authentication, we generally talk about three "factors" for determining identity[14]. A "factor" is a broad category for establishing that you are who you claim to be. The three types of authentication factors are:

A. *Something you know (a password, a PIN, the answer to a "security question", etc.)* Most of us are familiar with password authentication. To log onto a computer or network, you enter a user account name and the password assigned to that account. This password is checked against a database that contains all authorized users and their passwords. In a Windows 2000 network, for example, this information is contained in Active Directory. To preserve the security of the network, passwords must be "strong," that is, they should contain a combination of alpha and numeric characters and

[14] https://securityblog.redhat.com/tag/two-factor-authentication/

symbols, they should not be words that are found in a dictionary, and they should be relatively long (eight characters or more). In short, they should not be easily guessed. Password authentication is vulnerable to a password "cracker" who uses a brute force attack (trying every possible combination until hitting upon the right one) or who uses a protocol "sniffer" to capture packets if passwords are not encrypted when they are sent over the network.

B. *Something you have (an ATM card, a smart card, a one-time-password token, etc.)* Smart cards are credit card-sized devices that hold a small computer chip, which is used to store public and private keys and other personal information used to identify a person and authenticate him or her to the system. Logging onto the network with a smart card requires that you physically insert the card into (or slide it through) a reader and then enter a Personal Identification Number (PIN) in much the same way that you use an ATM card to access an automatic teller machine. Smart cards use cryptography-based authentication and provide stronger security than a password because in order to gain access, the user must be in physical possession of the card *and* must know the PIN.

C. *Something you are (your fingerprint, retinal pattern, DNA)*

An even more secure type of authentication than smart cards, biometric authentication involves the use of biological statistics that show that the probability of two people having identical biological characteristics such as fingerprints is infinitesimally small; thus, these biological traits can be used to positively identify a person. In addition to fingerprints, voice, retinal, and iris patterns are virtually unique to each individual and can be used for authentication purposes. This method of proving one's identity is very difficult to falsify, although it requires expensive equipment to input the fingerprint, voice sample, or eye scan. Another advantage over smart cards is that the user does not have to remember to carry a device; his or her biological credentials are never left at home.

Historically, most people have used the first of these three factors. Whenever you've logged into Facebook, you entered something you know: your user

name and password. One of the less common, but growing, authentication methods is biometrics. A couple years ago, a major PC manufacturer ran a number of television commercials advertising their laptop models with a fingerprint scanner. The claim was that it was easy and secure to unlock the machine with a swipe of a finger. Similarly, Google introduced a service to unlock an Android smartphone by using facial recognition with the phone's built-in camera.

Pay attention readers, because I am about to remove the scales from your eyes. Those three factors I listed above? I listed them in decreasing order of security. "But how can that be?", you may ask. "How can my unchangeable physical attributes be less secure than a password? Everyone knows passwords aren't secure." The confusion here is due to subtle but important definitions in the meaning of "security".

Most common passwords these days are considered "insecure" because people tend to use short passwords which by definition have a limited entropy pool (meaning it takes a smaller amount of time to run through all the possible combinations in order to brute-force the password or run through a password dictionary). However, the pure computational complexity of the authentication mechanism is not the only contributor to security.

The second factor above, "something you have" (known as a token), is almost always of significantly higher entropy than anything you would ever use as a password. This is to eliminate the brute-force vulnerability of passwords. But, it comes with a significant downside as well: something you have is also something that can be physically removed from you. Where a well-chosen password can only be removed from you by social engineering (tricking you into giving it to an inappropriate recipient), a token might be slipped off your desk while you are at lunch.

Both passwords and tokens have an important side-effect that most people never think about until an intrusion has been caught: remediation. When someone has successfully learned your password or stolen your token, you can call up your helpdesk and immediately ask them to reset the password or disable the cryptographic seed in the token. Your security is now restored and

you can choose a new password and have a new token sent to you.

However, this is not the case with a biometric system. By its very nature, it is dependent upon something that you cannot change. Moreover, the nature of its supposed security derives from this very fact. The problem here is that it's significantly easier to acquire a copy of someone's fingerprint, retinal scan or even blood for a DNA test than it is to steal a password or token device and in many cases it can even be done without the victim knowing. Many consumer retinal scanners can be fooled by a simple reasonably-high-resolution photograph of the person's eye (which is extremely easy to accomplish with today's cameras). Some of the more expensive models will also require a moving picture, but today's high-resolution smartphone cameras and displays can defeat many of these mechanisms as well. It's well- documented that Android's face-unlock feature can be beaten by a simple photograph.

These are all technological limitations and as such it's plausible that they can be overcome over time with more sensitive equipment. However, the real problem with biometric security lies with its inability to replace a compromised authentication device. Once someone has a copy of your ten fingerprints, a drop of your blood from a stolen blood-sugar test, or a close- up video of your eye from a scoped video camera, there is no way to change this data. You can't ask helpdesk to send you new fingers, an eyeball, or DNA. Therefore, I contend that I lied to you above. There is no full third factor for authentication, because, given a sufficient amount of time, any use of biometrics will eventually degenerate into a non-factor. Given this serious limitation, one should never under any circumstances use biometrics as the sole form of authentication for any purpose whatsoever.

One other thought: have you ever heard the argument that you should never use the same password on multiple websites because if it's stolen on one, they have access to the others? Well, the same is true of your retina. If someone sticks malware on your cellphone to copy an image of your eye that you were using for "face unlock", guess what? They can probably use that to get into your lab too.

The moral of the story is this: biometrics are minimally useful, since they are

only viable until the first exposure across all sites where they are used. As a result, if you are considering initiating a biometric-based security model, I encourage you to look into a two-factor solution involving passwords and a token of some kind.

1.3.5 Multi Factor and Two Factor Authentication

When two or more access methods are included as part of the authentication process, your implementing a multi-factor system[15]. A system that uses smartcards and passwords is referred to as a two-factor system. Two-factor authentication (also known as 2FA) is a technology patented in 1984 that provides identification of users by means of the combination of two different components. These components may be something that the user knows, something that the user possesses or something that is inseparable from the user. A good example from everyday life is the withdrawing of money from a cash machine. Only the correct combination of a bank card (something that the user possesses) and a PIN (personal identification number, i.e. something that the user knows) allows the transaction to be carried out. 2FA is ineffective against modern threats, like ATM skimming, phishing, and malware etc. Two-factor authentication is a type of multi-factor authentication. If you've ever used Google's two-factor authentication to log in, you probably used a code stored on your smartphone to do so.

1.4 AUTHENTICATOIN METHODS AND PROTOCOLS

There are a large number of authentication methods and protocols that can be used, depending on the application and security requirements. In the following sections, we will discuss different types of popular authentication methods and protocols.

1.4.1 Kerberos

Kerberos[16] is a network authentication protocol. It is designed to provide strong authentication or client-server applications by using secret-key cryptography. It allows nodes communicating over a non-secure network to

[15] http://www.go4expert.com/articles/understanding-authentication-t8842/
[16] http://computers.interactiva.org/Security/Authentication/Kerberos/

prove their identity to one another in a secure manner[17]. Its designers aimed it primarily at a client–server model and it provides mutual authentication—both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks. It was developed by Massachusetts Institute of Technology (MIT) developed Kerberos to protect network services provided by Project Athena. The protocol is based on the earlier Needham–Schroeder symmetric key protocol. The client authenticates itself to the Authentication Server (AS) which forwards the username to a key distribution center (KDC). The KDC issues a ticket- granting ticket (TGT), which is time stamped, encrypts it using the user's password and returns the encrypted result to the user's workstation. This is done infrequently, typically at user logon; the TGT expires at some point, though may be transparently renewed by the user's session manager while they are logged in. When the client needs to communicate with another node ("principal" in Kerberos parlance) the client sends the TGT to the ticket- granting service (TGS), which usually shares the same host as the KDC. After verifying the TGT is valid and the user is permitted to access the requested service, the TGS issues a ticket and session keys, which are returned to the client. The client then sends the ticket to the service server (SS) along with its service request.

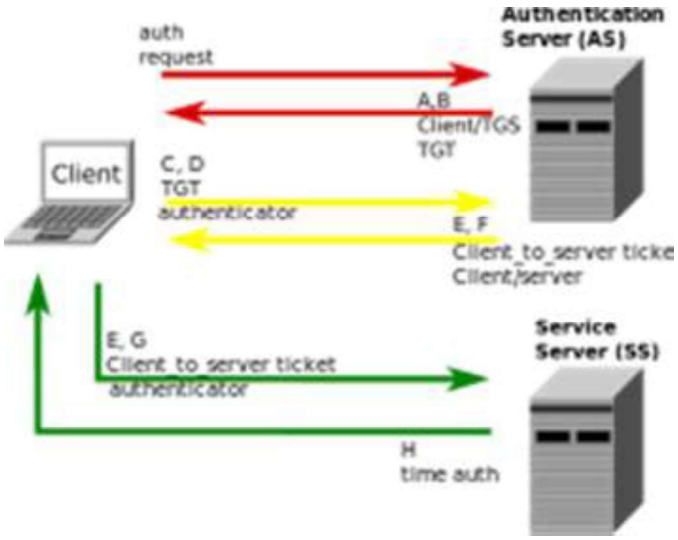


Figure 14: Kerberos Negotiations

[17] http://www.territorioscuola.com/enhancedwiki/en.php?title=Kerberos_(protocol)

1.4.2 Secure Sockets Layer(SSL)

The first thing you need to know about Secure Sockets Layer is that it is no longer called that[18]. For purist reasons, the protocol formerly known as SSL is now called Transport Layer Security, or TLS. The reasons for this name change are fairly esoteric and originate partly in a description of networking architecture as the Open Systems Interconnection seven-layer networking model. SSL hovered uncomfortably between the transport layer (4) and the presentation layer(6), and some experts felt, long after the OSI model had fallen out of fashion, that SSL was not really a layer at all. In the more recent TCP/IP model, which has fewer layers, SSL operates somewhere between the transport and application layers. Also, the protocol can - in principle - be applied to other networking protocols than just sockets, even though the vast majority of global communication are now made using the socket programming interface. Almost every product that implements TLS continues to refer to it as SSL, usually with some weasel words added like more properly known as TLS. The SSL protocol was originally invented by the Netscape Corporation as a way of providing secure browsing in their web browser. The Netscape Corporation was absorbed into AOL now.

The symmetric-key encryption is considerably more efficient than public key encryption. So, for encrypting bulk data transfer with high performance, symmetric-key encryption is a must. But to use it, both partners in the conversation must know a single shared secret key. But how do you share a secret key with a partner that you have never communicated with before? This is known as the key exchange problem. An early solution to this problem was for a trusted courier to carry the key, physically locked in a secure container, from one location to another. This is highly secure, but expensive and inconvenient, and hardly practical for electronic commerce. Furthermore, the same key is used for encrypting all traffic, which somewhat simplifies the possibility of an attacker breaking the key.

---

[18] http://peter.havercan.net/computing/plain-persons-guide-to-secure-sockets-layer.html

SSL, in brief, is a solution to the key exchange problem that is suitable for electronic communication. The two partners in the conversation must be identified as the client and the server as their roles are different: the conversation is not symmetric. The conversation is initiated by the client, who provides a list of suggested encryption techniques. The server responds with a certificate containing the server's public key, and an encryption technique that is acceptable to the client. The client validates the server's certificate, and uses the public key within it to encrypt a random string called the pre-master-secret, which it sends to the server. The server uses its private key to decrypt the pre-master-secret. At this point, the key exchange problem is solved: the client and server can both use the pre-master-secret to generate the key required by the mutually chosen encryption technique.

Both the client and server now possess a mutually chosen encryption algorithm and a key to use with it. They are now in a position to exchange secret encrypted messages using fast symmetric-key encryption, using a shared key that has never appeared in plain text in the conversation. Furthermore, a different key is used for each conversation, limiting the opportunity for an attacker to break it.

1.4.3 Microsoft NTLM

NTLM[19] is a suite of authentication and session security protocols used in various Microsoft network protocol implementations and supported by the NTLM Security Support Provider ("NTLMSSP"). Originally used for authentication and negotiation of secure DCE/RPC, NTLM is also used throughout Microsoft's systems as an integrated single sign-on mechanism. It is probably best recognized as part of the "Integrated Windows Authentication" stack for HTTP authentication; however, it is also used in Microsoft implementations of SMTP, POP3, IMAP (all part of Exchange), CIFS/SMB, Telnet, SIP, and possibly others.

The NTLM Security Support Provider provides authentication, integrity, and confidentiality services within the Window Security Support Provider Interface (SSPI) framework. SSPI specifies a core set of security functionality that is

[19] http://davenport.sourceforge.net/ntlm.html Copyright © 2003, 2006 Eric Glass

implemented by supporting providers; the NTLMSSP is such a provider. The SSPI specifies, and the NTLMSSP implements, the following core operations:

a. Authentication - NTLM provides a challenge-response authentication mechanism, in which clients are able to prove their identities without sending a password to the server.
b. Signing - The NTLMSSP provides a means of applying a digital "signature" to a message. This ensures that the signed message has not been modified (either accidentally or intentionally) and that that signing party has knowledge of a shared secret. NTLM implements a symmetric signature scheme (Message Authentication Code, or MAC); that is, a valid signature can only be generated and verified by parties that possess the common shared key.
c. Sealing - The NTLMSSP implements a symmetric-key encryption mechanism, which provides message confidentiality. In the case of NTLM, sealing also implies signing (a signed message is not necessarily sealed, but all sealed messages are signed).

NTLM has been largely supplanted by Kerberos as the authentication protocol of choice for domain-based scenarios. However, Kerberos is a trusted-third-party scheme, and cannot be used in situations where no trusted third party exists; for example, member servers (servers that are not part of a domain), local accounts, and authentication to resources in an untrusted domain. In such scenarios, NTLM continues to be the primary authentication mechanism (and likely will be for a long time).

1.4.4 Password Authentication Protocol

Password authentication protocol (PAP) is an authentication protocol that uses a password[20]. PAP is used by Point to Point Protocol to validate users before allowing them access to server resources. Almost all network operating system remote servers support PAP.

PAP transmits unencrypted ASCII passwords over the network and is therefore

[20] https://en.wikipedia.org/wiki/Password_Authentication_Protocol

considered insecure. PAP is the protocol where two entities share a password in advance and use the password as the basis of authentication. Existing password authentication schemes can be categorized into two types: weak-password authentication schemes and strong-password authentication schemes. When compared to strong-password schemes, weak-password schemes tend to have lighter computational overhead, the designs are simpler, and implementation is easier, making them especially suitable for some constrained environments.

PAP is a two step authentication protocol which are:

a. Authentication Request: the device which initiated the communication send *Authenticate-Request* message to the responder. This *Authenticate-Request* message contains a name and a password.

b. Authentication Reply: Once the *Authenticate-Request* message receives the responder, it authenticates the message by checking the username and the password. If the authentication is successful, it reply back with *Authenticate-Ack* message else *Authenticate-Nak* massage is send back to the initiator.

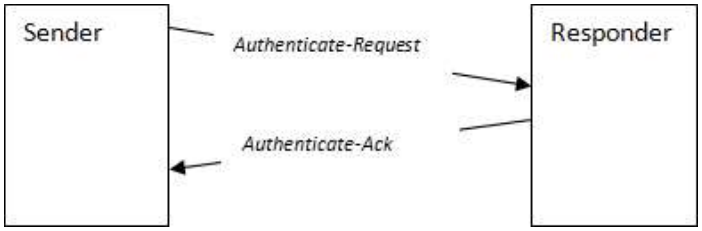


Figure 15: Authorization-Ack when authorization is secussful

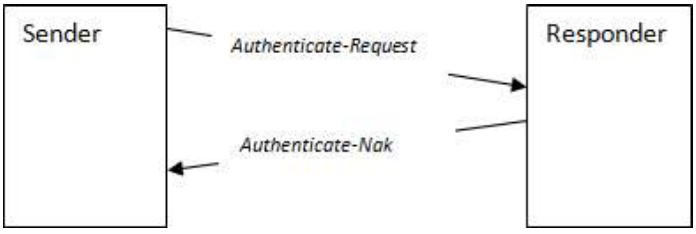
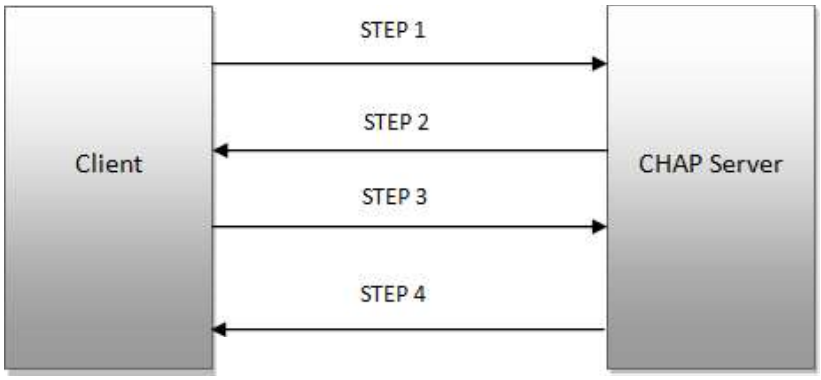


Figure 16: Authorization-Nak when authorization is not secussful

PAP is simple authentication protocol but have some serious security issues associated with it. First of all, it sends the username and the password as plain text, due to this becomes an easy prey for the hackers. Secondly, it does not keep any upper limit on the number of unsuccessful attempts on incorrect username and password, unlike most of the sites which block the attempts after three consecutive unsuccessful attempts.

1.4.5 Challenge-Handshake Authentication Protocol(CHAP)

Challenge-Handshake Authentication Protocol challenges a system to verify identity[21]. CHAP doesn't use userID/Password mechanism. Instead, the initiator sends a logon request from the client to the server. The server sends a challenge back to the client. The challenge is encrypted and then sent back to the server. The server compares the value from the client and, if the information matches, grants authorization. If the response fails, the session fails, and the request phase starts over.



Following are the steps[22] ::

a. STEP1: the authenticator (main server) sends a "challenge" message to the peer (client);
b. STEP2: the peer responds with a value calculated using a one-way hash function, using SHA checksum hash ;
c. STEP3: the authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator

[21] http://www.go4expert.com/articles/understanding-authentication-t8842/

[22] http://pychatter.wikidot.com/how-it-works

acknowledges the authentication; otherwise it should terminate the connection ;

d. STEP4: at random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.

The challenge is the hashed value of the client password concatenated to a random number. The whole is hashed and represents the challenge. The main server sends the random number to the client which in the same way calculates the challenge and sends it to the main server for comparison.

1.4.6 Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)

It is the Microsoft version of the Challenge-Handshake Authentication Protocol[23]. MS-CHAP is used as one authentication option in Microsoft's implementation of the PPTP protocol for virtual private networks. It is also used as an authentication option with RADIUS servers which are used for WiFi security using the WPA-Enterprise protocol. It is further used as the main authentication option of the Protected Extensible Authentication Protocol (PEAP).

Compared with CHAP, MS-CHAP:

a. Is enabled by negotiating CHAP Algorithm 0x80 (0x81 for MS-CHAPv2) in LCP option 3, Authentication Protocol
b. provides an authenticator-controlled password change mechanism
c. provides an authenticator-controlled authentication retry mechanism
d. defines failure codes returned in the Failure packet message field

1.4.7 Extensible Authentication Protocol

Extensible Authentication Protocol[24], or EAP, is an authentication framework frequently used in wireless networks and point-to-point connections. EAP is an authentication framework providing for the transport and usage of keying material and parameters generated by EAP methods. There are many methods

---

[23] https://en.wikipedia.org/wiki/MS-CHAP

[24] https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

defined by RFCs and a number of vendor specific methods and new proposals exist. EAP is not a wire protocol; instead it only defines message formats. Each protocol that uses EAP defines a way to encapsulate EAP messages within that protocol's messages.

1.4.8 Remote Authentication Dial-In User Service (RADIUS)

RADIUS is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service[25]. RADIUS was developed by Livingston Enterprises, Inc. in 1991 as an access server authentication and accounting protocol and later brought into the Internet Engineering Task Force (IETF) standards. Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. These networks may incorporate modems, DSL, access points, VPNs, network ports, web servers, etc.

1.4.9 Certificates

This is another common form of authentication[26]. A server or certificate authority (CA) can issue a certificate that will be accepted by the challenging system. Certificates can either be physical access devices, such as smart cards, or electronic certificates that are used as part of the logon process. A certificate practice statement (CPS) outlines the rules used for issuing and managing certificates. A certificate revocation list (CRL) lists the revocations that must be addressed (often due to expiration) in order to stay current. A simple way to think of certificates is like hall passes at school.

1.4.10 Security Tokens

These are similar to certificates. They contain the rights and access privileges of the token bearer as part of the token. Think of a token as a small piece of data that holds a sliver of information about the user. Many operating systems generate a token that is applied to every action taken on the computer system.

---

[25] https://en.wikipedia.org/wiki/RADIUS

[26] http://www.go4expert.com/articles/understanding-authentication-t8842/

If your token don't grant you access to certain information, then either that information won't be displayed or your access will be denied. The authentication system creates a token every time a user connects or a session begins. At the completion of a session, the token is destroyed.

1.5 Selecting a Strong Password

The weakest point in any security for your online accounts is usually your password[27]. One should pay attention to make sure your content is secure, protected, and can't be accessed by anyone other than the owner. But if someone else is able to guess or retrieve your password, they bypass almost every security measure provided by the host server as it will see this person as you. They could then make any changes they wish to your account. To avoid this scenario, this section will help you create strong passwords that are hard to guess or crack. Password-cracking techniques have matured quickly and significantly in the past few decades, but the way we create our passwords hasn't kept pace. As a result, the most common advice you'll hear about creating a strong password today is very outdated and impractical. A password created with that advice, like **jal43#Koo%a**, is very easy for a computer to break and very difficult for a human to remember and type.

The latest and most effective types of password attacks can attempt up to ***350 billion guesses per second***, and that number will no doubt increase significantly over the next few years. Creating a strong password today requires modern techniques. There are many different approaches to generating a strong password, but password managers and passphrases are the best. Creating a strong password and changing it frequently is one of the smartest things a user can do to protect themselves when working online[28]. For many institutions, usernames and domains are generated based on a common formula: for Uttarakhand Open University, first initial and last name, with the jpande@uou.ac.in

Because of this, it's really not enough to rely fully on the security systems of the

[27] https://en.support.wordpress.com/selecting-a-strong-password

[28] http://kb.cu-portland.edu/Password+Security

places that you use your password on. Often times, the least important passwords becomes the most important because hackers target those first. Sure, your bank is pretty secure. But if you use the same password in multiple locations, or iterations of the same password, it doesn't matter how secure your bank's security system is. Hackers start with the stupid websites that require a username and password to process web payments, or logins to read the news or comment on forums, or whatever. If the password you used to order a pizza last weekend is the same as the one you use to access your student loans…. well, no amount of security is going to stop someone when they know your password already.

1.5.1 Bad Password Combinations

Here are some of the most common passwords or password configurations people use. If this is you – it's time to change!

a. Your partner, child, or pet's name, possibly followed by a 0 or 1 (because they're always making you use a number, aren't they?)
b. The last 4 digits of your social security number.
c. 123 or 1234 or 123456.
d. "password"
e. Your city, or college, football team name.
f. Date of birth – yours, your partner's or your child's.
g. "god"
h. "money"
i. "love"

1.5.2 Tips for a Strong Password

a. Length. As computers that process Brute Force attacks (just running different combinations of passwords and usernames repeatedly until they get a result) become more intelligent, length becomes the defining variable in passwords that will take longer to process.

b. In conjunction with length, choose a pass phrase that means something to you instead of a word, a name, or a title. For example:

“mydogslovetoeatswisscheese” is a better pass phrase than “Fido123”.

c. Although it’s not the ‘rule’ for unbreakable passwords anymore, randomizing your capitalization and using special characters are still useful and effective in making your password harder to crack.

d. Turn a phrase into a string of characters that look completely unrelated, but in reality is easy to remember. So “all creatures great and small” would become “acg8@s” or something similar.

e. Don't use words that can be found in a dictionary or someone's name. Password generators can crack these in no time. At the very least, use something slightly off the beaten path.

f. Have problems remembering lots of different passwords? Try using an encrypted password utility like Roboform, LastPass and KeePass for Windows, or 1Password for Macs.

g. Changing your password often is important too, but not terribly effective if all you do is change the number at the end of a word. Using passphrases instead of passwords means you have to change them less often, and are more likely to remember them when you do.

h. Make a note. Don’t write your password down, but if you know you have trouble remembering, slip a piece of paper in your wallet with a clue that’s significant only to you.

i. Create a Passphrase instead of a Password – A passphrase is similar to a password, except that it’s based on a random collection of words, rather than just one. For example, copy indicate trap bright.

j. Because the length of a password is one of the primary factors in how strong it is, passphrases are much more secure than traditional passwords. At the same time, they are also much easier to remember and type.

k. They’re not as strong as the kinds of passwords generated by password managers, but they’re still a good option if you don’t want to use a password manager. They’re also the best way to generate the master

password for a password manager or your operating system account, since those can't be automatically filled in by the password manager.

l. Don't use the same password twice. Many popular websites fail to adequately secure your password in their systems, and hackers routinely break into them and access hundreds of millions of accounts. If you reuse passwords from site to site, then someone who hacks into one site will be able to login to your account on other sites. At the very least, make sure that you have unique passwords for all sites that store financial or other sensitive data, or ones that could be used to hurt your reputation.

m. Make sure your email password is also strong. With many online services like WordPress.com, your email address serves as your identification. If a malicious user gains access to your email, they can easily reset your passwords and login to your account.

n. Don't share your passwords. Even if you trust the person, it's possible an attacker could intercept or eavesdrop on the transmission, or hack that person's computer. If you suspect that someone else knows your password, you should change it immediately.

o. Don't send your password to anyone in an email. E-mails are rarely encrypted, which makes them relatively easy for attackers to read. WordPress.com staff will never ask you for your password. If you must share a password, use a secure method of transmission like pwpush.com, and set the link to expire after the first view.

p. Don't save your passwords in a web browser. They often fail to store the passwords in a secure manner, so use a password manager instead. See the section on password managers above for more information.

q. Don't save passwords or use "Remember Me" options on a public computer. If you do, then the next person to use the computer will be able to access your account. Also make sure you log out or close your browser when you are done.

r. Don't write down your password. If it's written down somewhere and

someone can find it, it's not secure. Store passwords in a password manager instead, so that they'll be encrypted. See the section on password managers above for more information. The exception to this rule is storing unrecoverable passwords (like the master password for a password manager, or your operating system account) in a secure manner. One good way to secure them is to keep it in a safe deposit box, or locked in a safe.

s. Don't change your passwords, unless you suspect they've been compromised. As long as you have the type of strong password recommended in this article, changing it frequently will not do anything to minimize the risk of it being compromised. Because changing them can be a burden, it often tempts people to adopt bad practices in order to make the process easier, which increases their vulnerability to attacks. If you suspect someone has gained access to your account, though, then it's always a good precaution to change your password.

t. Use a Password Manager: A password manager is a software application on your computer or mobile device that generates very strong passwords and stores them in a secure database. You use a single passphrase to access the database, and then the manager will automatically enter your username and password into a website's login form for you. There are many different manager applications to choose from, so you'll need to pick which one you'd like to use, and then install it on your computer. These are the general steps, but you may want to check the documentation for your specific application for more details. Choose a password manager. Some popular ones are:

   - 1Password (closed-source, commercial)
   - LastPass (closed-source, free/commercial)
   - Dashlane (closed-source, free/commercial)
   - KeePass (open source, free)
   - RoboForm (closed-source, commercial).

u. Use Passphrase: Creating a passphrase follows similar rules to creating

a traditional password, but it doesn't need to be as complex, because the length of the phrase will provide enough security to outweigh the simplicity.

- Choose 4 random words. You can use the xkcd Passphrase Generator if you'd like, but it's better if you make up your own.
- Add spaces between the words if you prefer.
- Make a few of the letters upper-case.
- Add in a few number and symbols.

1.5.2.1 Things to avoid when using Passphrase

v. Don't place the words in a predictable pattern or form a proper sentence; that would make it much easier to guess.

w. Don't use song lyrics, quotes or anything else that's been published. Attackers have massive databases of published works to build possible passwords from.

x. Don't use any personal information. Even when combined with letters and numbers, someone who knows you, or can research you online, can easily guess a password with this information.

1.6 LET US SUM UP

1. **Authentication** is the act of confirming the truth of an attribute of a single piece of data (a datum) claimed true by an entity.
2. **Identification** which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity.
3. **Electronic authentication**, also referred to as **e-authentication** is the process of establishing confidence in user identities electronically presented to an information system.
4. **Authorization** is the process of allocation of access rights to the used after the identity of the person is confirmed through authorization.
5. The three types of authentication factors are: Something you know (a password, a PIN, the answer to a "security question", etc.), Something you have (an ATM card, a smart card, a one-time-password token, etc.},

Something you are (your fingerprint, retinal pattern, DNA)

6. When two or more access methods are included as part of the authentication process, it is known as multi-factor system.
7. Some of the popular authentication methods and protocols are: Kerberos, SSL, CHAP, PAP, MS-CHAP, MS-NTML,EAP, RADIUS, Certificate, Security tokens, etc.
8. Kerberos is a network authentication protocol. It is designed to provide strong authentication for client-server applications by using secret-key cryptography.
9. The SSL protocol was originally invented by the Netscape Corporation as a way of providing secure browsing in their web browser.
10. Password authentication protocol (PAP) is an authentication protocol that uses a password.
11. Extensible Authentication Protocol, or EAP, is an authentication framework frequently used in wireless networks and point-to-point connections.
12. RADIUS is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service.
13. This is another common form of authentication[29]. A server or certificate authority (CA) can issue a certificate that will be accepted by the challenging system.
14. Security tokens are similar to certificates. They contain the rights and access privileges of the token bearer as part of the token.
15. The weakest point in any security for your online accounts is usually your password.
16. The latest and most effective types of password attacks can attempt up to ***350 billion guesses per second***, and that number will no doubt increase significantly over the next few years.

[29] http://www.go4expert.com/articles/understanding-authentication-t8842/

1.7 CHECK YOUR PROGRESS : POSSIBLE ANSWERS

1. Fill in the blanks:

I. _____refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity.

II. ____is for verifying who the user is and the_____is for verifying the user who he claims to be.

III. Massachusetts Institute of Technology (MIT) developed_____to protect network services provided by Project Athena.

IV. Secure Sockets Layer is now known as_____.

V. The SSL protocol was originally invented by the_____as a way of providing secure browsing in their web browser

VI. CHAP stands for____.

VII. _____can either be physical access devices, such as smart cards, or electronic certificates that are used as part of the logon process.

2. State True or False

I. State true or False: You should use the same password on multiple websites.

II. State true or False: Withdrawing of money from a cash machine is an example of two-factor authentication.

III. State true or False: Kerberos is a network authentication protocol.

IV. State true or False: The symmetric-key encryption is considerably more efficient than public key encryption.

V. State true or False: Don't save your passwords in a web browser.

Answers:

1. Fill in the blanks.
   I. Identification
   II. Login, password
   III. Kerberos
   IV. Transport Layer Security
   V. Netscape Corporation
   VI. Challenge-Handshake Authentication Protocol challenges
   VII. Certificates
2. State True or False
   I. False
   II. True
   III. True

IV. True

V. True

1.8 FURTHER READING

1 A mechanism for identity delegation at authentication level, N Ahmed, C Jensen - Identity and Privacy in the Internet Age - Springer 2009

2 " New NIST Publications Describe Standards for Identity Credentials and Authentication Systems" available at http://www.nist.gov/itl/csd/piv_090809.cfm

3 Forouzan (2007). Data Commn & Networking 4E Sie. McGraw-Hill Education (India) Pvt Limited. pp. 352–. ISBN 978-0-07-063414-5. Retrieved 24 November 2012.

4 Lloyd, Brian; Simpson, William Allen (October 1992). "Password Authentication Protocol". *PPP Authentication Protocols*. IETF. p. 2. RFC 1334. Retrieved 26 Sep. 2015 available at https://tools.ietf.org/html/rfc1334#page-2

5 "AAA and Network Security for Mobile Access. RADIUS, DIAMETER, EAP, PKI and IP mobility". M Nakhjiri. John Wiley and Sons, Ltd

6 Hassell, Jonathan (2002). *RADIUS - Securing Public Access to Private Resources*. O'Reilly & Associates. ISBN 0-596-00322-6.(Selecting a strong password, 2015)

1.9 ASSIGNMENTS

1 What is Authentication? How it is different from electronic authentication?

2 Compare Authentication with authorization.

3 Explain different types of authentication factors in details.

4 What is multi-factor authentication?

5 Write a short note on Kerberos.

6 What are the core operation specified by Security Support Provider Interface.

7 What are the two basic authentication steps of Password Authentication Protocol . Explain

8 Explain CHAP authentication process.

9 Define RADIUS.

10 What are the few bad password combination that people often use in daily life.

11 List some of the guidelines to create a strong password.

12 What is password manager? Give some examples of popular password managers.

Unit 2: WIRELESS SECURITY 2

Unit Structure

2.1 LEARNING OBJECTIVES

After going through this unit, you will able to:

- Define the terms cyber security
- Identify SSID
- Implementation of Encryption keys
- Understand the 802.11 IEEE wireless Standards
- Understand the wireless router
- Configure wireless router, WLAN

2.2 INTRODUCTION

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. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1999, which was outdated 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 over WEP.

Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks. As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

2.3 SERVICE SET IDENTIFICATION (SSID)

Service set identification (SSID) a series of 0 to 32 octets. It is used as a unique identifier for a wireless LAN. Since this identifier must often be entered into devices manually by a human user, it is often a human-readable string and thus commonly called the "network name".

An SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other. A network administrator often uses a public SSID that is set on the access point and broadcast to all wireless devices in range. Some newer wireless access points disable the automatic SSID broadcast feature in an attempt to improve network security.

A common, albeit incorrect assumption, is that an SSID is a string of human-readable characters (such as ASCII), terminated by a NUL character (as in a C-string). SSIDs must be treated and handled as what they are, a series of 0 to 32 octets, some of which may not be human-readable. Note that the 2012 version of the 802.11 standard defines a primitive SSID Encoding, an Enumeration of UNSPECIFIED and UTF-8, indicating how the array of octets can be interpreted.

In an IBSS, the SSID is chosen by the client device that starts the network, and broadcasting of the SSID is performed in a pseudo-random order by all devices that are members of the network.

2.3.1 Security of SSID hiding

Every wireless router has the ability to broadcast its name, or SSID (Service Set Identifier). Disabling SSID broadcasting means that your wireless network won't appear in the list of "Available Wireless Networks" on any nearby computer. Theoretically, this makes your network more secure. Since your neighbors won't be able to see your network, how could they connect to it? Unfortunately, disabling the SSID does nothing to hide your wireless network from hackers using programs that scan the airwaves for wireless networks. In fact, it makes it look like you've got something to hide, much like putting an expensive purchase in the back of a hatchback and covering it with a blanket does. Additionally, disabling SSID broadcasting makes it harder to troubleshoot connection

problems, and also makes it difficult for your guests to connect to your wireless network. Using WPA with a complex password means your neighbors can see your network, but they can't access it.

Figure 18: SSID settings

1.

2.4 ENCRYPTION METHODS

Encryption is used to hide or mask the data being sent through wireless transmission there are several popular and widely used encryption method used now a days including WEP (Wire Equivalent Privacy),WPA (Wi-Fi Protected Access) and WPA2(Wi-Fi Protected Access 2).

2.4.1 WEP (Wire Equivalent Privacy)

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in 1997, its intention was to provide data confidentiality comparable to that of a traditional wired network. WEP, recognizable by the key of 10 or 26 hexadecimal digits, was at one time widely in use and was often the first security choice presented to users by router configuration tools.

WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1999, which was outdated in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP.

2.4.2 Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2)

Wi-Fi Protected Access (WPA) is a security standard that improves on older

security standards by authenticating network users and providing more advanced encryption techniques. Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two most common security protocol and security certification programs developed by the Wi-Fi Alliance to secure wireless computer network. 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 over WEP.

WPA become available in 2003 and was intended as an intermediate measure in anticipation of the availability of the more secure and complex WPA2. WPA2 become available in 2004.

A feature added to Wi-Fi, called Wi-Fi Protected Setup, allows WPA and WPA2 security to be bypassed and effectively broken in many situations. WPA and WPA2 security implemented without using the Wi-Fi Protected Setup feature are unaffected by the security vulnerability.

Wi-Fi Protected Access (WPA) is a specification of standard-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN system.

WPA offers the benefits Enhancement data security, robust key management, Data origin authentication and Data integrity protection.

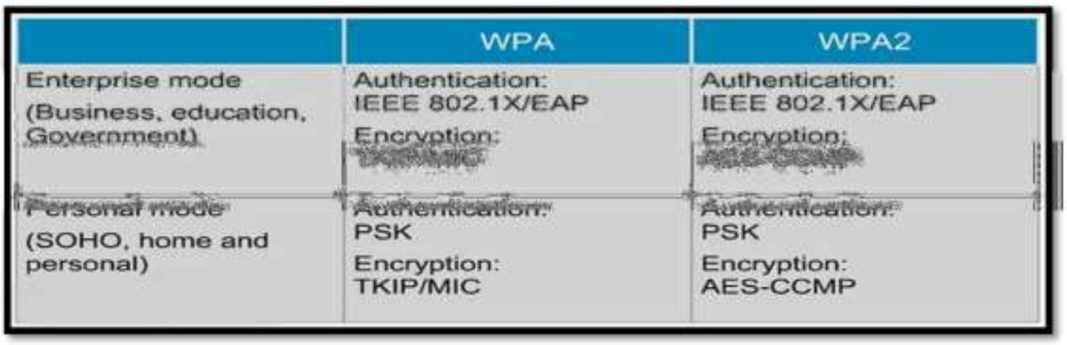
Difference between WPA & WPA2

WPA (sometimes referred to as the draft IEEE 802.11i standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2. WPA2 became available in 2004 and is a common shorthand for the full IEEE 802.11i (or IEEE 802.11i-2004) standard.

WPA and WPA2 Modes

WPA or Wi-Fi Protected Access leverages this authentication method of 802.1x plus EAP. It also supports pre-shared keys or PSKs. This defines two levels of authentication, one more suitable for enterprise environments, business, education, government which uses per user per session and authentication

keys obtained via the 802.1x EAP exchange. Another one which could be categorized as personal mode, more for home and personal use, which uses a Pre- Shared Key. It does not require the .1x EAP exchange and it can be set simply by configuring a pre-shared key manually.



	WPA	WPA2
Enterprise mode (Business, education, Government)	Authentication: IEEE 802.1X/EAP Encryption:	Authentication: IEEE 802.1X/EAP Encryption:
Personal mode (SOHO, home and personal)	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

Figure 19: Camparasion of WPA and WPA2

In WPA though, both modes would use WEP as the encryption algorithm and we know that is a vulnerable protocol and so some extra protection was built into WEP in the form of those two protocols, the Temporal Key Integrity Protocol and the Message Integrity Check, which basically added longer rotating keys and some integrity measures. Similar modes exist in WPA2, which is an implementation of Wi-Fi Alliance of the IEEE 802.11i standard. The main difference here is that WEP is no longer the encryption algorithm. The framework is still 802.1x EAP or pre-shared keys, but again the encryption algorithm is now AES or Advanced Encryption Standard.

2.5 MAC Filtering

In computer networking, **MAC Filtering** refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network.

While giving a wireless network some additional protection, MAC filtering can be

circumvented by scanning a valid MAC (via airodump-ng) and then spoofing one's own MAC into a validated one. This can be done in the Windows Registry or by using command line tools on a Linux platform. MAC Address filtering is often referred to as Security through obscurity. Unfortunately, using MAC Filtering may lead to a false sense of security. Also referencing to IP blocking.

MAC filtering is not an effective control in wireless networking as attackers can eavesdrop on wireless transmissions. However MAC filtering is more effective in wired networks, since it is more difficult for attackers to identify authorized MACs.

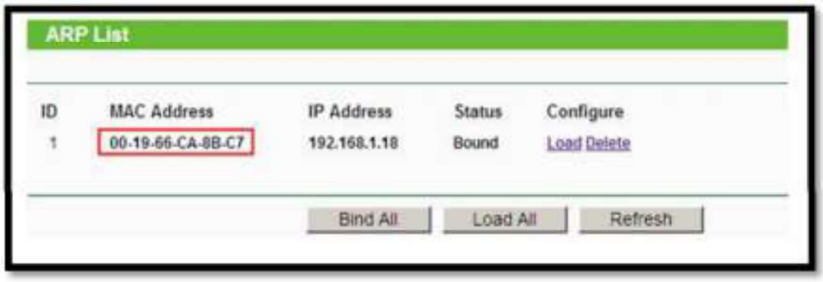
MAC filtering is also used on enterprise wireless networks with multiple access points to prevent clients from communicating with each other. The access point can be configured to only allow clients to talk to the default gateway, but not other wireless clients. It increases the efficiency of access to network.

2.5.1 Configuration of Wireless MAC address filter on wireless router

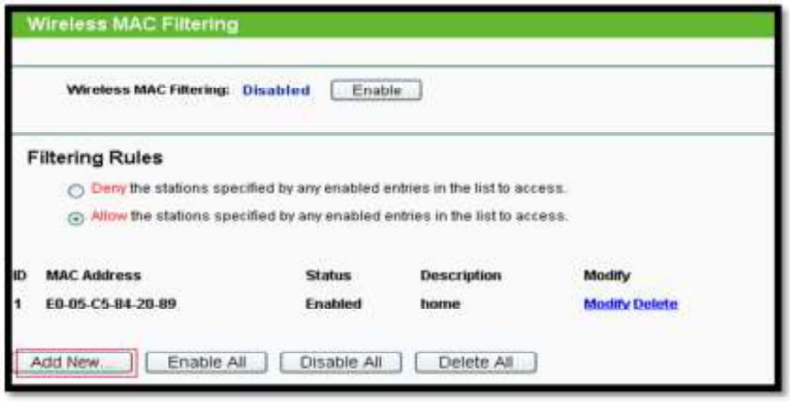
Step1: First step you need to open the web browser and then you have to type http://192.168.0.1or http://192.168.1.1 after that press enter. The user name and password are both “admin”

Figure 20: Configuring wireless router

Step 2: In the second step Go to IP & MAC Binding->ARP List page, you can find the MAC address of the all the devices which are connected to the router.

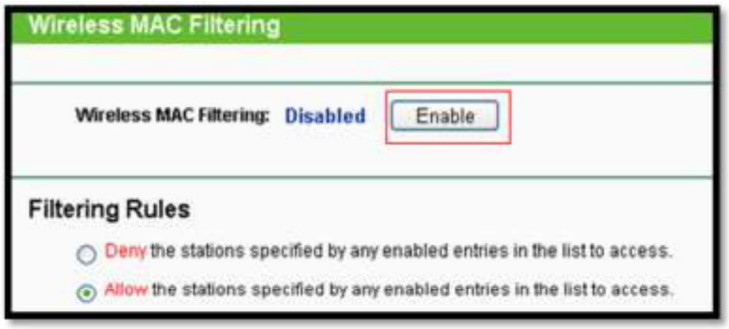


Step 3: In the third step Go to **Wireless->Wireless MAC Filtering** page, click the **Add New** button.



Step 4: In fourth step type in the MAC address you want to allow or deny to access the router, and give a description for this item. The status should be Enabled and at last, click the Save button. You need add items in this way one by one, 64 is the maximum number.

Step 5: In fifth step at the end, about the Filtering Rules, please choose Allow/Deny and Enable the Wireless MAC Filtering function.



2.6 WIRELESS ROUTER

A wireless router is the most important piece of equipment that allows the internet to work. The most popular wireless routers are ones with built in DSL or cable modems. Wireless routers are the main part transferring emails and signals coming across your Internet connection into a wireless broadcast, sort of like a cordless phone base station. It makes sure information goes to the right place. Wireless routers can be connected to the internet through a hard wire connection or a wireless connection. They make the internet much easier to use.

Although wireless routers have a lot of positives, there are some negatives. They can be very unsafe. People can have the ability to tap into your computer. You can prevent this by setting up security features. Firewalls, firmware, and other virus scanners are important to protect your wireless router.

Figure 21: Wireless Router

Radio Waves:

Wi-Fi uses radio waves like other wireless devices such as laptops and cellular phones, and radios. For the most part, to communicate with the wireless network, there is a two-way radio contact between computers. Because of this, the process that happens when wireless devices communicate via Wi-Fi is simple. First, the computer's wireless adapter changes its data to radio frequency and uses an antenna to send it out. Then, the computer's wireless router gets the signal and

translates it interprets the signal and sends the information to the internet using an Ethernet connection. That is the process to send information. To receive information, the process works in reverse.

Modem:

A modem is a device that converts the digital signals from a computer into specific frequencies that can travel to television or telephone lines. It transfers the information from the internet to the wireless router. At the destination point the receiving modem transfers the data that was sent back into data information. The modem allows the computer to translate information from one computer to another.

The modem can be either internal or external to the computer. Regardless if your cable modem is outside or inside the computer all modems have a few key components:

- A tuner- receiver of data
- A demodulator-changes signal into a simple signal which is processed by the convertor.
- A modulator- convert data into radio-frequency signals for transmission
- A media access control (MAC) unit- interface between hardware and the software of different protocols.

2.7 HOW TO CREATE A WIRELESS NETWORK

The following are four easy steps to create a wireless network:

Step 1: Choose your wireless equipment. You should have a wireless router and network adapter. The router converts the signals coming across your internet connection into a wireless broadcast. Make sure it is a wireless router and not a wireless access point. Network adapters wirelessly connect your computer to your wireless router. If you have a newer computer, you most likely already have a network adapter built in.

Computer networking is a great way to collaborate with other computer users in your home or office. While it is becoming increasingly easy for the basic computer user, it can still be a difficult, frustrating experience for many people.

Step 2: Second, connect your wireless router. Locate your cable modem or DSL modem and unplug it to turn it off. Next, connect your router to your modem. Next, plug in and turn on your cable or DSL modem. Wait a few minutes to give it time to

connect to the Internet, and then plug in and turn on your wireless router. Your computer will wirelessly connect to your router, and the router will send communications through your modem to the Internet. After a minute, the WAN or WLAN light on your wireless router should light up, indicating that it has been connected successfully.

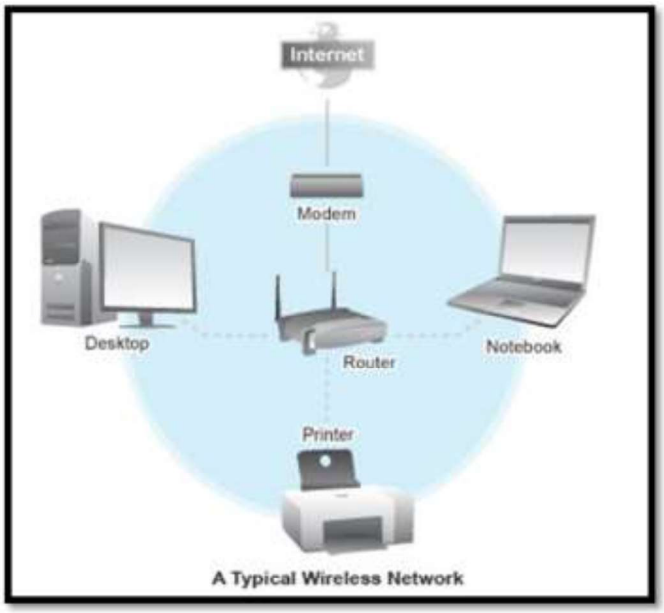


Figure 22: A typical Wireless Network

Step 3: Configure your wireless router. Using the network cable that came with your wireless router, you should temporarily connect your computer to one of the open network ports on your wireless router. If you need to, turn your computer on and it should automatically connect to your router. Next, open Internet Explorer and type in the address to configure your router.

Step 4: Connect your computers. If your computer does not have wireless network support built in, plug your network adapter into your USB port, and place the antenna on top of your computer (in the case of a desktop computer), or insert the network adapter into an empty PC card slot (in the case of a laptop). Windows XP will automatically detect the new adapter, and may require you to insert the CD that came with your adapter. The on-screen instructions will guide you through the configuration process.

Locate your cable modem or DSL modem and unplug it to turn it off. Next, connect your router to your modem. Next, plug in and turn on your cable or DSL modem.

Wait a few minutes to give it time to connect to the Internet, and then plug in and turn on your wireless router. Your computer will wirelessly connect to your router, and the router will send communications through your modem to the Internet. After a minute, the WAN or WLAN light on your wireless router should light up, indicating that it has been connected successfully.

2.8 CONFIGURATION OF WIRELESS ROUTER

1 **Step 1:** Plug the new wireless router into your internet connection point (filter/splitter if ADSL, directly into phone socket if DSL).

2 **Step 2:** If you have one, turn on your broadband connection and existing external modem FIRST (wait for all lights to return to normal).

3 **Step 3:** Plug the router into your PC with an Ethernet cable.

4 **Step 4:** Turn on your new wireless router Second.

5 **Step 5:** Go to your internet browser and type http://192.168.0.1/ (Belkin), http://192.168.1.1/ (Linksys), http://192.168.2.1/ (Others) and enter your username and password for your router (often this is "admin" for username and "admin" or "password" for password)

6 **Step 6:** Enable wireless capability (SSID) and enter your user name and password you got from your internet service provider.

7 **Step 7:** Choose WPA* (or WEP if your card cannot handle WPA) security and enter a passkey and write it down.

2.9 WLAN

A wireless local area network (WLAN) is a wireless computer network that links two or more devices using a wireless distribution method (often spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and still be connected to the network, and can provide a connection to the wider Internet. Most modern WLANs are based on IEEE 802.11 standards.

Figure 23: Wireless LAN

The other factors why WLANs are becoming more acceptable are:

1. No need to be connected physically with each other through any medium such as cables. You can roam around freely in office premises, home or around.
2. WLANs are cost effective. Cabling all the way in the offices, hotels etc. are not needed. So it's cheap and provide same quality of service.
3. Unreachable spots where a cable is hardly accessible, WLAN signals can reach out such as big installations like airports. Also surfing outdoors is also convenient. Just install the device called Access Points (AP) and you are done.
4. Less interruption and easy trouble shooting in case of failures as compared to cabled networks.
5. More secure as most of APs support best encryption methods which protect them from sniffing and other attacks.

2.9.1 Major issues with WLAN

WLAN are also as prone to various attacks as their counterpart wired LANs are. Actually WLANs are easier to hack as compared to wired LANs, if not properly configured, due to its easy accessibility around the installation. No need to be in contact of physical wires to hack, can be done from anywhere. Its convenience can turn into serious risk to the organization if not configured properly. Major attacks include such as, Sniffing, Key cracking, DoS (Denial of Service), De authentication attacks, War driving etc.

Secure WLAN

Wireless Security mainly depends on these 3 factors:

- How much is your wireless network secured in terms of encryption being used?
- Monitoring for suspicious and unusual activities.
- User awareness and education.

These are the combination of various approaches ranging from corporate to home networks. These are also for users how to remain safe while surfing.

Wi-Fi at home

Wi-Fi at home is not a luxury anymore it has become a necessity. However, when the question of security comes into the scene, the first thought that would arise in my mind is how you can protect something which you cannot see, neither can you feel it?

Protecting a home wireless network is altogether a different side of the coin as compared to wired networks. Most of wireless network device vendor's and Internet Service provider do not provide any security settings by default and leave the customer to find for herself. So make sure, your network is secured from being maliciously used. There is no silver bullet that will protect your wireless network infrastructure. These are, however, some countermeasures listed below that should be used in conjunction with each other to secure your wireless network to the highest level:

1. **Use most secure possible encryptio**n: The first and most necessary step- use industry standard encryptions. The old (however generally used) WEP-Wired Equivalent Privacy, has been known to be broken. Even you use complex passwords it can be broken and decrypted within minutes or hours. WEP uses 40 bit or 128 bits RC4 ciphers to encrypt the channel. Instead use secure protocols such as WPA 2 – Wi-Fi Protected Access -2, which uses strong 128 bits AES ciphers and is typically considered more robust encryption strategy available.
2. **Use Firewall:** All the wireless routers come with built-in firewalls. Enable them with all the security features. You should block any anonymous ping requests and place restrictions on website browsing, if required. Define additional security policies and apply them.
3. **Have a monitoring system in place:** There's a saying- prevention is better

than a cure. If you are able to detect some suspicious activities before it penetrates your network, you can block them or take precautionary measures. Deploy WIPS/WIDS for monitoring suspicious activities.

4. **Don't use default credentials:** Every wireless router comes with a set of default username/password. Sometimes, people don't change them and keep using them for long time. Username and passwords are used by computers or other devices to connect to wireless router. If any hacker is able to guess them, he can connect to your network easily. Studies show that majority of users use the same combination of username/passwords as set by manufacturers. Some default username combinations are: admin/admin, admin/password or admin/ " ".
5. **Disable Auto-connect feature:** Some devices or the computers/laptops have 'Let this tool manage your wireless networks' or 'Connect automatically to available network'. Such users having this auto-connect feature enabled are prone to Phishing attack or Rogue AP attack. Attackers keep their APs alive and kicking for such kind of unsuspecting users. They also use luring names as 'HotSpot', 'SecureConnect', 'Govt Networks' etc. The user will never suspect them and keep surfing the wireless network happily. Also if you have not changed the default password of your router, the attacker will try to use this feature on their machine and automatically connect using the easily guessable default passwords.
6. **Don't use public Wi-Fi spots to surf sensitive websites:** Free and open wireless networks available on airports, cafes, railway stations are not very secure by nature. They do not use any encryption to secure the channel between your laptop to the router. So any information which is not by default going on HTTPS from your laptop/smart phone is susceptible to sniffing and even more your session could be hijacked because the unencrypted channel may leak the active session ID used by your website. All the attacker needs to do is to just install this tool in Firefox and start sniffing the communications on a public unencrypted Wi-Fi. Some applications like Facebook encrypts the login page [HTTPS] but internal pages are served on unencrypted [HTTP] channel so your session ID can be leaked
7. **Change the default SSID:** Although this will not prevent hackers breaking into a network, using a default SSID acts as an indication that the user is careless. So

he may be an obvious target to explore further to see if he still uses the default passwords as well?

8. **Restrict access by assigning static IP addresses and MAC filtering:** Disable automatic IP assigning feature and use private static IPs to the legitimate devices you want to connect. This will help you in blocking unwanted devices from being connected to your network. Also, enable MAC filtering- router remembers MAC of each and every device connected to it and saves it as list. You can use this facility to restrict access. Only a set of trusted devices can be allowed to connect. However MAC spoofing is still possible but it raises an extra bar for your wireless network.
9. **Turn off your router when not in use:** Last but not least, a little obvious, but it will save your network from all the attacks for that time period.

2.10 LET US SUM UP

1. Wireless security is the prevention of unauthorized access or damage to computers using wireless networks.
2. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks.
3. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.
4. Service set identification (SSID) a series of 0 to 32 octets. It is used as a unique identifier for a wireless LAN. Since this identifier must often be entered into devices manually by a human user, it is often a human-readable string and thus commonly called the "network name".
5. Every wireless router has the ability to broadcast its name, or SSID (Service Set Identifier). Disabling SSID broadcasting means that your wireless network won't appear in the list of "Available Wireless Networks" on any nearby computer.
6. Encryption is used to hide or mask the data being sent through wireless transmission.
7. WEP is a notoriously weak security standard. The password it uses can

often be cracked in a few minutes with a basic laptop computer and widely available software tools.

8. WPA offers the benefits Enhancement data security, robust key management, Data origin authentication and Data integrity protection.
9. In computer networking, **MAC Filtering** refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network.
10. MAC filtering is not an effective control in wireless networking as attackers can eavesdrop on wireless transmissions.
11. A wireless router is the most important piece of equipment that allows the internet to work.
12. Wi-Fi uses radio waves like other wireless devices such as laptops and cellular phones, and radios
13. A modem is a device that converts the digital signals from a computer into specific frequencies that can travel to television or telephone lines.
14. A wireless local area network (WLAN) is a wireless computer network that links two or more devices using a wireless distribution method (often spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, or office building.
15. WLAN are also as prone to various attacks as their counterpart wired LANs are.

2.11 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Fill in the blank

I. WPA2 uses an……device that encrypts the network with a 256-bit key; the longer key length improves security over WEP.

II. WIPS stands for…….

III. Wired Equivalent Privacy (WEP) is a security algorithm for……. wireless networks.

IV. Service set identification (SSID) a series of 0 to……octets.

V. MAC addresses are……...assigned to each card.

VI. A wireless router is the most important piece of equipment that allows the…….to work.

VII. A modem is a device that converts the……. from a computer into specific frequencies that can travel to television or telephone lines

Answers:

I. Encryption

II. Wireless Intrusion Prevention Systems

III. IEEE 802.11

IV. 32

V. Uniquely

VI. Internet

VII. Digital signals

2.12 ASSIGNMENTS

1. What is wireless Security?
2. What is SSID? How do you disable SSID? Write step for that?
3. What is WEP, WPA and WPA2?
4. What is the difference between WPA and WPA2?
5. What are WPA and WPA2 Modes?
6. What is MAC filtering? How configure MAC address on wireless router.
7. What are 802.11 IEEE wireless Standards?
8. What is wireless router? How to create wireless network? Write steps for that.
9. How to configure wireless router? Write steps for that.
10. What is WLAN? What are major issues with WLAN?
11. What is firewall? Explain.

Unit 3: Investigation and Digital Forensic

3

Unit Structure

3.1 LEARNING OBJECTIVE

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

- Define the meaning of word cyber and cyber crime
- Know the basics digital forensic
- Know various types of forensic investigation techniques
- Know the steps involved in forensic investigation
- Study about various forensic tools
- Define how the email works
- Differentiate between various protocols like SMTP, POP3,IMAP, etc
- Study different types of email abuses
- Perform fake emails and their senders investigation
- Recognize scams or hoax emails and websites
- Perform social media profile investigation

3.2 INTRODUCTION

Welcome to the Post-PC Era, the era dominated by truly portable devices with embedded GPS, near-field communication capabilities, microphones and HD video cameras and processing power equal to or greater than traditional computers[30]. We 'wear' our computers, we are empowered. Our dependency on cyber space grows by the day, our access points and networked devices are legion, and our cyber security systems are losing their foothold. Passwords, firewalls, security keys, encrypted memory sticks: traditional security measures no longer fully address the many sophisticated new challenges we face. To guarantee security and trustworthiness of data, industry, governments, businesses and citizens are to align their behaviors and interests to secure the growing digital-based economy and society. But what are the drivers behind this new cyber reality?

[30] http://cybersecuritymanifesto.com/

3.2.1 Drivers behind this new cyber reality?

a. *The rise of bring your own device (BYOD):* Employees are bringing their own tools to work – whether hardware, software or application. Information is on the move. The boundaries between "Internet at home" and "Internet at work" are quickly eroding with the advent of the ambient web: the Internet is always there and always on, connected to the devices and systems of your own choosing, whether you are aware of it or not. The overlap of professional and private lives raises new challenges for security: who secures your data, who is in control and from where?

b. *An increasing reliance on cloud services:* Cloud computing is still in an infancy stage, but a fundamental component of IT services orientation and consumerization, heralding new avenues for producing, sharing and managing information. A truly globalized phenomenon, cloud computing is characterized by a services approach to satisfy the technology needs of organizations and individuals alike. Such is the new model in and for the IT-industry. Through this "hyper outsourcing", information and processes move beyond the company walls.

c. *The Internet of things will accelerate operational dependency on the net*: When all kinds of physical devices contain embedded networked software paving the way for 'the Internet of things' and so-called 'smart cities', cyber security becomes even more critical. The unique identification of citizens and objects in the virtual space may be some way off, yet we must still be prepared. The creation of an interconnected world and an ambient network will automatically create new possibilities for information breaches, system attacks and privacy violations.

d. *The increasing sophistication of hackers, supported by advanced tools, will turn complex attacks into a simple click of a button:* Amateurs turn professional, and the tools they use evolve accordingly – such is the common pattern to any popular and lucrative activity. The greater our dependency on the Internet and the more value we create from it, the smarter and more agile cyber attackers get. At the same time, hacking itself is becoming a commodity. For next to nothing you can buy the necessary tools for reading the SSID's of the wireless routers within 3km radius of you.

e. *Regulatory constraints exercise a growing influence on information security:* Protecting the interest of data stakeholders, be they clients, shareholders or private or public companies, is a raising issue for the regulators worldwide. For instance, communication about cyber attacks consequences will soon be legally binding and will lead organizations to ensure full transparent cyber security risk management. There is also increasing pressure on companies accepting credit cards payments to have their information system architecture certified by a third party, according to a standard (Payment Card Industry Data Security Standard) and to conduct penetration test campaigns with a frequency depending on payments volume.

3.2.2 Cyber Crime and Challenges Ahead

The word “cyber” is derived from the Greek term “cybernetic” meaning “skilled in steering or governing”. Securing the virtual space and protecting networked assets, is of critical importance now that digital goods and services permeate all levels of the economy and civil society. The growing importance of this space for business and our personal lives requires that we take all necessary measures to secure it.

With the growing incidence of cyber crime, and the increased adoption of digital devices, digital forensics has gained significant importance in the recent past, augmenting what was conventionally limited to the recovery and analysis of biological and chemical evidence during criminal investigations[31].

3.3 INVESTIGATION TECHNIQUES & COMPUTER FORENSICS

Forensics[32] is a discipline that dates back at least to the Roman era (and possibly event to ancient China), when people accused of crimes (and the accuser) presented evidence in front of a public audience (the Latin word forensics, means "of or before the forum"). In modern times it has come to mean the application of scientific processes to recover evidence related to

[31] http://opensourceforu.efytimes.com/2011/03/digital-forensic-analysis-using-backtrack-part-1/

[32] https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics/A_history

crime or other legal action.

3.3.1 Digital Forensics System

Digital forensics, as a discipline, grew out of the explosion in personal computer use during the late 1970s and early 1980s. The first specific computer crimes were recognized in the 1978 Florida Computer Crimes Act, which included legislation against the unauthorized modification or deletion of data on a computer system. Over the next few years the range of computer crimes being committed increased and laws were passed to deal with issues of copyright, privacy/harassment and child pornography.

It was not until the 1980s that federal laws began to incorporate computer offences. Canada was the first country to pass legislation in 1983. This was followed by the US Federal Computer Fraud and Abuse Act in 1986, Australian amendments to their crimes acts in 1989 and the British Computer Abuse Act in 1990.

Much of the forensic analysis during this period was performed on "live" systems, using traditional (and non-specialist) system administration tools. Very few standards or guidelines existed to help practitioners, and the evidence they produced was often rejected by courts.

Digital forensics is traditionally associated with criminal investigations and, as you would expect, most types of investigation centre on some form of computer crime. This sort of crime can take two forms; computer based crime and computer facilitated crime.

3.3.1.1 Computer based crime

This is criminal activity that is conducted purely on computers, for example cyber-bullying or spam. As well as crimes newly defined by the computing age it also includes traditional crime conducted purely on computers (for example, child pornography).

3.3.1.2 Computer facilitated crime

Crime conducted in the "real world" but facilitated by the use of computers. A classic example of this sort of crime is fraud: computers are commonly used to communicate with other fraudsters, to record/plan activities or to create fraudulent documents.

Not all digital forensics investigations focus on criminal behaviour; sometimes the techniques are used in corporate (or private) settings to recover lost information or to rebuild the activities of employees.

3.4 TYPES OF INVESTIGATION

There are four main types of investigation performed by digital forensics specialists. The first three are broadly similar in the activities involve, but differ in terms of the legal restrictions and guidelines imposed as well as the type of digital evidence and form of report.

3.4.1 Criminal forensics

The largest form of digital forensics and falling under the remit of law enforcement (or private contractors working for them). Criminal forensics is usually part of a wider investigation conducted by law enforcement and other specialists with reports being intended to facilitate that investigation and, ultimately, to be entered as expert evidence before the court. Focus is on forensically sound data extraction and producing report/evidence in simple terms that a lay man will understand.

3.4.2 Intelligence gathering

This type of investigation is often associated with crime, but in relation to providing intelligence to help track, stop or identify criminal activity. Unless the evidence is later to be used in court forensic soundness is less of a concern in this form of investigation, instead speed can be a common requirement.

3.4.3 Electronic discovery (eDiscovery)

Similar to "criminal forensics" but in relation to civil law. Although functionally identical to its criminal counter part, eDiscovery has specific legal limitations and restrictions, usually in relation to the scope of any investigation. Privacy laws (for example, the right of employees not to have personal conversation intercepted) and human rights legislation often affect electronic discovery.

3.4.4 Intrusion investigation

The final form of investigation is different from the previous three. Intrusion investigation is instigated as a response to a network intrusion, for example a

hacker trying to steal corporate secrets. The investigation focuses on identifying the entry point for such attacks, the scope of access and mitigating the hackers activities. Intrusion investigation often occurs "live" (i.e. in real time) and leans heavily on the discipline of network forensics.

3.5 EVIDENCE AND ANALYSIS

Obviously the main aim of any investigation is to recover some form of digital evidence, objective data that is relevant to the examination. On top of that the investigator might be asked to make some form of analysis of that evidence; either to form an expert conclusion, or to explain the meaning of the evidence. Here are some examples of the kind of analysis an examiner might be asked to undertake:

3.5.1 Attribution

Meta data and other logs can be used to attribute actions to an individual. For example, personal documents on a computer drive might identify its owner.

3.5.2 Alibis and statements

Information provided by those involved can be cross checked with digital evidence.

3.5.3 Intent

Intent as well as finding objective evidence of a crime being committed, investigations can also be used to prove the intent (known by the legal term mens rea).

3.5.4 Evaluation of source

File artifacts and meta-data can be used to identify the origin of a particular piece of data. for example, older versions of Microsoft Word embedded a Global Unique Identifer into files which identified the computer it had been created on. Proving whether a file was produced on the digital device being examined or obtained from elsewhere (e.g., the Internet) can be very important.

3.5.5 Document authentication

Related to "Evaluation of Source", meta data associated with digital documents can be easily modified (for example, by changing the computer clock you can

affect the created date of a file). Document authentication relates to detecting and identifying falsification of such details.

3.6 STEPS IN FORENSICS INVESTIGATION

A digital forensic investigation generally consists of five steps:

1. Identification: Identify the system to be investigated.
2. Data acquisition/data preservation: taking images of the drives/partition belonging to the identified system.
3. Data recovery: recover deleted data from the image file.
4. Analysis: of data for evidence: analyze digital artefacts inside the data for evidences.
5. Reporting: of the digital evidence found: reporting of evidences found during analysis phase.

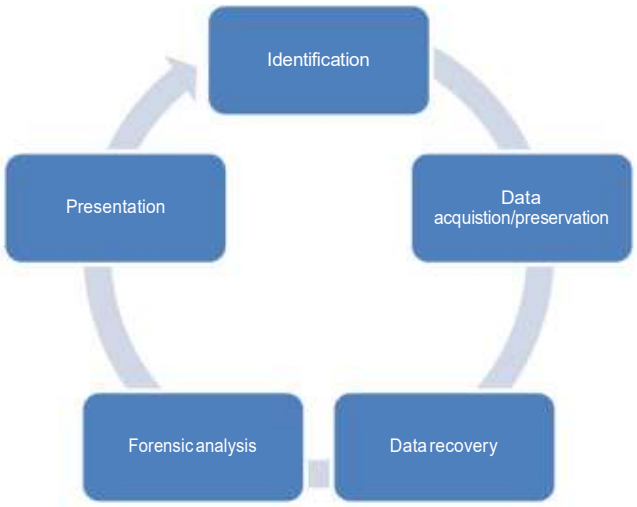


Figure 24: Digital forensic investigation process

3.7 FORENSICS TOOLS

In the early days of digital forensics analysts had to make do with existing system administration or information security tools. Plenty of these existed, but they were not particularly suited to the more formal approach of a forensic investigation. In particular much of the software required you to run it on the live system, which introduced all manner of problems with modifying evidence.

During the 1980s and 90s, however, increased funding and interest in the field encouraged the development of a variety of specialist commercial and freeware

tools. These can generally be broken down into three categories:

- **General forensic tools:** Tools allowing a wide variety of investigation, particularly keyword searching, on digital media.
- **Specialist forensic tools:** Which focus on a specific piece of forensic material for investigation - perhaps images, or internet artifacts. Often relying on output from one of the general tools.
- **Case Management tools** These are used to track, audit and report on cases

In addition there is a "fourth" category of useful software, a normal piece of software which can usefully be adapted for use in a forensic investigation. The next section makes mention of several commercial tools. This is not an endorsement of the tools, they are intended to serve as examples to explore

3.7.1 General forensic tools

Many of these tools are complex, commercially produced, and come with enterprise price tags (in the region of thousands of dollars a year). The majority of commercial tools run on Windows whilst free tools tend to run on Linux. Later on we will discuss the ways digital media can be investigated in more depth, but for the moment it is important to understand that general forensic software is usually centred around the act of keyword searching across a piece of digital media. The two most common ways of performing such searches is "live search" (where the digital media is parsed for a set of keywords and bookmarks of hit locations is stored) and "indexing" (where a text index of the digital media is created, allowing searches to be performed quickly using the index). Both styles have advantages and disadvantages.

The "de facto" industry standard tool is usually considered to be EnCase, produced by Guidance Software. It is a general forensics tool tailored for windows systems and focuses on the live search method. It includes a scripting interface, dubbed EnScript, which is useful for developing custom tools to extract information. EnCase is closely followed by Access Data's Forensic Toolkit (or FTK). FTK focuses on indexing media and is often used in cases where large volumes of data are being investigated, or where a large list of keywords needs to be searched.

3.7.2 Specialist forensic tools

Specialist tools focus on a particular aspect of forensic investigation; for example categorising images or recovering internet artefacts. The range of tools and software is vast, including commercial and free offerings.

One of the better known is a free tool called "Categoriser 4 Pictures" which is a helper tool for classifying images and presenting your results. C4P is a class of tool that relies on output from EnCase, using an EnScript to parse and extract images for processing.

Another common theme for specialist tools is internet artefacts; this can range from recovering internet cache data (web pages and other fragments) to analysing internet history or recovering chat transcript. Internet artefacts often contain a large amount of useful evidence and it is a common focus for investigations. Some notable tools include:

- *Netanalysis*; commercial tool, parses internet history files (.dat) and allows searching/analysis of the data.
- *Internet Evidence Finder*; commercial, scans digital media for a variety of internet artefacts (i.e. chat, webmail and internet history)
- *Virtual Forensic Computing*; allows digital media containing an operating system to be mounted as a virtual machine.

3.7.3 Case management

We already touched on case management in "Documenting evidence", but it is included here for completeness. Very few (if any) software tools exist for complete case management (although some practitioners adapt case management tools from the law field). Several free cases note tools exist for creating audit-able notes; the primary example being CaseNotes. Many analysts still use paper documents, partly because this is an audit trail that courts understand and accept!

3.7.4 Useful software

A wide variety of tools exist that are adaptable for forensic investigation; system administration tools, for example, can often tell you a lot about a system. VMWare is a commercial/free tool that can be used to view digital media as virtual machines. VLC media player can be useful for handling a diverse

collection of media.

3.8 INVESTIGATION

Today, nearly all abusive e-mail messages carry fake sender addresses[33]. The victims whose addresses are being abused often suffer from the consequences, because their reputation gets diminished and they have to disclaim liability for the abuse, or waste their time sorting out misdirected bounce messages.

You probably have experienced one kind of abuse or another of your e-mail address yourself in the past, e.g. when you received an error message saying that a message allegedly sent by you could not be delivered to the recipient, although you never sent a message to that address.

Sender address forgery is a threat to users and companies alike, and it even undermines the e- mail medium as a whole because it erodes people's confidence in its reliability. That is why your bank never sends you information about your account by e-mail and keeps making a point of that fact.

In the following sections we will touch upon how email works and techniques to find fake email. But before that, we are going to introduce some important terminologies which we are going to use throughout.

3.8.1 Some important terminologies

1. **Protocol:** Protocols are the set of rules and procedures governing the transmission of data over network.
2. **Internet Domains:** Internet domain names are the alphanumeric identifiers we use to refer to hosts on the Internet, like "LivingInternet.com". Internet domain names come in four main types[34]:

   - top-level domains
   - second-level domains
   - third-level domains, and
   - country domains.

[33] http://www.openspf.org/Introduction

[34] http://www.livinginternet.com/e/ew.htm

a. **Top-level domains**. Internet domain names are organized by their levels, with the higher levels on the right. For example, for the domain "mail.twenty.net" the top- level domain is "net", the second-level domain is "twenty.net", and the third-level domain is "www.twenty.net". Some of the popular top level domain names are .com, .net, .biz, .gov. etc/

b. **Second-level domains.** Top-level Internet domains like ".com" are shared by all the organizations in the domain. Second-level domain names like "yahoo.com" and "livinginternet.com" are registered by individuals and organizations. Second- level domains are the addresses commonly used to host Internet applications like web hosting and email addressing.

c. **Third-level domains.** Third-level Internet domain names are created by those that own second-level domains. Third-level domains can be used to set up individual domains for specific purposes, such as a domain for web access and one for mail, or a separate site for a special purpose:
   - www.livinginternet.com
   - mail.livinginternet.com

d. **Fourth-level domains:** Fourth-level domains and even higher Internet domains like "www2.un.news.media.twenty.net" can be also be established. Three of four levels is usually sufficient for most purposes. Each country in the world has its own top-level Internet domain with a unique alphabetic designation, known as country domains. A few countries and example domains are: .ae for United Arab Emirates, .in for India, .au for Australia, .us for United States, etc.

3. **The Domain Name System (DNS):** DNS as a whole consists of a network of servers that map *Internet* domain names like www.livinginternet.com to a local *IP addresses*. The Domain Name System (DNS) servers distribute the job of mapping *domain names* to *IP addresses* among servers allocated to each domain. Each second-level domain must have at least one domain name server responsible for maintenance of information about that domain and all subsidiary domains, and response to queries about those domains from other computers on the *Internet*. For example, management of domain name information and queries for the LivingInternet.com domain is handled by a

specific DNS server that takes care of the load required. This distributed architecture was designed to enable the Internet to grow, where as the number of domains grew, the number of DNS servers can grow to keep pace with the load. Today, everyone who registers a second-level domain name must at the same time designate two DNS servers to manage queries and return the current IP address for addresses in that domain. The primary domain name server is always consulted first, and the secondary domain name server is queried if the primary doesn't answer, providing a backup and important support to overall Internet reliability.

When your computer tries to access a domain like "www.livinginternet.com", the domain name system works like this:

- Your computer asks your default DNS server if it knows the IP address for www.livinginternet.com. If the DNS server has been asked that question recently, then it will have the answer stored in its local cache, and can answer immediately.
- Otherwise, your DNS server queries the *central zone files* for the address of the primary domain name server for livinginternet.com, and is answered with something like "ns1.livinginternet.com".
- Your DNS server will ask the livinginternet.com DNS server for the IP address of www.livinginternet.com, which will then look up the answer and send it back.
- Your DNS server will store the IP address returned in its local cache, and make the address available to your computer.
- Your computer then contacts www.livinginternet.com with the standard Internet routing protocols by using the returned IP address.

4. **Email servers:** Each Internet *domain* has an associated *email server* that manages all email addresses at that domain. Each email address is expressed in the form "name@domain" and is unique at that domain, as in for example "jane@twenty.net".
5. **IP Address:** Every computer on the *Internet* has a unique numerical address, called an Internet Protocol (IP) address, used to route packets to it across the Internet. Just as your postal address enables the postal system to send mail

to your house from anywhere around the world, your computer's IP address gives the Internet *routing* protocols the unique information they need to route *packets* of information to your desktop from anywhere across the Internet. If a machine needs to contact another by a *domain name*, it first looks up the corresponding IP address with the domain name service. The IP address is the geographical descriptor of the virtual world, and the addresses of both source and destination systems are stored in the header of every packet that flows across the Internet. You can find your IP address on a Windows computer by opening an MSDOS or Command window and typing one of "winipcfg" or "ipconfig". You can find your IP address on a Mac computer by checking your Network control panel. An IP address is made up of four bytes of information (totaling 32 bits) expressed as four numbers between 0 and 255 shown separated by periods. For example, your computer's IP address might be 238.17.159.4, which is shown below in human-readable decimal form and in the binary form used on the Internet.

Example IP Address	
Decimal:	238 . 17 . 159 . 4
Binary:	11101110 00010001 10011111 00000100

Each of the four numbers uses eight bits of storage, and so can represent any of the 256 numbers in the range between zero (binary 00000000) and 255 (binary 11111111). Therefore, there are more than 4 billion possible different IP addresses in all:

$$4{,}294{,}967{,}296 = 256 * 256 * 256 * 256$$

6. **Email client:** Your *email client* application communicates with an email server *over* the *Internet* to login, get mail status, and send and receive email. The most common email client are Internet Explorer, Morzila, Crome, etc.
7. **POP3:** Your email client talks to your email server to send it commands to login, get mail status, and send and receive email. The most common protocol used by email clients to communicate with email servers is the Post

Office Protocol. POP3 has become the most common email client connection protocol. The POP3 protocol enables any email program anywhere on the Internet to connect to any email server to perform the usual email functions, such as reading and sending, as long as they have a valid account and password.

8. **The Internet Message Access Protocol (IMAP):** is a less common but more richly featured email protocol than POP3. IMAP is a more modern protocol than POP3, first invented at Stanford University in 1986. The current version is IMAP4, providing similar services to the POP3 protocol, but with additional features. The IMAP features can be useful in several situations, for example when you are travelling and don't want to download your email onto a laptop because then you won't have them on your home computer when you get back. It can also be useful for use on low-bandwidth devices like personal digital assistants, enabling you to select a few email from a list of subject headers before downloading just the ones you want.
9. **Messaging Application Programming Interface (MAPI)**: is a Microsoft Windows specific email interface.
10. **Simple Mail Transfer Protocol** (**SMTP**): is an Internet communication protocol used to send and relay an email message between email servers. It is not used to retrieve email messages from a server. Instead either IMAP or POP is used to retrieve email messages.

3.9 HOW EMAIL WORKS

Email is based around the use of electronic mailboxes[35]. When an email is sent, the message is routed from server to server, all the way to the recipient's email server. More precisely, the message is sent to the mail server tasked with transporting emails (called the **MTA**, for *Mail Transport Agent*) to the recipient's MTA. On the Internet, MTAs communicate with one another using the protocol SMTP, and so are logically called **SMTP servers** (or sometimes *outgoing mail servers*).

The recipient's MTA then delivers the email to the incoming mail server (called

[35] http://ccm.net/contents/116-how-email-works-mta-mda-mua

the **MDA**, for *Mail Delivery Agent*), which stores the email as it waits for the user to accept it. There are two main protocols used for retrieving email on an MDA:

- POP3 (*Post Office Protocol*), the older of the two, which is used for retrieving email and, in certain cases, leaving a copy of it on the server.
- IMAP (*Internet Message Access Protocol*), which is used for coordinating the status of emails (read, deleted, moved) across multiple email clients. With IMAP, a copy of every message is saved on the server, so that this synchronization task can be completed.

For this reason, incoming mail servers are called **POP servers** or **IMAP servers**, depending on which protocol is used.

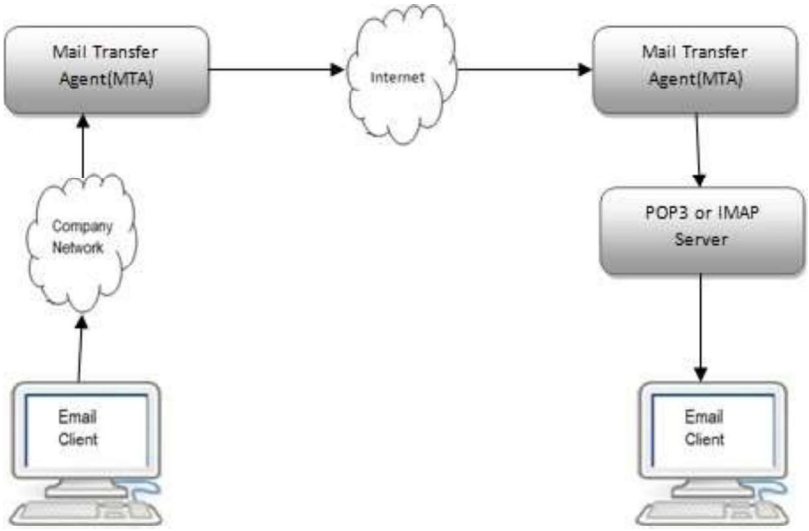


Figure 25: Working of an email

To use a real-world analogy, MTAs act as the post office (the sorting area and mail carrier, which handle message transportation), while MDAs act as mailboxes, which store messages (as much as their volume will allow) until the recipients check the box. This means that it is not necessary for recipients to be connected in order for them to be sent email.

To keep everyone from checking other users' emails, MDA is protected by a user name called a **login** and by a **password**.

Retrieving mail is done using a software program called an **MUA** (*Mail User Agent*).

When the MUA is a program installed on the user's system, it is called an **email client** (such as Mozilla Thunderbird, Microsoft Outlook, Eudora Mail, Incredimail or Lotus Notes).

3.10 COMMON TYPES OF E-MAIL ABUSE WHERE THE SENDER ADDRESS IS FORGED4

- **Spammers:** want to avoid receiving *non-delivery notifications (bounces)* to their real addresses.
- **Fraudsters:** want to cover their tracks and remain anonymous.
- **Computer worms:** want to cause confusion or just don't care about which sender addresses they use.
- **Phishers (password fishers):** want to impersonate well-known, trusted identities in order to steal passwords from users.

3.10.1 Sender Addresses in E-Mails

Like paper mail letters, e-mail messages have at least two kinds of sender addresses: one on the envelope and one in the letterhead.

- The ***envelope sender address*** (sometimes also called the *return-path*) is used during the transport of the message from mail server to mail server, e.g. to return the message to the sender in the case of a delivery failure. It is usually not displayed to the user by mail programs.

- The ***header sender address*** of an e-mail message is contained in the "From" or "Sender" header and is what is displayed to the user by mail programs. Generally, mail servers do not care about the header sender address when delivering a message.

3.10.2 Parts of an email

An email consists of three parts:

- Header
- Body
- Signature

An email structure is explained using the figure below.

Figure 26: Different parts of an email

The figure below explains the different fields of an email.

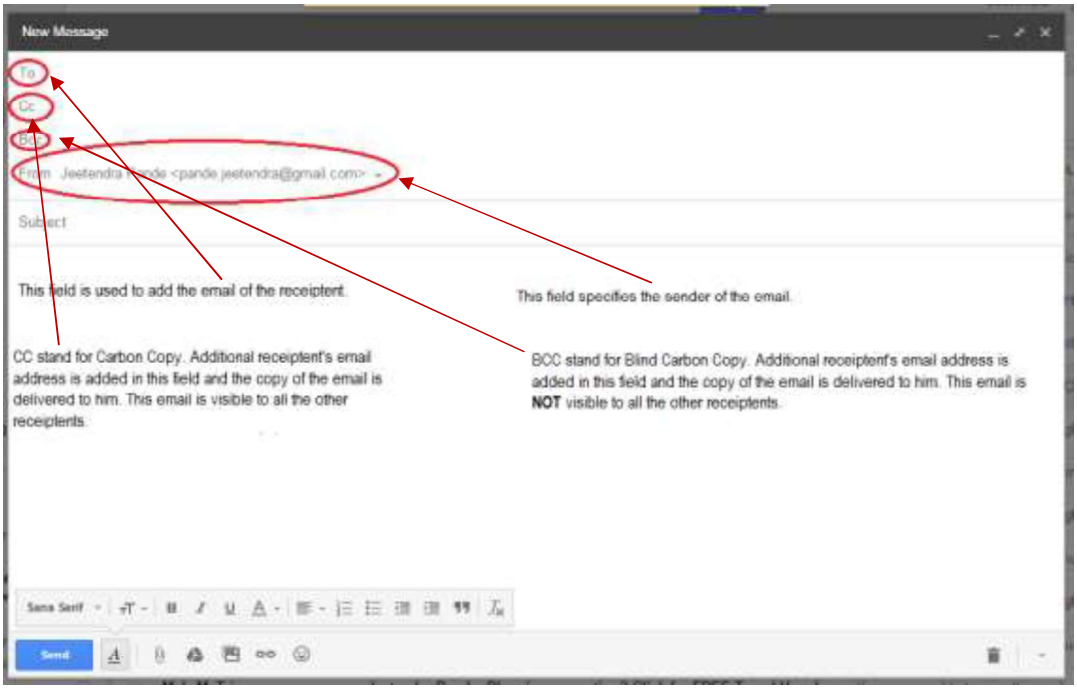


Figure 27: Fields of an email

One of the most important and useful applications of the internet is undoubtedly the sending and receiving of emails[36]. Apart from their almost instant nature

[36] http://codeworks.gnomedia.com/westhost-introduction/email-system-part-1-the-main-components/

they are also effectively free. Unfortunately this also makes email an ideal medium of abuse, in the sense that because it is free to send an email, it is also free to send a million emails. The major ISP's estimate that of the billions of emails being sent and receiving, about 50% of them are spam (or UCE – Unsolicited Commercial Email). For many people who have the same email address for a period of years, the amount of spam can be counted in thousands a day.

Then next section will discuss how to identify fake mails and procedure to identify the origin of a fake email.

3.10.3 How to Identify Fake EMail And Trace Sender's Location[37]

3.10.3.1 Fake Emails

Fake emails or fake mails are those emails which pretend to come from a specific email address but are sent from some fake email senders. It is not hard to send fake email address. Anyone can use those free fake email sender tools available online. These tools ask for the name and email of the sender which you want to show in the email.

Figure 28: A sample of fake email[8]

[37] http://www.usethistip.com/2012/11/how-to-identify-fake-email-and-trace.html

So you must know how to identify whether the email is fake or not.
See the sample email snapshot:

Figure 29:Sample spam email

See the sender's name and email. It's Mark Zuckerberg from email address mark@facebook.com.
This email is just an example. But these can be very harmful when sent by spammers. Suppose it pretends to be sent from your bank and asks for your banking username or password. There are so many examples which show why you must know about fake emails.

3.10.3.2 How to Identify Fake Email

It is really simple to identify a fake email. Click on the down arrow at the right side of the Me as shown in the snapshot.

Figure 30: Procedure to find out the details of the sender

You will see something like this:

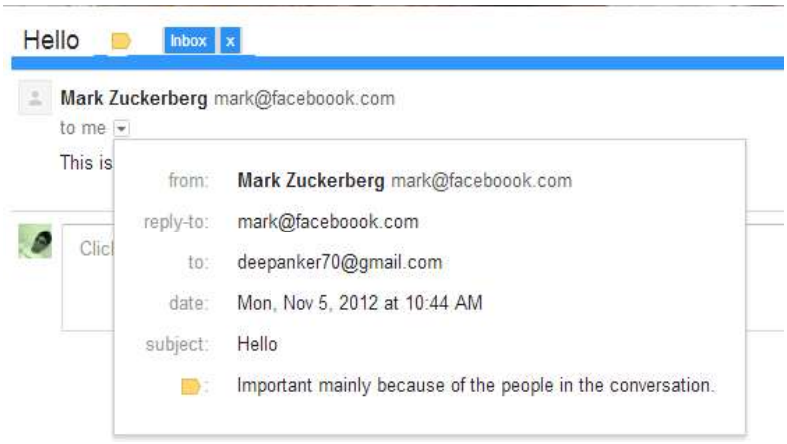


Figure 31: Finding sender's details

Here you will see some details about the email. If the email comes from a trusted source, you will be able to see two more fields, **Mailed By** and **Signed By**. See the snap below:

Figure 32: Investigating mailed by and signed by fields

This method can be applied only for the emails coming from big companies like Google, Facebook, LinkedIn, Twitter and other companies which have their own servers. Email sent from Gmail will be mailed by and signed by Gmail. But there are so many small companies that does not have dedicated server. They use Gmail labs or their own hosting server. Email coming from those may not show these two fields in mail. So we need to confirm this by one more way.

Now we will see the header of email. To see the header of email, click on down arrow at the right side of the reply icon and click on show original. Now it will open plain text email content with header information in a new tab.

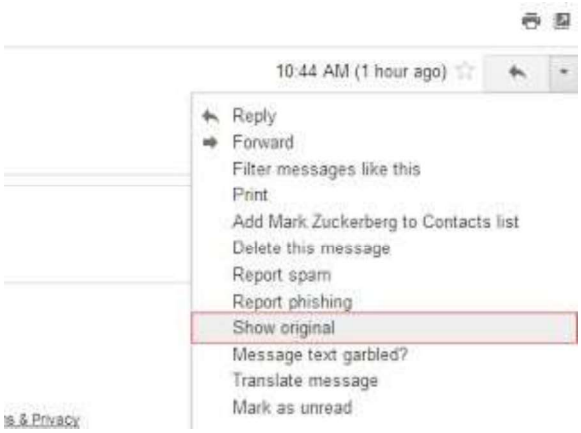


Figure 33: Procedure to find the headers of an email

Header information looks like this. Search for Received: from in this page. If there are more than one Received: from in the page, the go for the last one and see the domain there.

```
Delivered-To: deepanker70@gmail.com
Received: by 10.49.41.99 with SMTP id e3csp159879qel;
        Sun, 4 Nov 2012 21:14:39 -0800 (PST)
Received: by 10.14.172.195 with SMTP id t43mr32609652eel.17.1352092478680;
        Sun, 04 Nov 2012 21:14:38 -0800 (PST)
Return-Path: <mark@faceboook.com>
Received: from emkei.cz ([2a01:5e0:36:5001::21])
        by mx.google.com with ESMTP id k8si3491540eed.96.2012.11.04.21.14.37;
        Sun, 04 Nov 2012 21:14:38 -0800 (PST)
Received-SPF: temperror (google.com: error in processing during lookup of mark@fa
Authentication-Results: mx.google.com; spf=temperror (google.com: error in proces
Received: by emkei.cz (Postfix, from userid 33)
        id 9FCF5D5586; Mon,  5 Nov 2012 06:14:37 +0100 (CET)
To: deepanker70@gmail.com
Subject: Hello
From: "Mark Zuckerberg" <mark@faceboook.com>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: mark@faceboook.com
Reply-To: mark@faceboook.com
Content-Type: text/plain; charset=utf-8
Message-Id: <20121105051437.9FCF5D5586@emkei.cz>
Date: Mon,  5 Nov 2012 06:14:37 +0100 (CET)

This is just a friendly email to say "Hello"
```

Figure 34: Headers of an email

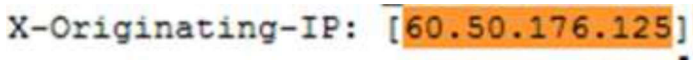
It shows emkei.cz in the fake mail sent by me. Now see the website **emkei.cz** and you will know that the domain belongs to a fake mail sender website.

If you see the header of some other emails, you will see that header comes with too many information which are not present in the header of this fake mail.

3.11 HOW TO TRACE LOCATION OF EMAIL SENDER

Email address can be traced or not. It depends on the mail server it has been sent. If the email is sent from Gmail using GMail web, you will never get the original IP address of the sender. Some other email servers (It may be a fake mail sender) also do not reveal the IP address of the sender in the email header. But in most of the cases (Other than sender is gmail) you can easily get the IP address of the person.

To get the IP address of the sender in the email header, search for **X-originating-IP:** and you will get the IP address of the sender.

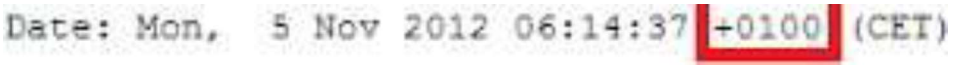


Now see the header of fake mail added above as snap by me, you will not find this field. It means it does not reveal the IP address of sender.If you get the IP address, now you can use any IP tracer online tool to get the IP address. Use WhatIsMyAddress Ip Lookup tool available at https://www.whatismyip.com/ip-address- lookup/

Note: If a person is using dialup connection with dynamic IP, IP Tracing will only trace up to the IP address of the ISP. For getting exact location, you need to contact ISP which is impossible without the permission of cyber police. If a person has purchased a dedicated IP connection, you will get the exact location of it.

3.11.1 What to do if IP is not there or Email is sent from Gmail

If you are not able to get the IP address of the person, At least you can know the country of the email. Search for Date: and at the end of line, see the time zone:



Here the time zone is +0100. Treat it as +01:00. Although, there will be so many countries belongs to a timezone, but you may get an approx idea.

3.12 RECOGNISE SCAM OR HIAX EMAIL AND WEBSITES[38]

Scam and hoax websites and emails are designed to:

- trick you into disclosing personal information such as bank account details, passwords or credit card numbers.
- con you into paying money for fake get-rich-quick offers, prizes or lottery wins, or fraudulent or poor quality goods.

[38] https://www.communications.gov.au/what-we-do/internet/stay-smart-online/your-identity/recognise- scam-or-hoax-emails-and-websites

Be suspicious of emails from people or businesses you don't know, particularly if they promise you money, good health or a solution to all your problems.

Be suspicious of unexpected emails from your bank or financial institution. Remember banks don't do business via email and never ask for confidential information via email. Scammers put a lot of time and money into making hoax emails and bogus websites look real. Don't be fooled.

3.12.1 Scams

There is a huge range of scams on the internet, from promises of non-existent free products in return for clicking through to a website (which make advertising profits), to sophisticated targeted scams which can run for years and cost victims hundreds of thousands of dollars.

Table 4: Some common scams

Scam	Delivery	Characteristics
419 or 'Nigerian letter' advance fee These messages are sent to thousands of people on the probability that some will believe the story and forward the advance fee.	Email (or letter) claiming to be from a solicitor, barrister, public official or some other authoritative person.	The writer is in another (usually underdeveloped) country. They own of a huge sum of money, but need the help of a foreign partner (you) in order to access it. Help them access the money and you will receive a share of it. You 'wire' them a small advance fee for some contrived reason (for example clearance fees, tax).

Dating and romance *They attempt to enter into an online relationship with the victim in order to persuade them to forward money or divulge personal details.*	*Fake profiles on dating sites or responding to profiles with fake personas* *A friend request or message in social media or a communications service such as Skype.*	*Their profile pictures look professional and might have been cut and pasted from a website or magazine.* They attempt to become intimate quickly. *They may say they live close by, but are unable to arrange a meeting or suddenly have to travel overseas.* *There are signs the correspondence might be cut and pasted or taken from template, for example wrong names, inconsistent or disjointed grammar.* *Requests for money accompanied by elaborate scenarios and effusive language.*

Generally, any offer that promises a large reward for a small fee is almost certainly a scam.

3.12.2 Steps to avoid online scams and hoaxes

Delete suspicious emails and leave websites that:

- ask you to provide your banking details or personal information promise you money
- present hard luck or exotic stories telling you that you can share in hidden millions of dollars
- offer jobs where you need no qualifications, but just ask for a bank account for money transfers.

3.12.3 Points to Remember

- Never provide personal details via emails or links from emails. If you are unsure, double check by telephone with the company or institution.
- Never follow the links in spam emails; these could lead to downloading unwanted viruses, spyware or malware.
- Ensure that you have up-to-date anti-virus and anti-spyware software installed on your computer.
- Install a firewall on your computer and make sure it is activated.

3.13 FAKE SOCIAL MEDIA PROFILE INVESTIGATION

There are social media platforms like facebook, twiter, etc. which are used to launch social engineering attacks, identity thefts, cyber stalking etc. So it is very important to identify fake social media profile to save yourself being a victim of such attacks. We will discuss investigating a fake social media profile in one of the most common social media platform, facebook in the next section.

3.13.1 How to spot fake facebook account[39]

1. **Know why it is important to spot a fake account:** First and foremost, somebody with a fake account is- almost by definition- a con artist. Unless you run with that crowd, you probably don't want them in your life.

- While they may present themselves as a friend, or even a romantic interest, their sole purpose in friending you may be as harmless as a mind game, or they may be after much more, such as your money, goods and property.
- The impostor might also be setting you up to steal your identity or valuable information from you that they can use to manipulate someone else.

2. **Don't talk to strangers.** At the least, think twice about accepting friend requests from people you don't know and who are not connected to you through legitimate, verifiable means. If you're not sure, do the following:

- Ask them questions: What makes you want to be your friend? How did they find out about you? Who do you know in common? By clicking on their name,

[39] http://www.wikihow.com/Reveal-a-Fake-Facebook-Account

you can see if you have any mutual friends. If you do, contact your friend. If not—that's a big red flag.

3. **Do a little detective work.** At the very least, it can be fun. You might also find out that your would-be "friend" is really bad news.

4. **Read the profile carefully.** Does what is being said add up or are there some really hard- to-believe statements being made? For example, maybe there is a photo of a very young person next to claims of being a professor or a CEO. Does the embellishment seem more than the usual "making oneself look good" and come across as simply implausible? Trust your own senses on this one. You could even ask for proof of some of the things the person has stated—they're approaching *you*, after all. You have every right to make sure they're legitimate.

5. **Check out their profile picture.** Is there only one? Is it way too perfect or does it seem touched up in any way? Maybe you've seen it before? A good photo — or a touched up one

— may not be a negative sign, but it could be that they've simple scoured Google for an attractive photo, thinking nobody would ever find out. Try this:

- Click and drag their profile picture to your desktop.
- Launch Google Chrome or Firefox, and navigate to Google Images.

Figure 35: Google Image search

- Drag and drop the profile pic into the search field: it will expand, as shown:

Figure 36: Searching image in google

- Google will either return an exact match (with information like names), or pictures similar to the original.

6. **Search their name online to see if it returns.** This won't be so useful if the name is a common one, but for a more unusual one there might be some interesting returns.
   - If they have a common name, add other information such as their location, approximate age, or any other information you can glean from their profile.
   - Have they been tagged? A real person is generally tagged here and there as part of the Facebook sharing experience.
7. **Check out their friends.** Are their friends global or local? The more local the friends, the more likely the person is to be real. The more global their friendship list, with very few or no local friends, start getting suspicious. The lack of local friends suggests that this is not a real person you're dealing with but a fake account. This is often used by people pretending to be attractive young women. They will often contact you with a line like "I saw your picture and you looked nice."
8. **Block the request.** If you don't have a good feeling about somebody, there's a simple solution: don't just turn down the request for friendship, block them completely.
   - Click on their Facebook name, and go to their Timeline. On the right, under the Cover Photo, click on the Message settings.

- You can block them from contacting you, or report them to Facebook if you feel they are a threat or involved in illicit or illegal activities.

9. **Create a "probationary period."** If you're in the (not-so-great) habit of accepting friend requests from friends of friends' friends, or friend people because they seem to have similar tastes to yours in music, cooking, dancing, or whatever, then you leave yourself open to the occasional fake.

- While you can make wonderful connections in this way, try to always have someone you do know vouch for this person first. And if that's not possible, be alert to signs of weird behavior, such as suddenly bombarding you with likes, comments, photos, etc. on a daily basis.
- If you hardly know this person, they should be taking things slowly and politely, not invading your space immediately.
- If, after a week or two, you're not comfortable with your new friend, unfriend them!

10. **Beware interconnected faking.** At one time it was probably reasonable to think that if someone had a group of friends interacting with them and vouching for each other, that that person must be real. Not anymore!

- There are increasing cases of one person running numerous fake Facebook accounts, pretending to be an array of different people, all vouching for one another and all trying to be friends with someone real!
- An excellent example is the case of Natalia Burgess, who wove a web of deceit and caused many young males to fall for her various aliases — all because she felt inadequately loved. Sadly, impostors of this sort go to incredible lengths to create an array of fake accounts including other social media accounts and websites to give the impression that their fake personas are "real".

11. **Look for and record inconsistencies.** If you're being targeted by an elaborate web of lies, eventually these start to unravel. This is most evident in someone who is trying to maintain several fake Facebook accounts at once and eventually, they will drop the ball and mix up their stories.

- If you start noticing this in response to questions, or in their comments, take note and remain alert for more inconsistencies.

12. **Do a double take if the person says anything weird or "out-of-character".** For example: if an adult is pretending to be a teen, they may say something that dates them by referring to a historic event or person that teens wouldn't really know much about. Or they may prove to know way too much about a topic that someone they're claiming to be would not.

- Take note of what the suspicious person says, as everyone slips up! No one is perfect, and they're bound to eventually say something that will give you a hint that your hunch is correct.

13. **Be really wary of undying declarations of** love**, affection, and romance.** If someone you've never met, who lives thousands of miles away from you, and who has barely revealed themselves gets amorous with you, be suspicious. Sometimes the faker does this because they love the feeling of playing with the life and feelings of someone else; sometimes it's because they're in love with online love but are too afraid to reveal their true selves (or they're in a relationship in real life); and other times it could be that they're after something, like money, sex, or drugs.
    - Question your own feelings and motivations if you start to feel something for a person who declares they love you online. Is it too sudden? Too weird? Too freaky? A little bit icky? Trust those feelings and delete this fake friend from your account.
    - If they ask you for sexy pictures, immediately be suspicious. A fake account is a good shill for getting free pornographic material that then gets passed around online.

14. **Unfriend them!** If you're suspicious, unsure, or uncomfortable with having them as part of your Facebook friends, pull the plug. It's not like they're your real friends or family, and they could cause you a lot of future problems.
    - Warn other friends of yours on Facebook if you know they have also friended the fake account; one of the tactics of an impostor is to befriend others in your circle of friends to try to make the friendship seem more "real

Tips

a. Be careful what you put online and what you tell people you don't really know. Some people act very caring until they have enough information about you and then they turn around and blackmail you with it. If you don't know the person, no matter how friendly you've become in the online context, keep back your private details and keep everything very general.

b. Look for evidence of offline interaction with their Facebook friends. However, keep in mind that even this can be faked if they're running multiple Facebook accounts.

c. Check any links they've provided to personal websites, social media pages, etc., to help you to see if things add up.

Warnings

a. Read How to Reveal a fake Facebook account if an impostor has stolen your own identity.

b. Keep an eye on your teens. Young people are the most vulnerable to building online relationships with people who don't exist. They fall in love with an image of the perfect person and the faker is happy to oblige for their own gratification or other reasons.

3.14 LET US SUM UP

1. The word “cyber” is derived from the Greek term “cybernetic” meaning “skilled in steering or governing”.
2. Forensics is a discipline that dates back at least to the Roman era (and possibly event to ancient China), when people accused of crimes (and the accuser) presented evidence in front of a public audience (the Latin word forensic, means "of or before the forum").
3. The first specific *computer crimes* were recognized in the 1978 Florida Computer Crimes Act, which included legislation against the unauthorized modification or deletion of data on a computer system.
4. Canada was the first country to pass legislation in 1983.
5. Computer based crime is a criminal activity that is conducted purely on computers, for example cyber-bullying or spam.
6. Computer facilitated crime is a crime conducted in the "real world" but

facilitated by the use of computers.

7. There are four main types of investigation performed by digital forensics specialists. They are criminal forensic, intelligence gathering, electronic discovery and intrusion investigation.
8. A digital forensic investigation generally consists of five steps viz. identification, data acquisition, data recovery, analysis and reporting.
9. Protocol are the set of rules and procedures governing the transmission of data over network.
10. You can find your IP address on a Windows computer by opening an MSDOS or Command window and typing one of "winipcfg" or "ipconfig".
11. The POP3 protocol enables any email program anywhere on the *Internet* to connect to any email server to perform the usual email functions, such as reading and sending, as long as they have a valid account and password.
12. IMAP is a more modern protocol than POP3.
13. The IMAP features can be useful in several situations, for example when you are travelling and don't want to download your email onto a laptop because then you won't have them on your home computer when you get back.
14. Spammers want to avoid receiving *non-delivery notifications (bounces)* to their real addresses.
15. Fraudsters want to cover their tracks and remain anonymous.
16. Computer worms want to cause confusion or just don’t care about which sender addresses they use.
17. Phishers want to impersonate well-known, trusted identities in order to steal passwords from users.
18. The envelope sender address is used during the transport of the message from mail server to mail server, e.g. to return the message to the sender in the case of a delivery failure.
19. The header sender address of an e-mail message is contained in the "From" or "Sender" header and is what is displayed to the user by mail programs.
20. Fake emails or fake mails are those emails which pretend to come from a specific email address but are sent from some fake email senders.

21. Use WhatIsMyAddress Ip Lookup tool available at https://www.whatismyip.com/ip- address-lookup/ to lookup the origin of an IP address.

3.15 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. State True and False

I. US was the first country to pass legislation for computer offence in 1983.
II. Child pornography is an example of computer facilitated crime.
III. Focus is criminal forensic on forensically sound data extraction and producing report/evidence in simple terms that a lay man will understand.
IV. Meta data and other logs can be used to attribute actions to an individual.
V. Data acquisition/data preservation is taking images of the drives/partition belonging to the identified system.
VI. Specialist forensic tools are used to track, audit and report on cases.
VII. Live search is a place where a text index of the digital media is created, allowing searches to be performed quickly using the index.
VIII. Netanalysis scans digital media for a variety of internet artefacts.
IX. Spammers want to impersonate well-known, trusted identities in order to steal passwords from users.
X. The envelope sender address is used during the transport of the message from mail server to mail server.

2. Fill in the blanks

i. BYOD stands for_____.
ii. PCIDSS stands for_____..
iii. _____is instigated as a response to a network intrusion.
iv. File_____and meta-data can be used to identify the origin of a particular piece of data.
v. C4P stands for_____.
vi. MTA stands for_____.

Answers:

1. State true or False

   i. False
   ii. False
   iii. True
   iv. True
   v. True
   vi. False
   vii. False
   viii. False
   ix. False
   x. True

2. Fill in the blanks

   i. Bring Your Own Device.
   ii. Payment Card Industry Data Security Standard.
   iii. Intrusion investigation
   iv. Artefacts
   v. Categoriser 4 Pictures.
   vi. Mail Transport Agent.

3.16 ASSIGNMENTS

1. What are the drivers behind this new cyber reality?
2. What do you mean by cyber?
3. What are the two forms of cyber crime?
4. There are the main types of investigation performed by digital forensics specialists
5. Explain some examples of the kind of analysis an examiner might be asked to undertake.

6. Explain the various steps involved in digital forensic investigation.
7. What are the three broad categories into which the forensic tools are categorized into?
8. What is “ live search”?
9. What are internet domains?
10. What is the difference between POP3 protocol and IMAP protocol. Which is better?
11. What is an IP address.
12. How email works? Explain with a help of a diagram.
13. Explain the different types of email abuse.
14. Explain the steps to trace the location of an email sender.
15. Explain the motivation behind designing scam or hoax websites.

3.17 ACTIVITIES

1 Google the term identity theft and find out more on the topic.
2 Google the term social engineering attacks and find out how hackers use this techniques to find out your personal information.
3 Find out more about “Internet of things (IOT)”. Study about the latest application of IOT.
4 Find all the country level domains.
5 Search the procedure to find out the email headers of yahoo mail.

Unit 4: Introduction to Cryptography

4

Unit Structure

4.1 LEARNING OBJECTIVES

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

- Know the basic terminologies of cryptography
- Define the meaning of word cryptography
- Know the objectives of cryptography
- Differentiate various cryptographic techniques
- Define encryption
- Describe the importance and working of encryption
- Describe the working of Secret key cryptography
- Recognize application of Secret key cryptography
- Describe the working of Public key cryptography
- Recognize applications of public key cryptography

4.2 INTRODUCTION

Cryptography is "Art of writing or hiding secret". It is a science of protecting the information from theft or unauthorized access. To do so, important or confidential information is hided as or converted to some other form of gibberish data. Now original information can be recovered only by the right person or application[40].

Cryptography was developed to create secure communication while there was a third-party present also known as adverseries[41]. In the beginning, the cryptographic codes were written by hand to convert plaintext to cipher-text and vise-versa. Early cryptography was messages written in a language the other party could not read or words that were written in reverse order. Cryptography was used mainly by military officers and spies to secure the confidentiality of the messages.

[40] http://www.go4expert.com/articles/introduction-cryptography-t24529/

[41] http://icsproject.wikispaces.com/Cryptography

Cryptography is the art of writing and solving code. It is used to secure files and is similar to a puzzle in which the message is scrambled using algorithms and unscrambled using another set of algorithms. Encryption is used in protecting passwords, securing classified messages and also used to protect personal and sensitive data.

The example of cryptography can be seen everywhere in our daily lives. For example the e- mails we send through g-mail or other mail servers are encrypted using algorithm to make sure no one else can intercept the messages being send and read them. The way the computer hides the password when we log in is also a form of cryptography.

4.2.1 Cryptography Objectives

Cryptography is needed in various scenarios varying from simple encryption of a small file to the complicated usages of smart cards used for windows authentications. Fundamentally, it is used in below mentioned scenarios

- Data at Motion - Cryptography is required when communicating over any non trusted medium. This medium can be internet, mobile phones, bank automatic teller machines, wireless intercom systems, Bluetooth devices, wireless microphones and portable storage disks. These days, organizations invest heavily to secure all the business communications like emails using cryptographic techniques and products. This is to ensure that no one else other than the trusted recipient can read the message.
- Data at Rest - Cryptography is must in securely storing all the sensitive and vital data. This is a basic provision mentioned in most of the compliances which an organization must meet. A simple example for this is Encrypting File system (EFS) which is a file system introduced in Windows operating system to provide file system level protection.
- Data integrity - Cryptography not only protects the information, but also verifies the integrity of data. This is necessary to ensure that the transferred data has not been tampered by a hacker.
- Before discussing cryptography in detail, let us first gear up with some common terminologies used frequently in cryptography.

4.2.2 Cryptography Glossary

1. **Key-** In the world of cryptography, "Key" refers to a digital data or file which mathematically determines the output of a cryptographic algorithm when applied to an input message.
2. **Encryption-** Encryption is a process of transforming information, using mathematical algorithms, to some sort of "nonsense" data. To encrypt a message or plain text, one needs to select an Encryption algorithm and a key (or a key – pair, based on encryption algorithm)
3. **Decryption-** Decryption is the reverse process of encryption, in which the encrypted message is processed and transformed back to the original message. Decryption can succeed if and only if, the correct algorithm (the one used during encryption process) and authentic keys are used.
4. **Digital certificates-** Digital certificates are file used for proving the authenticity of the user or sender. Digital certificates have information about the authority, which has issued the certificate and also, to whom the certificate is issued. Now, there are worldwide trusted certifying authorities (CA) like VeriSign, etc. So, any certificate issued by a Trusted CA, can be trusted as authentic and any information (generally cryptographic keys) contained in the certificate can be safely assumed to be from a trusted source.

4.3 TYPES OF CRYPTOGRAPHY

Cryptography[42] is essentially the science of writing in secret code. In data and telecommunications, cryptography has specific security requirements, such as authentication, privacy or confidentiality, integrity, and non-repudiation. To meet these security requirements, we employ secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions.

[42] https://learn.saylor.org/course/cs409

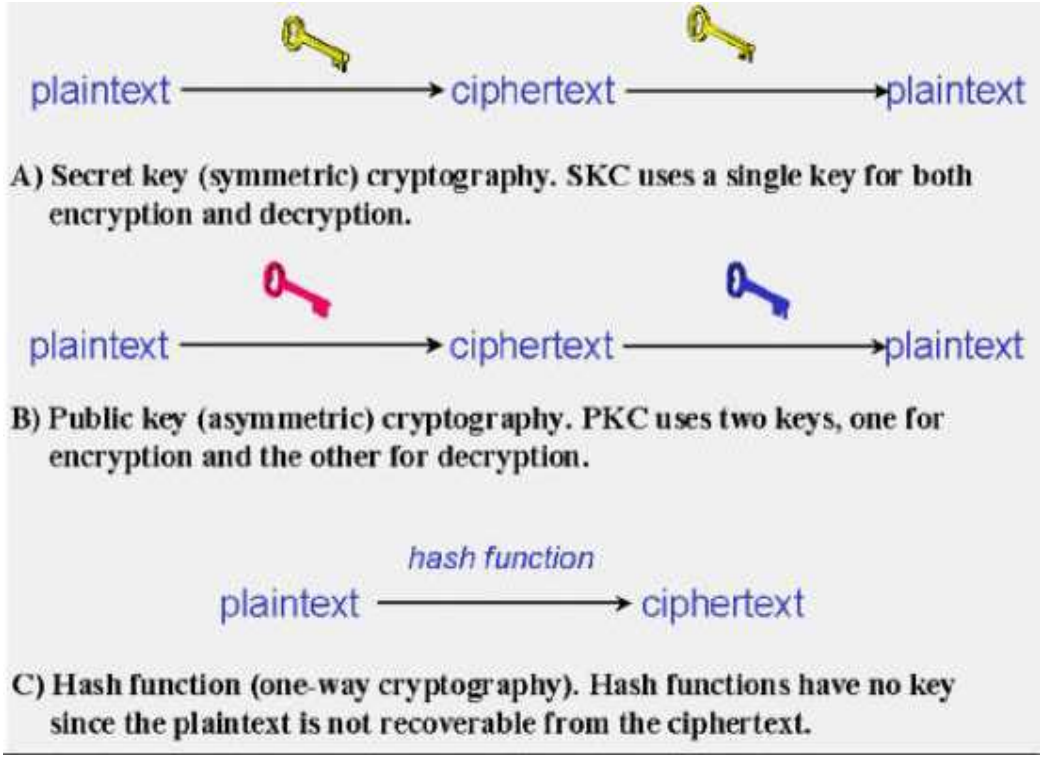


Figure 37: Types of cryptography[1]

There are three main types of cryptography:

1. Secret key cryptography
2. Public key cryptography
3. Hash function

1. Secret key cryptography – In this type of cryptography, the information is encrypted using a "secret" key. For decrypting the information, the user must possess the secret key. This type of encryption scheme is also known as Symmetric key encryption. In case of confidential data being transferred after encrypted with Symmetric key algorithms, both the sender and receiver must share the secret key. This encryption scheme is preferred over Public key cryptography when a large amount of data is to be encrypted, because it takes lesser time to encrypt or decrypt the data. An example of symmetric key cryptography is the whole disk encryption used by EFS of Windows operating system (EFS).
2. Public key cryptography – This scheme of cryptography involves two keys or

Key- pair, one is a Public key and the other one is private key. Public and private keys are mathematically related and it is impossible to calculate the private or public half of the pair given one key (private or public) of the key pair. The public key is meant to be distributed publicly whereas the corresponding private key must be kept much secured, ideally in a HSM (Hardware Security Module) device. If some information is encrypted by a public key, it can be decrypted only by the corresponding private key. Thus, in this scheme, it is not necessary for the sending and receiving users to share the common secret. The recipient distributes his public key. Sender encrypts the data using this public key. Now the data can be decrypted only by the receiver because he only has the correct private key.

3. Hash functions - Hash functions are one-way cryptographic schemes. In this method, a plain text is processed by the hash algorithm and the output is the hashed value of the original text. From this hashed value, it is impossible to recover the original information. Now a days, Hashing function and algorithms are used in the Authentication module of almost every application including the Windows authentication mechanism.

4.4 Why OS Encryption Important?[43]

Do you know who may be reading your E-Mail? It is transmitted in plain text over unknown pathways and resides for various periods of time on computer files over which you have no control. Whether you're planning a political campaign, discussing your finances, having an affair, completing a business deal, or engaging in some totally innocuous activity, your messages have less privacy than if you sent all of your written correspondence on postcards.

4.4.1 Why should Encryption be used?

Encryption is important because of the nature of the Internet and the electronic medium. It allows effective scanning of message contents using sophisticated filtering software. Electronic mail is gradually replacing

[43] https://www.efa.org.au/Issues/Crypto/crypto1.html

conventional paper mail and messages can be easily and automatically intercepted and scanned for interesting keywords. Another problem with E-Mail is that it is very easy to forge the identity of the sender. The solution to these problems is to use cryptography. However, there are restrictions on the export and use of strong cryptography, particularly in the USA, but now gaining momentum in other countries. Furthermore, some governments, and again the USA is the most prominent, want decryption keys lodged with escrow agents, so that law enforcement agencies can, with appropriate authorization, intercept and decrypt private messages. It is often claimed that this facility is no different from powers that the government has always possessed to wiretap telephones. There is however, a vital difference. Citizens are now being asked to take action to make themselves available for surveillance.

Cryptography today involves more than encryption and decryption of messages. It also provides mechanisms for authenticating documents using a digital signature, which binds a document to the possessor of a particular key, while a digital timestamp binds a document to its creation at a particular time. These are important functions which must take the place of equivalent manual authentication procedures as we move into the digital age. Cryptography also plays an important part in the developing field of digital cash and electronic funds transfer.

The major applications for encryption may then be summarised as:

- To protect privacy and confidentiality.
- To transmit secure information (e.g. credit card details)
- To provide authentication of the sender of a message.
- To provide authentication of the time a message was sent.

4.4.2 How does it work?

Up until the mid 1970's cryptography was an arcane science practised largely by government and military security experts. That situation changed dramatically following the development of public key cryptography by Hellman and Diffie in 1975. This development solved a major problem with most cryptographic systems - that of exchanging keys, and preceded a rapid escalation in civil involvement in this field of endeavour.

Public key cryptography systems work with public and secret (or private) keys. You generate these yourself as a once-only task. You distribute your public key to anyone who may need to send you encrypted information, or you can place it on one of the many public-key repositories around the globe. Your public key is then used by others to encrypt messages sent to you. Only you can decrypt such a message since the secret key is needed to perform this task. In practice, because public key encryption is a time-consuming process, many cryptosystems only use the public key to encrypt a random session key, which is then used to encrypt the actual message.

As an example, to exchange secure communications with someone the procedure would be as follows. Here we will introduce Alice and Bob, the renowned "first couple" of cryptography.

- Alice and Bob exchange their respective public keys or obtained them from a public key repository.
- Alice transmits the message encrypted with the *Bob's* public key.
- Bob decrypts it with his *secret* key.
- Only Bob can decipher the message. Even Alice will be unable to decipher the message once encrypted, unless she has included herself as a recipient (using multiple keys to encrypt the message).
- Cryptography can also be used to produce a digital signature which proves that the transmission is unchanged and can authenticate the sender. In this case the Bob would use Alice's *public* key to read the signature created by Alice's *secret* key.

4.5 Public Key Cryptography[44]

4.5.1 Public keys and private keys

When using public key cryptography, Alice and Bob both have their own key pairs. A key pair consists of a public key and a private key. If the public key is used to encrypt something, then it can be decrypted only using the private key. And similarly, if the private key is used to encrypt something, then it can be decrypted only using the public key. It is not possible to figure out what the private key is given only the public key, or vice versa.

[44] http://www.iusmentis.com/technology/encryption/crashcourse/publickeycrypto/

This makes it possible for Alice and Bob to simply send their public keys to one another, even if the channel they are using to do so is insecure. It is no problem that Eve now gets a copy of the public keys. If Alice wants to send a secret message to Bob, she encrypts the message using Bob's public key. Bob then takes his private key to decrypt the message. Since Eve does not have a copy of Bob's private key, she cannot decrypt the message. Of course this means that Bob has to carefully guard his private key. With public key cryptography it is thus possible for two people who have never met to securely exchange messages.

4.5.2 Combining public key and secret key cryptography

A problem with public key cryptography is that it is very slow. Encrypting a message that is several megabytes long takes a very long time, much longer than when using secret key cryptography. For this reason few people use only public key cryptography. What Alice usually does is encrypt the message using a secret key encryption algorithm and a key she made up on the spot. She then encrypts this key (called the session key) using Bob's public key. Bob can then obtain the session key by decrypting it using his private key. And with the session key he can decrypt the message. This way a long message is encrypted very quickly and Alice can still send it to Bob without needing a secure way of agreeing on the key.

4.5.3 How public key cryptography works

Public key cryptography systems are usually based on the assumption that a particular mathematical operation is easy to do, but difficult to undo unless you know some particular secret. This particular secret that serves as the private key. The two most famous public key cryptography systems are Diffie-Hellman and the RSA system, named after its inventors Rivest, Shamir and Adleman. More recently public key cryptography based on so-called elliptic curves has gotten a lot of attention. Using public key cryptography it is possible to easily encrypt a message for multiple recipients. It is even possible to later authorize recipients to read the message. The message is simply encrypted with a session key. The session key is encrypted multiple times, once for every recipient using his public key. If later another recipient needs to be added, the session key is

simply then also encrypted using his public key. Every recipient can now decrypt the session key independently from every other recipient.

4.6 APPLICATIONS OF PUBLIC KEY CRYPTOGRAPHY

4.6.1 Secure Web communication

One important application of public key cryptography is encrypted communication with a Web server. This enables Alice to securely place an order and to transmit her credit card details. Alice's Web browser generates a random number which will be used to encrypt all communication with the server using secret key cryptography. The browser obtains a copy of the public key of the server and uses this public key to encrypt this random number (called the session key). The result is sent to the server. After that, browser and server can encrypt all information so that Eve cannot read it.

Alternatively, it is the server that generates the session key. This requires that the browser sends its own public key to the server so that the session key can be transmitted securely. This makes it easier to upgrade the hardware or software that generates the session key.

4.6.2 Secure content distribution

Content such as music or video can be distributed in encrypted form. To be able to play it back, the recipient needs the decryption key. To avoid having to encrypt the entire movie or song again for every recipient, the content is encrypted with a session key. Every recipient receives the encrypted content together with the session key. The session key is of course encrypted using the recipient's public key. This way only a very small amount of data needs to be encrypted again for every recipient.

It is even possible to distribute the encrypted content in advance. If the recipient wants to play back the content, he can at any time contact the distributor and obtain (purchase) a copy of the session key encrypted using his public key. This is sometimes called 'superdistribution'.

4.7 SECRET KEY CRYPTOGRAPHY[45]

4.7.1 Encryption and decryption using a secret key

To secretly communicate with Bob, Alice encrypts her messages before sending them. There are many techniques (cryptographic algorithms) that she can use. All these algorithms have in common that they can transform a message using a key into something that resembles random noise. This is called encrypting the message. Only the persons who know the key can transform the random noise back into the original message, or in other words, decrypt the message. This means that those persons must keep this key a secret, hence the name secret key cryptography.

4.7.2 How to get the key to the recipient

A fundamental problem with secret key encryption is that somehow the secret key has to be delivered to the recipient of the message in a secure way. Once that key has been securely delivered, other keys can be delivered by simply encrypting them with that first key. One way to solve this problem is to have Alice and Bob meet in person so they can agree on a key. They must make sure that Eve is not listening in on them, otherwise Eve also learns the key. This applies especially if Alice and Bob agree on a key via telephone or e-mail. Of course Bob must also be able to distinguish Alice and Eve if they meet for the first time (for Alice it shouldn't be a problem to tell Bob from Eve).

If Alice and Bob cannot meet in private to agree on the key, it is very difficult for them to use secret key cryptography. If they simply agree on a key by e-mail for example, Eve could be listening in on their e-mail conversation and thus also learn what the key is. If Alice and Bob had a secure channel that Eve could not tap, they could use that channel to agree on a secret key. However, then they could also use the secure channel to simply transmit their messages. This problem is solved by using public key cryptography, which is discussed in the next section.

4.7.3 How secret key cryptography works

[45] http://www.iusmentis.com/technology/encryption/crashcourse/secretkeycrypto/

Secret key cryptography transforms (scrambles) a message into something resembling random noise. The precise transformation is determined by the key. Mathematically seen, a cryptographic algorithm is a function that maps a message onto a ciphertext (an encrypted message). By using keys, it is possible to encrypt many different messages using one particular cryptographic algorithm in different ways. And keeping the key a secret is much easier than keeping a complete algorithm a secret.

Some cryptographic algorithms operate on single characters of the message. These are called stream ciphers. Others operate on entire blocks, and therefore are called block ciphers. Stream ciphers are easier to implement in hardware than block ciphers, and they are also generally faster. Block ciphers tend to be harder to crack. We will discuss an example of a secret key cryptographic system to further elaborate the concept.

A very simple technique to encrypt messages is to replace every letter of the message with one that is a certain number of positions further in the alphabet. The key then is the number of positions. For example, the message "This is an example" can be encrypted using the key "1 position" into the encrypted message "Uijt jt bo fybnqmf". Taking the letter that is 1 position previous in the alphabet results in the original message again.

This system is of course not very secure. There are only twenty-six possible keys. Eve can simply try out all the keys to see which one results in a readable message. Furthermore, it is a well-known fact that certain letters occur more often in messages than others. The letter "e" is the most frequently used letter in the English language, for example. Using this fact Eve can simply count which letter occurs the most often in the encrypted message and replace that one with the letter "e". She then knows how many positions she has to rotate to get from "e" to the encrypted version of "e" and thus she immediately knows the key.

In principle, all cryptographic systems can be broken. At the very least, Eve can try out all different keys until she finds one that successfully decrypts the message. Eve might also be able to break one of the

mathematical principles behind the cryptographic algorithm that Alice and Bob use. For example, some cryptographic systems assume that it is very difficult to divide a number into its prime factors. Eve might find a quick way to do this. This then enables Eve to read Alice and Bob's messages or to recover their keys.

There is one cryptographic algorithm that cannot be broken. This algorithm is called the one- time pad (OTP). According to this algorithm, Alice generates a very large sequence of random numbers. The numbers in the sequence serve as the key. The sequence is called the "pad". Alice communicates the sequence to Bob in a secure way, so that Eve cannot obtain a copy of the key.

Every character in the message that Alice wants to send to Bob is encrypted with a different number in the sequence. In practice this means that the first character of the message will be encrypted with the first number in the sequence, the second character with the second number, and so on. When Bob receives the encrypted message, he takes out his copy of the sequence and simply decrypts the first character with the first number in the sequence, the second character with the second number, and so on.

Because every character of the message is encrypted with a different key, there is nothing Eve can do to guess the key. Even if she knew that the first words of the message were "Dear Bob", she could not use this information to recover the key of other words in the message. Every number is chosen randomly, so Eve has no way to know which number is the right one, even if Eve knew how to decrypt all other characters.

It is absolutely essential that every number in the sequence is chosen randomly and is only used once. If Eve can recover some of the numbers in the sequence and use those to predict other numbers, she can eventually reconstruct the entire sequence and thereby decrypt the message. For this reason it is not a good idea to use a random number generator implemented in software. Those generators are unable to generate really random numbers. They use a mathematical function that generates a set of numbers that appears to be random. But if you know

the mathematical function and the number that it last generated, you can immediately compute the next "random" number.

To achieve this unbreakability, Alice and Bob must have very large sequences that contain only really random numbers. This makes an OTP very difficult to manage. It is said to have been used for the "hotline" between Washington and Moscow during the Cold War. In a case like that, it is practical to send couriers carrying suitcases chained to their arms to securely transmit the pad.

4.8 Applications of Symmetric Key Cryptography

Secret key encryption is most often used to encrypt data to be stored on a particular location. If the encrypted data has to be transmitted, there always is the problem of how to get the secret key to the recipient in a safe way. Usually the key is encrypted using public key encryption so it can be transmitted safely.

4.8.1 Hiding spoilers

Even though it is not secure, the simple alphabet shifting system is still in use on the Internet. It is used to hide "spoilers" (revealing plot twists in movies or books) and potentially offensive messages from unsuspecting readers. Such messages are encrypted using the key "13 positions". Anyone can thus decrypt the message by simply taking the letter that is 13 positions previous in the alphabet. However, this requires some active step by the reader, and so he should then not be surprised or upset if the decrypted message reveals something about the plot of a movie he wanted to see. This system is commonly known as "ROT-13".

4.8.2 Encrypting the contents of hard disks

Using secret key encryption Alice can encrypt her entire hard disk so the data on it is safe if the disk (or laptop containing it) is ever stolen. Disk encryption programs exist that can encrypt and decrypt data as it is being written and read to and from the hard disk. This way Alice does not notice that her data is stored encrypted, except for the fact that disk access might be a bit slower. Once she turns off her computer, it is not possible anymore for Eve to read the data.

4.8.3 Protecting pay TV transmissions

Secret key encryption and smart cards are used for example in pay TV

applications. Sometimes this is referred to as "conditional access" television. Television programs(usually premium movies, football or soccer matches and adult content) are encrypted using a secret key. To make it difficult for Eve to obtain this key, the secret key is changed every few minutes or sometimes even every few seconds. This way, even if Eve can successfully use a brute force attack to guess the key, she only has a very small portion of the television program. Alice has a set-top box and a smart card that allows her to decrypt the television programs. The set-top box passes the decrypted television program on to the television.

Originally these boxes were designed to be placed on top of the television set, hence the name.

Special messages, called Entitlement Control Messages (ECMs), are sent along with the program. These messages contain the secret keys. Of course the ECMs themselves are also encrypted, this time using a key stored on the smart card. Alice's set-top box receives the ECMs and passes them on to the smart card. The smart card decrypts the ECMs and extracts the secret keys contained therein. This allows the set-top box to decrypt the television program.

The keys needed to decrypt the ECMs can be programmed on the smart card in advance. By regularly changing these keys, Alice is forced to purchase a new smart card every month or so. If Eve manages to make a copy of the smart card, or to extract the keys from it, she will only be able to watch the programs for the rest of that particular month.

Another option is to regularly send out so-called Entitlement Management Messages (EMMs) that contain the keys needed to decrypt the ECMs. The EMMs themselves are then encrypted with keys stored on the smart card. The service provider then every month simply sends out a new EMM. This provides much greater flexibility, and Alice does not have to go to the store every month. Every smart card can now have a different key. The service provider sends out different EMMs for all the smart cards in the system. Every EMM thus is readable only by one smart card. If the service provider thinks a particular smart card has been copied illegally, he simply does not send out a new EMM for that particular smart card.

4.9 LET US SUM UP

1. Cryptography is art of writing or hiding secret.
2. Encryption is used in protecting passwords, securing classified messages and also used to protect personal and sensitive data.
3. Key refers to a digital data or file which mathematically determines the output of a cryptographic algorithm when applied to an input message.
4. Digital certificates are file used for proving the authenticity of the user or sender.
5. In secret key cryptography the information is encrypted using a "secret" key. For decrypting the information, the user must possess the secret key.
6. In public key cryptography, two keys or Key-pair are invloved, one is a Public key and the other one is private key. Public and private keys are mathematically related and it is impossible to calculate the private or public half of the pair given one key (private or public) of the key pair.
7. In Hash functions method, a plain text is processed by the hash algorithm and the output is the hashed value of the original text. From this hashed value, it is impossible to recover the original information.

4.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. Fill in the blanks.
   i. Cryptography was developed to create secure communication while there was a third- party present also known as_____.
   ii. _____is used in protecting passwords, securing classified messages and also used to protect personal and sensitive data.
   iii. Cryptography not only protects the information, but also verifies the_____ of data.
   iv. _____is the reverse process of encryption.
   v. EMM stands for_____.
   vi. _____are file used for proving the authenticity of the

user or sender

vii. OTP stands for_____.

2. State True or False

i. Hash functions are two-way cryptographic schemes.
ii. Encryption is also used to provide authentication of the time a message was sent.
iii. Secret key cryptography transforms (scrambles) a message into something resembling random noise.
iv. Your private key is used by others to encrypt messages sent to you.

Answers:

1. Fill in the blanks

i. adverseries
ii. Encryption
iii. integrity
iv. Decryption
v. Entitlement Management Messages
vi. Digital certificates
vii. One Time Pad

2. State True or False

i. False
ii. True
iii. True
iv. False

4.11 FURTHER READING

1. (n.d.). Retrieved Dec. 07, 2015, from Istqbexamcertification.com
2. (n.d.). Retrieved Dec. 07, 2015, from Softwaretestinghelp.com
3. (n.d.). Retrieved Dec. 07, 2015, from www.onestoptesting.com
4. Babu B., S., & Venkataram, P. *Wireless and Mobile Security 1st Edition.* Mcgraw Hill Education.
5. Bose, R. (2008). *Mcgraw Hill Education.* Mcgraw Hill Education.
6. Bunting, S., & Wei, W. (2006). *The Official EnCE: EnCase Certified ExaminorStudy Guide.*

7. Wiley Publishing Inc. *Cryptography*. (n.d.). Retrieved Sep. 29, 2015, from Wikispaces: http://icsproject.wikispaces.com/Cryptography
8. *Cryptography*. (n.d.). Retrieved Oct. 01, 2015, from ICSProjects.Wikispaces.com: http://icsproject.wikispaces.com/Cryptography
9. *CYBER SECURITY MANIFESTO 2.0*. (2012, Oct. 01). Retrieved Sep. 26, 2015, from cybersecuritymanifesto: http://cybersecuritymanifesto.com/
10. *CYBER SECURITY MANIFESTO 2.0*. (2012, Oct. 01). Retrieved Sep. 28, 2015, from cybersecuritymanifesto.com: http://cybersecuritymanifesto.com/
11. Edson, J. (2011, July 25). *A Brief History Of Forensic Science*. retrieved Oct. 04, 2015, from riaus.org.au: http://riaus.org.au/articles/a-brief-history-of-forensic-science/
12. Gallagher, S. (2013, Oct. 02). *We are not who we are*. Retrieved Sep. 26, 2015, from Security Blog: https://securityblog.redhat.com/tag/two-factor-authentication/
13. *Gardner, M. (1972). Codes, ciphers, and secret writing.*
14. *Glass, E. (2003). The NTLM Authentication Protocol and Security Support Provider. Retrieved Sep. 26, 2015, from Sourceforge: http://davenport.sourceforge.net/ntlm.html*

4.12 ASSIGNMENTS

1. What is cryptography? What are the objectives of cryptography?
2. What are the various types of cryptographic techniques?
3. Define:
   a. Encryption
   b. Decryption
   c. Key
   d. Digital Certificate
4. Explain the importance of using encryption.
5. Define public key cryptography in details.
6. Explain various public key cryptography examples.
7. How secret key cryptography works.
8. Explain various secrets key cryptography examples.

Block-4

Unit 1: Disaster Recovery 1

Unit Structure

1.1 Learning Objectives

After going through this unit, you will able to:

- Know about disaster recovery plan (DRP)
- Know the benefits of DRP
- Understand the relationship of DRP with Business continuity plan
- Know, why DRP is important
- Know different types of Disasters
- Know different types of planning methodology
- Know DRP controversies

1.2 Introduction

Organizations cannot always avoid disasters, but with careful planning the effects of a disaster can be minimized. The objective of a disaster recovery plan is to minimize downtime and data loss. The primary objective is to protect the organization in the event that all or parts of its operations and/or computer services are rendered unusable. The plan minimizes the disruption of operations and ensures that some level of organizational stability and an orderly recovery after a disaster will prevail. Minimizing downtime and data loss is measured in terms of two concepts: the recovery time objective (RTO) and the recovery point objective (RPO). The recovery time objective is the time within which a business process must be restored, after a major incident (MI) has occurred, in order to avoid unacceptable consequences associated with a break in business continuity. The recovery point objective (RPO) is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a MI. The RPO is expressed backwards in time (that is, into the past) starting from the instant at which the MI occurs, and can be specified in seconds, minutes, hours, or days. The recovery point objective (RPO) is thus the maximum acceptable amount of data loss measured in time. It is the age of the files or data in backup storage required to resume normal operations after the MI.

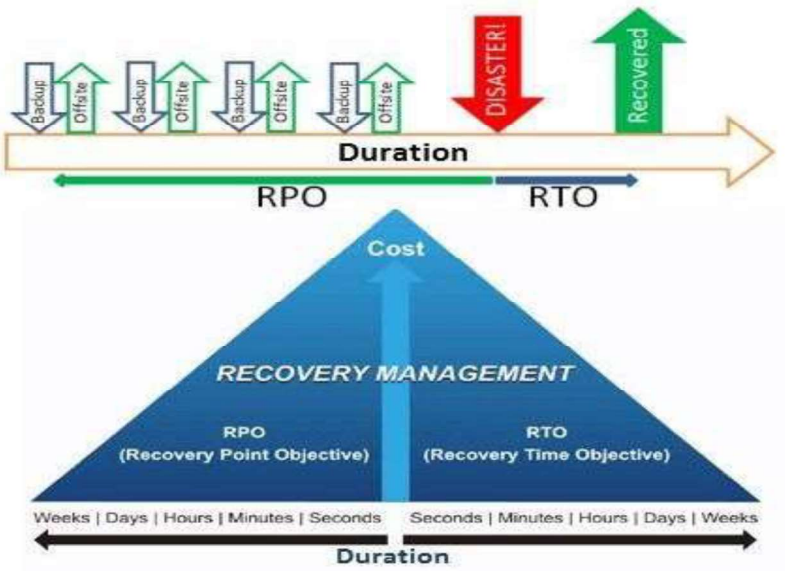


Fig: A DR plan illustrating the chronology of the RPO and the RTO

1.3 The Development of Disaster Recovery

Disaster recovery was developed in late 1970s because computer center managers started to recognize dependence of their organizations on their systems. Most systems at that time were batch-oriented mainframes that could be down for some days before significant damage could be done to organization. As the knowledge sensibility of potential business disruption which should follow the IT-related disaster, disaster recovery industry was developed in order to provide Sun Information Systems to the backup computer centers becoming the first major US commercial hot site vendor in 1978. (Sun Information Systems became later SunGard Availability Services). During 1980s and 1990s, customer's knowledge sensibility and this industry grew rapidly through an advent of real-time processing and open systems that increased the dependence of different organizations on their IT systems. With the rapid growth during 1990s and 2000s of the Internet, organizations in different sizes became dependent on continuous availability of their IT systems. This increasing dependence on the IT systems, besides the increased knowledge sensibility from large-scale disasters like tsunami, flood, earthquake, and volcanic eruption, could spawn disaster recovery-related services and products, ranging from the high-availability solutions to the hot-site facilities. The rise of the cloud computing technology in 2010 continues that trend and

nowadays, it even matters less where computing services are served physically, just too long as network itself is reliable sufficiently. Recovery as a Service (RaaS) is now one of the security features of the cloud computing as it's promoted by Cloud Security Alliance.

1.4 What is Disaster Recovery Plan?

A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Such a plan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster. It is "a comprehensive statement of consistent actions to be taken before, during and after a disaster." The disaster could be natural, environmental or man- made. Man-made disasters could be intentional (for example, an act of a terrorist) or unintentional (that is, accidental, such as the breakage of a man- made dam). Given organizations' increasing dependency on information technology to run their operations, a disaster recovery plan, sometimes erroneously called a Continuity of Operations Plan (COOP), is increasingly associated with the recovery of information technology data, assets, and facilities.

1.5 Importance of Disaster Recovery Plan

As IT systems have become increasingly critical to the smooth operation of a company, and arguably the economy as a whole, the importance of ensuring the continued operation of those systems, and their rapid recovery, has increased. For example, of companies that had a major loss of business data, 43% never reopen and 29% close within two years. As a result, preparation for continuation or recovery of systems needs to be taken very seriously. This involves a significant investment of time and money with the aim of ensuring minimal losses in the event of a disruptive event.

1.6 Don't ignore it until it's too late!

Maybe software developers are naturally optimistic but in my experience they rarely consider system failure or disaster scenarios when designing software. Failures are varied and range from the likely (local disk failure) to the rare (tsunami) and from low impact to fatal (where fatal may be the death of people or bankruptcy of a business). Failure planning broadly fits into the following areas:

- Avoiding failure
- Failing safely
- Failure recovery
- Disaster Recovery

Avoiding failure is what a software architect is most likely to think about at design time. This may involve a number of High Availability (HA) techniques and tools including; redundant servers, distributed databases or real time replication of data and state. This usually involves removing any single point of failure but you should be careful to not just consider the software and hardware that it immediately runs on - you should also remove any single dependency on infrastructure such as power (battery backup, generators or multiple power supplies) or telecoms (multiple wired connections, satellite or radio backups etc). Failing safely is a complex topic that I touched on recently and may not apply to your problem domain (although you should always consider if it does). Failure recovery usually goes hand-in-hand with High Availability and ensures that when single components are lost they can be re-created/started to join the system. There is no point in having redundancy if components cannot be recovered as you will eventually lose enough components for the system to fail!

1.7 Benefits of Disaster Recovery

Like every insurance plan, there are benefits that can be obtained from the drafting of a disaster recovery plan. Some of these benefits are:

1. Providing a sense of security
2. Minimizing risk of delays

3. Guaranteeing the reliability of standby systems
4. Providing a standard for testing the plan
5. Minimizing decision-making during a disaster
6. Reducing potential legal liabilities
7. Lowering unnecessarily stressful work environment

1.8 Classification of Disasters

Disasters can be classified into two broad categories:

1.8.1 Natural Disasters

The first is natural disasters. A **natural disaster** is a major adverse event resulting from **natural** processes of the Earth. The examples include floods, tsunamis, tornadoes, hurricanes/cyclones, volcanic eruptions, earthquakes, heat waves, and landslides. While preventing, a natural disaster is very difficult, risk management measures such as avoiding disaster-prone situations and good planning can help. A natural disaster is a major adverse event resulting from the earth's natural hazards. Other types of disasters include the more cosmic scenario of an asteroid hitting the Earth.

Fig: Natural Disaster

1.8.2 Man-Made Disasters

Man-made disasters are the consequence of technological or human hazards. Examples include stampedes, urban fires, industrial accidents, oil spills, nuclear explosions/nuclear radiation and acts of war. Other types of man-made disasters include the more cosmic scenarios of catastrophic global warming, nuclear war, and bioterrorism.

Fig: Man-made disaster

1.9 Relationship to the Business Continuity Plan

The Business Continuity Plan (BCP) is a comprehensive organizational plan that includes the disaster recovery plan. The Institute further states that a Business Continuity Plan (BCP) consists of the five component plans:

1. Business Resumption Plan
2. Occupant Emergency Plan
3. Continuity of Operations Plan
4. Incident Management Plan
5. Disaster Recovery Plan

The Institute states that the first three plans (Business Resumption, Occupant Emergency, and Continuity of Operations Plans) do not deal with the IT infrastructure. They further state that the Incident Management Plan (IMP) does deal with the IT infrastructure, but since it establishes structure and procedures to address cyber-attacks against an organization's IT systems, it generally does not

represent an agent for activating the Disaster Recovery Plan, leaving The Disaster Recovery Plan as the only BCP component of interest to IT. Disaster Recovery Institute International states that disaster recovery is the area of business continuity that deals with technology recovery as opposed to the recovery of business operations.

1.10 It Disaster Recovery Control Measures

Control measures are steps or mechanisms that can reduce or eliminate various threats for organizations. Different types of measures can be included in disaster recovery plan (DRP). Disaster recovery planning is a subset of a larger process known as business continuity planning and includes planning for resumption of applications, data, hardware, electronic communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity.

IT disaster recovery control measures can be classified into the following three types:

1. **Preventive measures** - Controls aimed at preventing an event from occurring.
2. **Detective measures** - Controls aimed at detecting or discovering unwanted events.
3. **Corrective measures** - Controls aimed at correcting or restoring the system after a disaster or an event.

Good disaster recovery plan measures dictate that these three types of controls be documented and exercised regularly using so-called "DR tests".

1.11 Disaster Recovery Planning Methodology

According to Geoffrey H. Wold of the Disaster Recovery Journal, the entire process involved in developing a Disaster Recovery Plan consists of 10 steps:

1.11.1 Obtaining Top Management Commitment

For a disaster recovery plan to be successful, the central responsibility for the plan must reside on top management. Management is responsible for coordinating the disaster recovery plan and ensuring its effectiveness within the organization. It is also responsible for allocating adequate time and resources required in the development of an effective plan. Resources that management must allocate include both financial considerations and the effort of all personnel involved.

1.11.2 Establishing a Planning Committee

A planning committee is appointed to oversee the development and implementation of the plan. The planning committee includes representatives from all functional areas of the organization. Key committee members customarily include the operations manager and the data processing manager. The committee also defines the scope of the plan.

1.11.3 Performing a Risk Assessment

The planning committee prepares a risk analysis and a business impact analysis (BIA) that includes a range of possible disasters, including natural, technical and human threats. Each functional area of the organization is analyzed to determine the potential consequence and impact associated with several disaster scenarios. The risk assessment process also evaluates the safety of critical documents and vital records. Traditionally, fire has posed the greatest threat to an organization. Intentional human destruction, however, should also be considered. A thorough plan provides for the “worst case” situation: destruction of the main building. It is important to assess the impacts and consequences resulting from loss of information and services. The planning committee also analyzes the costs related to minimizing the potential exposures.

1.11.4 Establishing Priorities for Processing and Operations

At this point, the critical needs of each department within the organization are evaluated in order to prioritize them. Establishing priorities is important because no organization possesses infinite resources and criteria must be set as to where to allocate resources first. Some of the areas often reviewed during the prioritization process are functional operations, key personnel and their functions, information flow, processing systems used, services provided, existing documentation, historical records, and the department's policies and procedures. Processing and operations are analyzed to determine the maximum amount of time that the department and organization can operate without each critical system. This will later get mapped into the Recovery Time Objective. A critical system is defined as that which is part of a system or procedure necessary to continue operations should a department, computer center, main facility or a combination of these be destroyed or become inaccessible. A method used to determine the critical needs of a department is to document all the functions performed by each department. Once the primary functions have been identified, the operations and processes are then ranked in order of priority: essential, important and non-essential.

1.11.5 Determining Recovery Strategies

During this phase, the most practical alternatives for processing in case of a disaster are researched and evaluated. All aspects of the organization are considered, including physical facilities, computer hardware and software, communications links, data files and databases, customer services provided, user operations, the overall management information systems (MIS) structure, end-user systems, and any other processing operations. Alternatives, dependent upon the evaluation of the computer function, may include: hot sites, warm sites, cold sites, reciprocal agreements, the provision of more than one data center, the installation and deployment of multiple computer system, duplication of service center, consortium arrangements, lease of equipment, and any combinations of the above. Written agreements for the specific recovery alternatives selected are prepared, specifying contract duration, termination conditions, system testing, cost, any special security procedures, procedure for the notification of system changes, hours of operation, the specific hardware and other equipment required

for processing, personnel requirements, definition of the circumstances constituting an emergency, process to negotiate service extensions, guarantee of compatibility, availability, non-mainframe resource requirements, priorities, and other contractual issues.

1.11.6 Collecting Data

Among advised data gathering materials or documentation usually included are different lists such as (Critical telephone numbers list, master vendor list, employee backup position listing, master call list, notification checklist), inventories such as (Off-site storage location equipment, documentation, communications equipment, microcomputer hardware and software, forms, insurance policies, office equipment, workgroup and data center computer hardware, office supply, telephones, etc.), distribution register, temporary location specifications, software and data files backup/retention schedules, and any other lists, materials, inventories and documentation. The pre-formatted forms are usually used in order to facilitate data gathering process.

1.11.7 Organizing and Documenting a Written Plan

Next, an outline of the plan's contents is prepared to guide the development of the detailed procedures. Top management reviews and approves the proposed plan. The outline can ultimately be used for the table of contents after final revision. Other four benefits of this approach are that

1 It helps to organize the detailed procedures,
2 Identifies all major steps before the actual writing process begins,
3 Identifies redundant procedures that only need to be written once, and
4 Provides a road map for developing the procedures.

It is often considered best practice to develop a standard format for the disaster recovery plan so as to facilitate the writing of detailed procedures and the documentation of other information to be included in the plan later. This helps ensure that the disaster plan follows a consistent format and allows for its ongoing future maintenance. Standardization is also important if more than one person is involved in writing the procedures. It is during this phase that the actual written plan is developed in its entirety, including all detailed procedures to be used

before, during, and after a disaster. The procedures include methods for maintaining and updating the plan to reflect any significant internal, external or systems changes. The procedures allow for a regular review of the plan by key personnel within the organization. The disaster recovery plan is structured using a team approach. Specific responsibilities are assigned to the appropriate team for each functional area of the organization. Teams responsible for administrative functions, facilities, logistics, user support, computer backup, restoration and other important areas in the organization are identified. The structure of the contingency organization may not be the same as the existing organization chart. The contingency organization is usually structured with teams responsible for major functional areas such as administrative functions, facilities, logistics, user support, computer backup, restoration, and any other important area. The management team is especially important because it coordinates the recovery process. The team assesses the disaster, activates the recovery plan, and contacts team managers. The management team also oversees, documents and monitors the recovery process. It is helpful when management team members are the final decision-makers in setting priorities, policies and procedures. Each team has specific responsibilities that are completed to ensure successful execution of the plan. The teams have an assigned manager and an alternate in case the team manager is not available. Other team members may also have specific assignments where possible.

1.11.8 Developing Testing Criteria and Procedures

Best practices dictate that DR plans be thoroughly tested and evaluated on a regular basis (at least annually). Thorough DR plans include documentation with the procedures for testing the plan. The tests will provide the organization with the assurance that all necessary steps are included in the plan. Other reasons for testing include:

- Determining the feasibility and compatibility of backup facilities and procedures.
- Identifying areas in the plan that needs modification.
- Providing training to the team managers and team members.
- Demonstrating the ability of the organization to recover.

- Providing motivation for maintaining and updating the disaster recovery plan.

1.11.9 Testing the Plan

After the testing procedures been completed, initial “dry run” plan is performed through conducting structured walk-through test. This test will provide an additional information towards any further changes in procedures which are not effective, steps which may need to be included, and other appropriate adjustments. Remember that these cannot become an evident unless actual dry-run test is performed. The plan is updated subsequently in order to correct any problems that are identified during the test. But initially, the testing of the plan will be done in sections and even after normal business hours in order to minimize disruptions to overall operations of organization and as plans are further polished, future tests also occur during the normal business hours.

Different types of tests include:

1 Checklist tests.

2 Full interruption tests.

3 Parallel tests.

4 Simulation tests.

1.11.10 Obtaining Plan Approval

Once the disaster recovery plan has been written and tested, the plan is then submitted to management for approval. It is top management’s ultimate responsibility that the organization has a documented and tested plan. Management is responsible for:

1 Establishing the policies, procedures and responsibilities for comprehensive contingency planning, and

2 Reviewing and approving the contingency plan annually, documenting such reviews in writing.

Organizations that receive information processing from service bureaus will, in addition, also need to:

- Evaluate the adequacy of contingency plans for its service bureau, and
- Ensure that its contingency plan is compatible with its service bureau’s plan.

1.12 Caveats/Controversies

Due to its high cost, disaster recovery plans are not without critics. Cormac Foster has identified five "common mistakes" organizations often make related to disaster recovery planning:

1.12.1 Lack of Buy-In

One factor is the perception by executive management that DR planning is "just another fake earthquake drill" or CEOs that fail to make DR planning and preparation a priority, are often significant contributors to the failure of a DR plan.

1.12.2 Incomplete RTOs and RPOs

Another critical point is failure to include each and every important business process or a block of data. "Every item in your DR plan requires a Recovery Time Objective (RTO) defining maximum process downtime or a Recovery Point Objective (RPO) noting an acceptable restore point. Anything less creates ripples that can extend the disaster's impact." As an example, "payroll, accounting and the weekly customer newsletter may not be mission-critical in the first 24 hours, but left alone for several days, they can become more important than any of your initial problems".

1.12.3 Systems Myopia

A third point of failure involves focusing only on DR without considering the larger business continuity needs: "Data and systems restoration after a disaster are essential, but every business process in your organization will need IT support, and that support requires planning and resources." As an example, corporate office space lost to a disaster can result in an instant pool of teleworkers which, in turn, can overload a company's VPN overnight, overwork the IT support staff at the blink of an eye and cause serious bottlenecks and monopolies with the dial-in PBX system.

1.12.4 Lax Security

When there is a disaster, an organization's data and business processes become vulnerable. As such, security can be more important than the raw speed involved in a disaster recovery plan's RTO. The most critical consideration then becomes securing the new data pipelines: from new VPNs to the connection from offsite backup services. Another security concern includes documenting every step of the recovery process— something that is especially important in highly regulated

industries, government agencies, or in disasters requiring post-mortem forensics. Locking down or remotely wiping lost handheld devices is also an area that may require addressing.

1.12.5 Outdated Plans

Another important aspect that is often overlooked involves the frequency with which DR Plans are updated. Yearly updates are recommended but some industries or organizations require more frequent updates because business processes evolve or because of quicker data growth. To stay relevant, disaster recovery plans should be an integral part of all business analysis processes, and should be revisited at every major corporate acquisition, at every new product launch and at every new system development milestone.

1.13 Let us Sum-up

A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Organizations cannot always avoid disasters, but with careful planning the effects of a disaster can be minimized. Minimizing downtime and data loss is measured in terms of two concepts: the recovery time objective (RTO) and the recovery point objective (RPO). The recovery time objective is the time within which a business process must be restored, after a major incident (MI) has occurred, in order to avoid unacceptable consequences associated with a break in business continuity. The recovery point objective (RPO) is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a MI. As IT systems have become increasingly critical to the smooth operation of a company, and arguably the economy as a whole, the importance of ensuring the continued operation of those systems, and their rapid recovery, has increased. Benefits include providing a sense of security, Minimizing risk of delays, Guaranteeing the reliability of standby systems, Providing a standard for testing the plan, Minimizing decision-making during a disaster, Reducing potential legal liabilities, Lowering unnecessarily stressful work environment. A natural disaster is a major adverse event resulting from the earth's natural hazards.Man-made disasters is the consequence of technological or human hazards. Disaster Recovery Institute International states that disaster

recovery is the area of business continuity that deals with technology recovery as opposed to the recovery of business operations. Control measures are steps or mechanisms that can reduce or eliminate various threats for organizations. Different types of measures can be included in disaster recovery plan (DRP) like Preventive measures, Detective measures and Corrective measures. With the help of planning methodology the impact of disaster can be minimized and Business continuity may be achieved.

1.14 Further Readings

1. Information Security Assurance: Framework, Standards & Industry Best Practices (PGDCS-05), Study Materials of Uttarakhand Open University, Haldwani, for Post-Graduate Diploma in Cyber Security
2. *Disaster recovery.* Computer Business Research
3. *Disaster Recovery and Business Continuity, version 2011.* IBM.
4. A Brief History of Disaster Recovery, safetynet247.co.uk .
5. https://www.google.co.in//Image

1.15 Assignments

1. What is disaster recovery plan (DRP)?
2. Why DRP is important? Write its benefits.
3. What is Disaster recovery? What are its impacts on different organization?
4. Describe different types of Disasters with appropriate example.
5. What is the relationship between BCP and DRP?
6. What are different types of Disaster recovery control measures?
7. Write the steps of Disaster Recovery planning methodology.

Unit 2: Digital Signatures 2

Unit Structure

2.1 Learning Objectives

After learning this unit, you should be able to

- Understand the concept of digital signature.
- Understand Mechanism of Digital signature
- Know the uses and Importance of Digital signature.

Know the mechanism and use of digital signature certificates (DSC)

2.2 Introduction

Cryptography today involves more than encryption and decryption of messages. It also provides mechanisms for authenticating documents using a digital signature, which binds a document to the possessor of a particular key, while a digital time stamp binds a document to its creation at a particular time. These are important functions which must take the place of equivalent manual authentication procedures as we move into the digital age. Cryptography also plays an important part in the developing field of digital cash and electronic funds transfer.

The encryption techniques applied for the following purposes:

- To protect privacy and confidentiality.
- To transmit secure information (e.g. credit card details)
- To provide authentication of the sender of a message.
- To provide authentication of the time a message was sent.

2.3 What is a Digital Signature?

A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).

A digital signature is the electronic equivalent of a handwritten signature, verifying the authenticity of electronic documents. In fact, digital signatures provide even more security than their handwritten counterparts.

Some banks and package delivery companies use a system for electronically recording handwritten signatures. Some even go so far as to use biometric analysis to record the speed with which you write and even how hard you press down, ensuring the authenticity of the signature. However, this is not what is usually meant by digital signatures — a great relief to those of us with limited budgets and resources.

More often than not a digital signature uses a system of public key encryption to verify that a document has not been altered.

2.4 Applications of Digital Signature

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

2.5 Mechanism of Digital Signatures

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to

encrypt the hash. The encrypted hash - along with other information, such as the hashing algorithm - is the digital signature. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing.

The value of the hash is unique to the hashed data. Any change in the data, even changing or deleting a single character, results in a different value. This attribute enables others to validate the integrity of the data by using the signer's public key to decrypt the hash. If the decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed. If the two hashes don't match, the data has either been tampered with in some way (integrity) or the signature was created with a private key that doesn't correspond to the public key presented by the signer (authentication). A digital signature can be used with any kind of message - whether it is encrypted or not -- simply so the

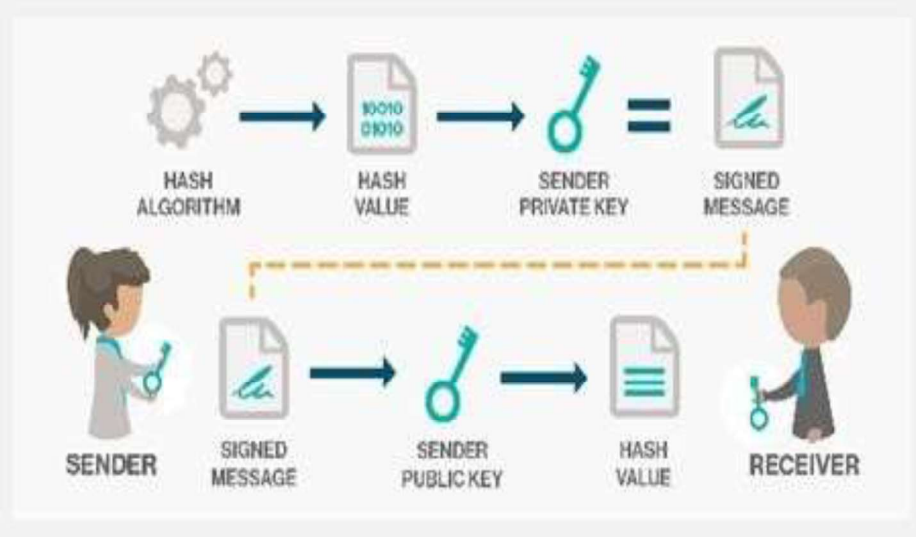


Fig: Digital Signature Process

receiver can be sure of the sender's identity and that the message arrived intact. Digital signatures make it difficult for the signer to deny having signed something (non-repudiation) - assuming their private key has not been compromised - as the digital signature is unique to both the document and the signer, and it binds them together. A digital certificate, an electronic document that contains the digital signature of the certificate- issuing authority, binds together a public key with an

identity and can be used to verify a public key belongs to a particular person or entity.

Most modern email programs support the use of digital signatures and digital certificates, making it easy to sign any outgoing emails and validate digitally signed incoming messages. Digital signatures are also used extensively to provide proof of authenticity, data integrity and non- repudiation of communications and transactions conducted over the Internet.

2.6 What Is Public Key Encryption?

Public key encryption (PKE) is a cryptographic system that uses a system of two keys:

- a **private key**, which only you use (and of course protect with a **well-chosen, carefully protected passphrase**); and
- a **public key**, which other people use. Public keys are often stored on **public key servers**.

A document that is encrypted with one of these keys can be decrypted only with the other key in the pair.

For example, let's say that Alice wants to send a message to Bob using **PGP** (a popular public key encryption system). She encrypts the message with Bob's public key and sends it using her favorite email program. Once the message is encrypted with Bob's public key, only Bob can decrypt the message using his private key. Even major governments using supercomputers would have to work for a very long time to decrypt this message without the private key.

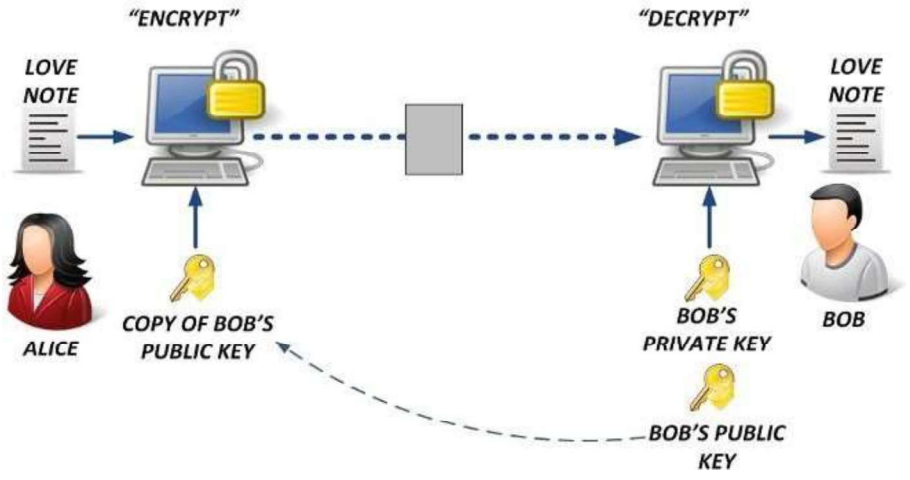


Fig: Public Key Encryption Process

2.7 What does PKE Have to do with Digital Signatures?

Digital signatures often use a public key encryption system. Consider Alice and Bob again: how can Bob be sure that it was really Alice who sent the message, and not the criminally-minded Eve pretending to be Alice?

This is where digital signatures come in. Before encrypting the message to Bob, Alice can sign the message using her private key; when Bob decrypts the message, he can verify the signature using her public key. Here's how it works:

1. Alice creates a digest of the message — a sort of digital fingerprint. If the message changes, so does the digest.
2. Alice then encrypts the digest with her private key. The encrypted digest is the digital signature.
3. The encrypted digest is sent to Bob along with the message.
4. When Bob receives the message, he decrypts the digest using Alice's public key.
5. Bob then creates a digest of the message using the same function that Alice used.
6. Bob compares the digest that he created with the one that Alice encrypted. If the digests match, then Bob can be confident that the signed message is indeed from Alice. If they don't match, then the message has been tampered with — or isn't from Alice at all.

If this sounds complicated, rest assured that the software makes it all very easy.

2.8 How to verify a signature from someone?

That's where digital certificates and certificate authorities come in. Let's start with how it works in PGP. Say that someone claiming to be Bob's acquaintance Carol sends a message to Alice. How does Alice know that Carol is who she claims to be? Carol signed the message with her own private key, which has been digitally

signed by Bob (essentially saying, "I trust that this key is valid and hope that you will, too"). Because Alice knows and trusts Bob's key (and therefore his signature), Alice can trust that Carol's key is valid — so the person claiming to be Carol almost certainly really is Carol.

Furthermore, once Alice trusts Carol's key, she can sign it. Then someone who has and trusts Alice's key will be able to trust Carol's. This builds a web of trust among PGP users.

However, this informal web of trust may not be rigorous enough for business or government purposes. For these cases, third-party entities known as certificate authorities validate identities and issue certificates. These certificates, signed with the CAs' well-known and trusted keys, can be used to verify someone's identity.

2.9 How Digital Signatures are used?

Digital signatures can be used anywhere that a system for authenticating data is necessary, i.e. anywhere a handwritten signature could be used but can't or shouldn't for some reason — online banking or payroll transactions, for example, or web registration for college courses. A system of digital signatures and encryption is used in e-commerce all the time, to protect confidential information.

2.10 Model of Digital Signature

As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration.

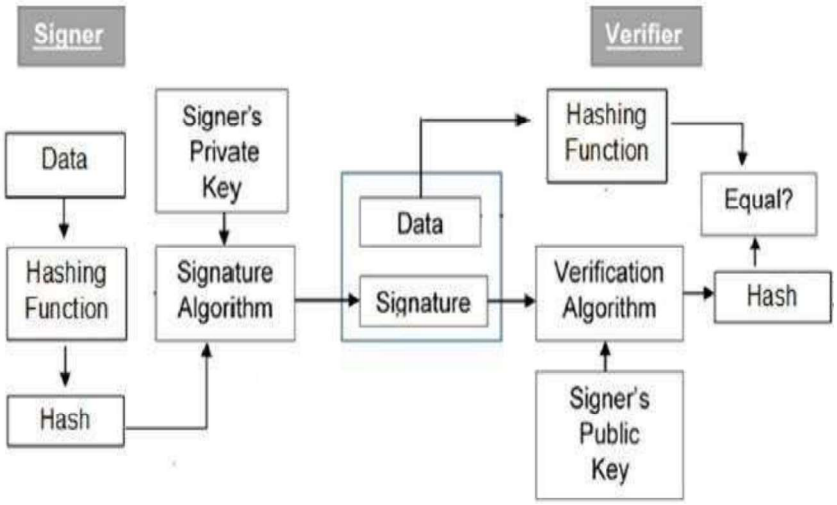


Fig: Digital Signature Process

The following points explain the entire process in detail −

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.

Let us assume RSA is used as the signing algorithm. As discussed in public key encryption chapter, the encryption/signing process using RSA involves modular exponentiation.

Signing large data through modular exponentiation is computationally expensive and time consuming. The hash of the data is a relatively small digest of the data, hence signing a hash is more efficient than signing the entire data.

2.11 Importance of Digital Signature

Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.

Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature −

- **Message authentication** − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- **Data Integrity** − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
- **Non-repudiation** − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signatureon a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely − Privacy, Authentication, Integrity, and Non-repudiation.

2.12 Applications of digital signatures

As organizations move away from paper documents with ink signatures or authenticity stamps, digital signatures can provide added assurances of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory. The United States Government Printing Office (GPO) publishes electronic versions of the budget, public and private laws, and congressional bills with digital signatures. Universities including Penn State, University of Chicago, and Stanford are publishing electronic

student transcripts with digital signatures. Below are some common reasons for applying a digital signature to communications:

2.12.1 Authentication

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

2.12.2 Integrity

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

2.12.3 Non-repudiation

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Note that these authentications, non-repudiation etc. properties rely on the secret key not having been revoked prior to its usage. Public revocation of a key-pair is a required ability; else leaked secret keys would continue to implicate the claimed

owner of the key-pair. Checking revocation status requires an "online" check, e.g. checking a "Certificate Revocation List" or via the "Online Certificate Status Protocol". Very roughly this is analogous to a vendor who receives credit-cards first checking online with the credit- card issuer to find if a given card has been reported lost or stolen. Of course, with stolen key pairs, the theft is often discovered only after the secret key's use, e.g., to sign a bogus certificate for espionage purpose.

2.13 Encryption with Digital Signature

In many digital communications, it is desirable to exchange an encrypted message than plaintext to achieve confidentiality. In public key encryption scheme, a public (encryption) key of sender is available in open domain, and hence anyone can spoof his identity and send any encrypted message to the receiver.

This makes it essential for users employing PKC for encryption to seek digital signatures along with encrypted data to be assured of message authentication and non-repudiation.

This can archive by combining digital signatures with encryption scheme. Let us briefly discuss how to achieve this requirement. There are **two possibilities, sign-then-encrypt** and **encrypt-then-sign**.

However, the crypto system based on sign-then-encrypt can be exploited by receiver to spoof identity of sender and sent that data to third party. Hence, this method is not preferred. The process of encrypt-then-sign is more reliable and widely adopted. This is depicted in the following illustration-

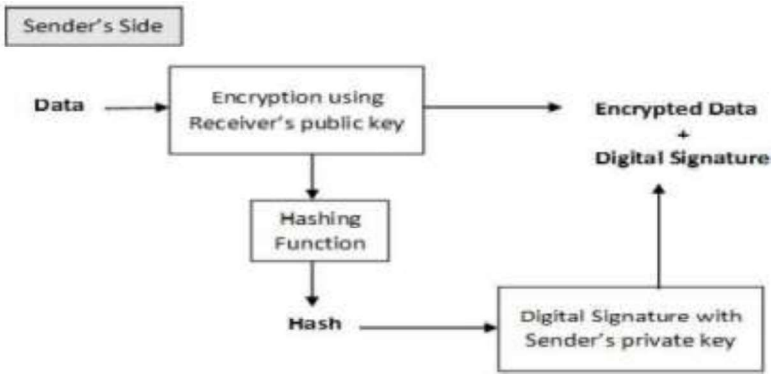


Fig Encryption with Digital Signature

The receiver after receiving the encrypted data and signature on it, first verifies the signature using sender's public key. After ensuring the validity of the signature, he then retrieves the data through decryption using his private key.

2.14 Digital Signature to Electronic Signature

Digital Signature was the term defined in the old I.T. Act, 2000. Electronic Signature is the term defined by the amended act (I.T. Act, 2008). The concept of Electronic Signature is broader than Digital Signature. Section 3 of the Act delivers for the verification of Electronic Records by affixing Digital Signature.

As per the amendment, verification of electronic record by electronic signature or electronic authentication technique shall be considered reliable.

According to the United Nations Commission on International Trade Law (UNCITRAL), electronic authentication and signature methods may be classified into the following categories −

- Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.
- Those bases on the physical features of the user, i.e., biometrics.
- Those based on the possession of an object by the user, i.e., codes or other information stored on a magnetic card.
- Types of authentication and signature methods that, without falling under any of the above categories might also be used to indicate the originator of an electronic communication (Such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message).
- According to the UNCITRAL Model Law on Electronic Signatures, the following technologies are presently in use
- Digital Signature within a public key infrastructure (PKI)
- Biometric Device
- PINs
- Passwords
- Scanned handwritten signature
- Signature by Digital Pen

- Clickable “OK” or “I Accept” or “I Agree” click boxes

2.15 Digital Signatures Versus Ink on Paper Signatures

An ink signature could be replicated from one document to another by copying the image manually or digitally, but to have credible signature copies that can resist some scrutiny is a significant manual or technical skill, and to produce ink signature copies that resist professional scrutiny is very difficult. Digital signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document. Paper contracts sometimes have the ink signature block on the last page, and the previous pages may be replaced after a signature is applied. Digital signatures can be applied to an entire document, such that the digital signature on the last page will indicate tampering if any data on any of the pages have been altered, but this can also be achieved by signing with ink and numbering all pages of the contract.

2.15.1 Some Digital Signature Algorithms

- RSA-based signature schemes, such as RSA-PSS
- DSA and its elliptic curve variant ECDSA
- ElGamal signature scheme as the predecessor to DSA, and variants Schnorr signature and Point cheval–Stern signature algorithm
- Rabin signature algorithm
- Pairing-based schemes such as BLS
- Undeniable signatures
- Aggregate signature - a signature scheme that supports aggregation: Given n signatures on n messages from n users, it is possible to aggregate all these signatures into a single signature whose size is constant in the number of users. This single signature will convince the verifier that the n users did indeed sign the n original messages.
- Signatures with efficient protocols - are signature schemes that facilitate efficient cryptographic protocols such as zero-knowledge proofs or secure computation.

2.16 The Current State of Use- Legal and Practical

All digital signature schemes share the following basic prerequisites regardless of cryptographic theory or legal provision:

1. **Quality algorithms**: Some public-key algorithms are known to be insecure, practical attacks against them having been discovered.
2. **Quality implementations:** An implementation of a good algorithm (or protocol) with mistake(s) will not work.
3. **The private key must remain private:** If the private key becomes known to any other party, that party can produce perfect digital signatures of anything whatsoever.
4. The public key owner must be verifiable: A public key associated with Bob actually came from Bob. This is commonly done using a public key infrastructure (PKI) and the public key ↔ user association is attested by the operator of the PKI (called a certificate authority). For 'open' PKIs in which anyone can request such an attestation (universally embodied in a cryptographically protected identity certificate), the possibility of mistaken attestation is nontrivial. Commercial PKI operators have suffered several publicly known problems. Such mistakes could lead to falsely signed, and thus wrongly attributed, documents. 'Closed' PKI systems are more expensive, but less easily subverted in this way.
5. Users (and their software) must carry out the signature protocol properly.

Only if all of these conditions are met will a digital signature actually be any evidence of who sent the message, and therefore of their assent to its contents.

2.17 Industry Standards

Some industries have established common interoperability standards for the use of digital signatures between members of the industry and with regulators. These include the Automotive Network Exchange for the automobile industry and the SAFE-Bio Pharma Association for the healthcare industry.

2.17.1 Using Separate Key Pairs for Signing and Encryption

In several countries, a digital signature has a status somewhat like that of a traditional pen and paper signature, like in the EU digital signature legislation. Generally, these provisions mean that anything digitally signed legally binds the signer of the document to the terms therein. For that reason, it is often thought best to use separate key pairs for encrypting and signing. Using the encryption key pair, a person can engage in an encrypted conversation (e.g., regarding a real estate transaction), but the encryption does not legally sign every message he sends. Only when both parties come to an agreement do they sign a contract with their signing keys, and only then are they legally bound by the terms of a specific document. After signing, the document can be sent over the encrypted link. If a signing key is lost or compromised, it can be revoked to mitigate any future transactions. If an encryption key is lost, a backup or key escrow should be utilized to continue viewing encrypted content. Signing keys should never be backed up or escrowed unless the backup destination is securely encrypted.

2.18 Introduction to Digital Signature Certificates (DSC)

Digital Signature Certificate (DSC) is a secure **digital** key that certifies the identity of the holder, issued by a Certifying Authority (CA). A **digital certificate** is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web.

Digital Signature Certificates (DSC) are the digital equivalent (that is electronic format) of physical or paper certificates. Few Examples of physical certificates are drivers' licenses, passports or membership cards. Certificates serve as proof of identity of an individual for a certain purpose; for example, a driver's license identifies someone who can legally drive in a particular country. Likewise, a digital certificate can be presented electronically to prove one's identity, to access information or services on the Internet or to sign certain documents digitally.

2.19 Digital Signature Certificates (DSC) Polices

A Digital Signature is a method of verifying the authenticity of an electronic document. Digital signatures are going to play an important role in our lives with the gradual electronization of records and documents. The IT Act has given legal

recognition to digital signature meaning, thereby, that legally it has the same value as handwritten or signed signatures affixed to a document for its verification. The Information Technology Act, 2000 provides the required legal sanctity to the digital signatures based on asymmetric cryptosystems. The digital signatures are now accepted at par with handwritten signatures and the electronic documents that have been digitally signed are treated at par with paper documents.

2.20 How does a Digital Signature Certificate Work?

A Digital Signature Certificate explicitly associates the identity of an individual/device with a pair of electronic keys - public and private keys - and this association is endorsed by the CA. The certificate contains information about a user's identity (for example, their name, pin code, country, email address, the date the certificate was issued and the name of the Certifying Authority that issued it).

These keys complement each other in that one does not function in the absence of the other. They are used by browsers and servers to encrypt and decrypt information regarding the identity of the certificate user during information exchange processes. The private key is stored on the user's computer hard disk or on an external device such as a token. The user retains control of the private key; it can only be used with the issued password. The public key is disseminated with the encrypted information. The authentication process fails if either one of these keys in not available or do not match. This means that the encrypted data cannot be decrypted and therefore, is inaccessible to unauthorized parties.

2.21 Use of Digital Certificates

Three uses are outlined here. Your digital certificate could be used to allow you to access membership-based web sites automatically without entering a user name and password. It can allow others to verify your "signed" e-mail or other electronic documents, assuring your intended reader(s) that you are the genuine author of the documents, and that the content has not been corrupted or tampered with in any way. Finally, digital certificates enable others to send private messages to you: anyone else who gets his/her hands on a message meant for you will not be able to read it.

2.21.1 Sending Digitally Signed Mail

You can use your Digital Certificate to digitally sign your emails sent through Outlook Express / MS-Outlook etc. Digitally signing the mail authenticates your identity and enables the receiver to ensure that the mail has come from you only. It also ensures that the content of the mail is not tampered in the transit and the mail received by the receiver is the same what you have sent.

2.22 Who Needs a Digital Signature Certificate?

MCA21 Mission Mode Project (MCA21) is the e-governance initiative from the Ministry of Corporate Affairs, Government of India. Under MCA21, Every person who is required to sign manual documents and returns filed with ROC is required to obtain a Digital Signature Certificate (DSC). Accordingly following have to obtain Digital Signature Certificate:

1. Directors
2. Auditors
3. Company Secretaries
4. Bank Officials - for Registration and Satisfaction of Charges
5. Other Authorized Signatories.

2.23 Types Of Digital Signature Certificate

There are 3 types of Digital Signature Certificates, having different security levels, namely:-

- Class-1
- Class-2
- Class-3

For filing documents under **MCA21**, a Class**-2** Digital Signature Certificate issued by a Licensed Registration Authority is required. We also offer Class 1 and 3 besides Class 2 certificates.

2.24 Let us Sum-up

The digital signature has become a significant tool in international commerce. Because a digital signature provides the legal elements of a traditional hand written signature (i.e., evidence, ceremony, approval, and efficiency) and enhanced security, integrity, and authenticity, additional businesses will likely use digital signatures in an increasing percentage of their commercial transactions. Secure electronic commerce provides a "paperless" way of transacting business.

Currently, the PKI-digital signature is the best type of signature for electronic contracts. PKI-digital signature software is inexpensive and the technology is mathematically improbable to break. With future advances in technology, other types of electronic signatures may replace the PKI- digital signature. Regardless of the technology used, digital and electronic signatures are an increasingly significant part of commerce and will continue to evolve.

2.25 Further Reading

1 Digital Signature. (2016). Retrieved Jan. 09, 2016, from Wikipedia: https://en.wikipedia.org/wiki/Digital_signature available under the Creative Commons Attribution-Share Alike License

2 Course-I-Fundamentals of Information Security, Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e- Governance and Cyber Security

3 W. Everett Lupton, Comment, The Digital Signature: Your Identity by the Numbers, Volume VI, Issue 2, Fall 1999.

4 https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm

5 https://www.tutorialspoint.com/information_security_cyber_law/digital_and_electronic_signatures.htm

2.26 Assignments

1. What is a Digital Signature? What is its purpose?
2. Explain the working of a Digital Signature.
3. Compare Digital Signatures with Ink-on paper signatures.
4. Write the uses of Digital Certificates.
5. Discuss the importance of Digital Signature in Information Security.

Unit 3: Ethical Hacking and Penetration Testing

3

Unit Structure

3.1 Learning Objectives

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

- Understand the meaning of hacking.
- Know the benefits of Penetration Testing and Ethical Hacking.
- Identify various types of penetration testing.
- Classify various types of Hackers.
- Analyze various phases involved in Penetration Testing.
- Know various hacking tools and techniques.

3.2 Introduction

Computers have become mandatory to run a successful business. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and cybercrime. Cybercrime is using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data etc**. Cybercrimes cost many organizations millions of dollars every year**. Businesses need to protect themselves against such attacks.

Most people think hackers have extraordinary skill and knowledge that allow them to hack into computer systems and find valuable information. The term hacker conjures up images of a young computer whiz who types a few commands at a computer screen—and poof! The computer spits out passwords, account numbers, or other confidential data. In reality, a good hacker, or security professional acting as an ethical hacker, just has to understand how a computer system works and know what tools to employ in order to find a security weakness. In this unit we book will discuss different types of hacking, some techniques and software tools that many hackers use to gather valuable data and attack computer systems.

3.3 About Ethical Hacking and Penetration Testing

There are many definitions of hacking. In this unit, we will define **hacking as the process of identifying weakness in computer systems and/or networks and exploiting the weaknesses to gain access**. An example of hacking is using by passing the login algorithm to gain access to a system. A **hacker** is a person who finds and exploits weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

Vulnerability analysis and Penetration Testing, commonly known as Ethical Hacking is a branch wherein, hackers engage in sanctioned hacking—that is, hacking with permission from the system's owner. In the world of ethical hacking, most tend to use the term pen tester, which is short for penetration tester. Pen Testers penetrate systems like a hacker, but for "benign" purposes. As an ethical hacker and future test candidate you must become familiar with the jargons of the trade. Here are some of the terms you will encounter in pen testing.

Glossary

1. **Hack Value:** This term describes a target that may attract an above- average level of attention to an attacker. Presumably because this target is attractive, it has more value to an attacker because of what it may contain.
2. **Target of Evaluation (TOE):** A TOE is a system or resource that is being evaluated for vulnerabilities. A TOE would be specified in a contract with the client.
3. **Attack:** This is the act of targeting and actively engaging aTOE.
4. **Exploit:** This is a clearly defined way to breach the security of a system.
5. **Zero Day:** This describes a threat or vulnerability that is unknown to developers and has not been addressed. It is considered a serious problem in many cases.
6. **Security:** This is described as a state of well-being in an environment where only actions that are defined are allowed.
7. **Threat:** This is considered to be a potential violation of security.
8. **Vulnerability:** This is a weakness in a system that can be attacked and used as

an entry point into an environment.

9. **Daisy Chaining:** This is the act of performing several hacking attacks in sequence with each building on or acting on the results of the previous action. As an ethical hacker, you will be expected to take on the role and use the mind-set and skills of an attacker to simulate a malicious attack. The idea is that ethical hackers understand both sides, the good and the bad, and use this knowledge to help their clients. By understanding both sides of the equation, you will be better prepared to defend yourself successfully.

Some things to remember about being an ethical hacker are:

- You must have explicit permission in writing from the company being tested prior to starting any activity. Legally, the person or persons that must approve this activity or changes to the plan must be the owner of the company or their authorized representative. If the scope changes, update the contracts to reflect those changes before performing the new tasks.
- You will use the same tactics and strategies as malicious attackers.
- You have every potential to cause harm that a malicious attack will have and should always consider the effects of every action you carry out.
- You must have knowledge of the target and the weaknesses it possesses.
- You must have clearly defined rules of engagement prior to beginning your assigned job.
- You must never reveal any information pertaining to a client to anyone but the client. If the client asks you to stop a test, do so immediately.
- You must provide a report of your results and, if asked, a brief on any deficiencies found during a test.
- You may be asked to work with the client to fix any problems that you find.
- As an ethical hacker you must agree to the following code of ethics:
- Keep private and confidential information gained in your professional work (in particular as it pertains to client lists and client personal information). Do not collect, give, sell, or transfer any personal information (such as name, e-mail address, social security number, or other unique identifier) to a third party without prior client consent.
- Protect the intellectual property of others by relying on your own innovation and efforts, thus ensuring that all benefits vest with its originator.
- Disclose to appropriate persons or authorities potential dangers to any e-

commerce clients, the Internet community, or the public, that you reasonably believe to be associated with a particular set or type of electronic transactions or related software or hardware.

- Provide service in your areas of competence; be honest and forthright about any limitations of your experience and education. Ensure that you are qualified for any project on which you work or propose to work by an appropriate combination of education, training, and experience.
- Never knowingly use software or a process that is obtained or retained either illegally or unethically.
- Do not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.
- Use the property of a client or employer only in ways properly authorized, and with the owner's knowledge and consent.
- Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.
- Ensure good management for any project you lead, including effective procedures for promotion of quality and full disclosure of risk.
- Add to the knowledge of the e-commerce profession by constant study, share the lessons of your experience with fellow EC- Council members, and promote public awareness of the benefits of e-commerce.
- Conduct yourself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in your knowledge and integrity.
- Ensure ethical conduct and professional care at all times on all professional assignments without prejudice.
- Do not associate with malicious hackers or engage in any malicious activities.
- Do not purposefully compromise or allow the client organization's systems to be compromised in the course of your professional dealings.
- Ensure all pen testing activities are authorized and within legal limits.
- Do not take part in any black hat activity or be associated with any black hat community that serves to endanger networks.
- Do not take part in any underground hacking community for purposes of preaching and expanding black hat activities.

- Do not make inappropriate references to the certification or misleading use of certificates, marks or logos in publications, catalogs, documents, or speeches.
- Do not violate any law of the land or have any previous conviction.
- Under the right circumstances and with proper planning and goals in mind, you can provide a wealth of valuable information to your target organization. Working with your client, you should analyze your results thoroughly and determine which areas need attention and which need none at all. Your client will determine the perfect balance of security versus convenience. If the problems you uncover necessitate action, the next challenge is to ensure that existing usability is not adversely affected if security controls are modified or if new ones are put in place. Security and convenience often conflict: the more secure a system becomes, the less convenient it tends to be.

A pen test is the next logical step beyond ethical hacking. Although ethical hacking sometimes occurs without a formal set of rules of engagement, pen testing does require rules to be agreed on in advance in every case.

3.4 Types of Pen testing

When a pen test is performed it typically takes one of three forms: white box, gray box, or black box. The three forms of testing are important to differentiate between, as you may be asked to perform any one of them at some point during your career, so let's take a moment to describe each:

3.4.1 Black Box

A type of testing in which the pen tester has little or no knowledge of the target is said to be Black Box testing. This situation is designed to closely emulate the situation an actual attacker would encounter as they would presumably have an extremely low level of knowledge of the target going in.

3.4.2 Gray Box

It is a form of testing where the knowledge given to the testing party is limited. In this type of test, the tester acquires knowledge such as IP addresses, operating systems, and the network environment, but that information is limited. This type of

test would closely emulate the type of knowledge that someone on the inside might have; such a person would have some knowledge of a target, but not always all of it.

3.4.3 White Box

White Box is a form of testing in which the information given to the tester is complete. This means that the pen tester is given all information about the target system. This type of test is typically done internally or by teams that perform internal audits of systems.

3.4.4 CIA Triad

An ethical hacker is trying to preserve what is known as the CIA triad: confidentiality, integrity, and availability. The following list describes these core concepts and what they mean. Keep these concepts in mind when performing the tasks and responsibilities of a pen tester:

a) **Confidentiality:** The core principle that refers to the safeguarding of information and keeping it away from those not authorized to possess it. Examples of controls that preserve confidentiality are permissions and encryption.
b) **Integrity:** Deals with keeping information in a format that is true and correct to its original purposes, meaning that the data that the receiver accesses is the data the creator intended them to have.
c) **Availability:** The final and possibly one of the most important items that you can perform. Availability deals with keeping information and resources available to those who need to use it. Information or resources, no matter how safe and sound, are only useful if they are available when called upon.

CIA is possibly the most important set of goals to preserve when you are assessing and planning security for a system. An aggressor will attempt to break or disrupt these goals when targeting a system. As an ethical hacker your job is to find, assess, and remedy these issues whenever they are discovered to prevent an aggressor from doing harm. Another way of looking at this balance is to observe the other side of the triad and how the balance is lost. Any of the following break the CIA triad:

- **Disclosure** is the inadvertent, accidental, or malicious revealing or accessing of information or resources to an outside party. If you are not supposed to have access to an object, you should never have access to it.
- **Alteration** is the counter to integrity; it deals with the unauthorized or other forms of modifying information. This modification can be corruption, accidental access, or malicious in nature.
- **Disruption** (also known as loss) means that access to information or resources has been lost when it should not have. Information is useless if it is not there when it is needed. Although information or other resources can never be 100-percent available, some organizations spend the time and money to get 99.999-percent uptime, which averages about 6 minutes of downtime per year.

Think of these last three points as the anti-CIA triad or the inverse of the CIA triad. The CIA triad deals with preserving information and resources, whereas the anti-CIA triad deals with violating those points. You can also think of the anti-CIA as dealing more with the aggressor's perspective rather than the defender's.

An ethical hacker will be entrusted with ensuring that the CIA triad is preserved at all times and threats are dealt with in the most appropriate manner available (as required by the organization's own goals, legal requirements, and other needs). For example, consider what could happen if an investment firm or defense contractor suffered a disclosure incident at the hands of a malicious party. The results would be catastrophic.

In this unit you will encounter legal issues several times. You are responsible for checking the details of what laws apply to you, and you will need to get a lawyer to do that. You should be conscious of the law at all times and recognize when you may be crossing into a legal area that you need advice on. Both ethical hackers and hackers follow similar processes as the one outlined here though in less or stricter ways. Hackers are able to write their own rules and use the process however they want without concern or reasons except those that make sense to them. Ethical hackers follow the same type of process as seen here with little modification, but there is something that they have added that hackers do not have: Ethical hackers will not only have permission prior to starting the first phase, but they will also be generating a report that they will present at the end of the

process. The ethical hacker will be expected to keep detailed notes about what is procured at each phase for later generation of that report.

When you decide to carry out this process, seek your client's guidance and ask the following questions along with any others that you think are relative. During this phase, your goal is to clearly determine why a pen test and its associated tasks are necessary.

- Why did the client request a pen test?
- What is the function or mission of the organization to be tested?
- What will be the constraints or rules of engagement for the test?
- What data and services will be included as part of the test?
- Who is the data owner?
- What results are expected at the conclusion of the test?
- What will be done with the results when presented?
- What is the budget?
- What are the expected costs?
- What resources will be made available?
- What actions will be allowed as part of the test?
- When will the tests be performed?
- Will insiders be notified?
- Will the test be performed as black or white box?
- What conditions will determine the success of the test?
- Who will be the emergency contacts?
- Pen testing can take several forms. You must decide, along with your client, which tests are appropriate and will yield the desired results. Tests that can be part of a pen test include the following:
- An insider attack is intended to mimic the actions that may be undertaken by internal employees or parties who have authorized access to a system.
- An outsider attack is intended to mimic those actions and attacks that would be undertaken by an outside party.
- A stolen equipment attack is a type of attack where an aggressor steals a

piece of equipment and uses it to gain access or extracts the information desired from the equipment itself.

- A social engineering attack is a form of attack where the pen tester targets the users of a system seeking to extract the needed information.

The attack exploits the trust inherent in human nature. Once you discuss each test, determine the suitability of each, and evaluate the potential advantages and side effects, you can finalize the planning and contracts and begin testing.

3.5 Vulnerability Research and Tools

An important part of your toolkit as an ethical hacker will be the information gathered from vulnerability research. This process involves searching for and uncovering vulnerabilities in a system and determining their nature. Additionally, the research seeks to classify each vulnerability as high, medium, or low. You or other security personnel can use this research to keep up to date on the latest weaknesses involving software, hardware, and environments. The benefit of having this information is that an administrator or other personnel could use this information to position defenses. Additionally, the information may show where to place new resources or be used to plan monitoring. Vulnerability research is not the same as ethical hacking in that it passively uncovers security issues whereas the process of ethical hacking actively looks for the vulnerabilities.

3.6 Ethics and the Law

As an ethical hacker, you need to be aware of the law and how it affects what you will do. Ignorance or lack of an understanding of the law is not only a bad idea, but it can quickly put you out of business—or even in prison. In fact, under some situations the crime may be serious enough to get you prosecuted in several jurisdictions in different states, counties, or even countries due to the highly distributed nature of the Internet. Of course, prosecution of a crime can also be difficult considering the web of various legal systems in play. A mix of common, military and civil laws exists, requiring knowledge of a given legal system to be successful in any move toward prosecution.

Depending on when and where you're testing takes place, it is even possible for you to break religious laws. Although you may never encounter this problem, it is something that you should be aware of—you never know what type of laws you may break.

Always ensure that you exercise the utmost care and concern to ensure that you observe proper safety and avoid legal issues. When your client has determined their goals along with your input, the contract must be put in place. Remember the following points when developing a contract and establishing guidelines:

Trust The client is placing trust in you to use the proper discretion when performing a test. If you break this trust, it can lead to the questioning of other details such as the results of the test. Legal Implications Breaking a limit placed on a test may be sufficient cause for your client to take legal action against you.

When we work in this area of specialization, it is paramount to know laws of various countries. Since most of the laws have their roots in US Laws, it is mandatory that we go through them.

3.7 Hacking

Hacking is any technical effort to manipulate the normal behavior of network connections and connected computers or systems. A hacker is any person engaged in hacking.

3.7.1 Culture of Hacking

To be accepted as hacker one should have the attitude, behave as though one have the attitude, and belief in that. Some of them can be listed as follows:

- Strong zeal to learn and obtain more knowledge
- Breaking law
- Anonymity
- Stealing confidential information.

3.7.2 Types of Hackers

Hackers can be classified in to the following types based on their depth of knowledge and activities.

a. **White Hats:** White hats are the good guys, the ethical hackers who use their hacking skills for defensive purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge to locate weaknesses and implement countermeasures.
b. **Black Hats:** Black hats are the bad guys: the malicious hackers or crackers who use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote systems, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and just cause problems for their targets. Black-hat hackers and crackers can easily be differentiated from white-hat hackers because their actions are malicious. This is the traditional definition of a hacker and what most people consider a hacker to be.
c. **Gray Hats:** Gray hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Grayhat hackers may just be interested in hacking tools and technologies and are not malicious black hats. Gray hats are self-proclaimed ethical hackers, who are interested in hacker tools.
d. **Suicide Hackers:** Individuals who will aim to bring down the critical infrastructure whatever the consequence may be.
e. **Script Kiddies:** In hacker culture a script kiddie or skiddie are unskilled individuals who use scripts or programs developed by others to attack computer systems and networks and deface websites. It is generally assumed that script kiddies are juveniles who lack the ability to write sophisticated hacking programs or exploits on their own, and that their objective is to try to impress their friends or gain credit in computer-enthusiast communities. The term is typically intended as an insult.
f. **Hacktivist:** Detects and sometimes reports or exploits security vulnerabilities as a form of social activitism. A hacktivist is a hacker who utilizes technology to announce a social ideological, religious or political message. In general most

hacktivism involve defacement or denial of service attacks. Hacktivits are also known as Neo hackers.

3.8 Phases of Penetration Testing

As brought out earlier that a Pen-tester uses the same methodology as a hacker does, we will be using this terminology interchangeably

3.8.1 Foot printing

Now let's circle back around to the first step in the process of ethical hacking i.e. Foot printing. Foot printing, or reconnaissance, is a method of observing and collecting information about a potential target with the intention of finding a way to attack the target. Foot printing looks for information and later analyzes it, looking for weaknesses or potential vulnerabilities. The end result should be a profile of the target that is a rough picture but one that gives enough data to plan the next phase of scanning. When you conduct foot printing- as with all phases and processes described in this unit—you must be quite methodical. A careless or haphazard process of collecting information can waste time when moving forward or, in a worst-case scenario, cause the attack to fail. The smart or careful attacker spends a good amount of time in this phase gathering and confirming information. Foot printing generally entails the following steps to ensure proper information retrieval:

1 Collect information that is publicly available about a target (for example, host and network information).
2 Ascertain the operating system(s) in use in the environment, including web server and web application data where possible.
3 Issue queries such as whois, DNS, network, and organizational queries.
4 Locate existing or potential vulnerabilities or exploits that exist in the current infrastructure that may be conducive to launching later attacks.

3.8.1.1 Why Perform Foot printing?

Foot printing is about gathering information and formulating a hacking strategy. With proper care you, as the attacking party, may be able to uncover the path of least resistance into an organization. Passively gathering information is by far the

easiest and most effective method. If done by a skilled, inventive, and curious party (you!), the amount of information that can be passively gathered is staggering. Expect to obtain information such as:

- Information about an organization's security posture and where potential loopholes may exist. This information will allow for adjustments to the hacking process that make it more productive.
- A database that paints a detailed picture with the maximum amount of information possible about the target.
- A network map using tools such as the Tracert utility to construct a picture of a target's Internet presence or Internet connectivity. Think of the network map as a roadmap leading you to a building; the map gets you there, but you still have to determine the floor plan of the building.

3.8.1.2 Goals of the Foot Printing Process

Before you start doing foot printing and learn the techniques, you must set some expectations as to what you are looking for and what you should have in your hands at the end of the process. Keep in mind that the list of information here is not exhaustive, nor should you expect to be able to obtain all the items from every target. The idea is for you to get as much information in this phase as you possibly can, but take your time!

Here's what you should look for:

- Network information
- Operating system information
- Organization information, such as CEO and employee information, office information, and contact numbers and e-mail
- Network blocks
- Network services
- Application and web application data and configuration information
- System architecture
- Intrusion detection and prevention systems
- Employee names

- Work experience

3.8.1.3 Types of Reconnaissance

Process of Reconnaissance can be categorized as Passive and Active Reconnaissance.

3.8.1.3.1 Passive Reconnaissance

This involves gathering information about a potential target without the targeted individual‘s or company‘s knowledge. Passive reconnaissance canbe as simple as watching a building to identify what time employees enter the building and when they leave. However, most reconnaissance is done sitting in front of a computer. When hackers are looking for information on a potential target, they commonly run an Internet search on an individual or company to gain information. This process when used to gather information regarding a TOE is generally called information gathering. Social engineering and dumpster diving are also considered passive information- gathering methods. These two methods will be discussed Sniffing the network is another means of passive reconnaissance and can yield useful information such as IP address ranges, naming conventions, hidden servers or networks, and other available services on the system or network. Sniffing tools are simple and easy to use and yield a great deal of valuable information. These tools are which literally let you see all the data that is transmitted on the network. Many times this includes usernames and passwords and other sensitive data. Examples: Domain name lookup, Whois, NSlookup, Sam Spade. Information that can be gathered during this phase includes:

- IP address ranges
- Namespaces
- Employee information
- Phone numbers
- Facility information
- Job information

3.8.1.3.2 Active reconnaissance

This involves probing the network to discover individual hosts, IP addresses, and services on the network. This process involves more risk of detection than passive reconnaissance and is sometimes called rattling the doorknobs. Active reconnaissance can give a hacker an indication of security measures in place (is the front door locked?), but the process also increases the chance of being caught or at least raising suspicion. Many software tools that perform active reconnaissance can be traced back to the computer that is running the tools, thus increasing the chance of detection for the hacker. Both passive and active reconnaissance can lead to the discovery of useful information to use in an attack. For example, it's usually easy to find the type of web server and the operating system (OS) version number that a company is using. This information may enable a hacker to find vulnerability in that OS version and exploit the vulnerability to gain more access. Foot printing takes advantage of the information that is carelessly exposed or disposed of inadvertently.

3.8.2 Scanning

It focuses on an active engagement of the target with the intention of obtaining more information. Scanning the target network will ultimately locate active hosts that can then be targeted in a later phase. Foot printing helps identify potential targets, but not all may be viable or active hosts. Once scanning determines which hosts are active and what the network looks like, a more refined process can take place.

Scanning involves taking the information discovered during reconnaissance and using it to examine the network.

Scanning is of two types.

i. **Network Scanning**: Network scanning is a procedure for identifying active hosts on a network. Hosts are identified by their individual IP addresses. Network- scanning tools attempt to identify all the live or responding hosts on the network and their corresponding IP addresses.
ii. **Vulnerability Scanning:** Vulnerability scanning is the process of proactively

identifying the vulnerabilities of computer systems on a network. Generally, a vulnerability scanner first identifies the operating system and version number, including service packs that may be installed. Then, the scanner identifies weaknesses or vulnerabilities in the operating system.

During this phase most commonly used tools are:

- Pings
- Ping sweeps
- Port scans
- Tracert

Hackers are seeking any information that can help them perpetrate an attack on a target, such as the following:

- IP addresses and open/closed ports on live hosts
- Information on the operating system(s) and the system architecture
- Services or processes running on hosts

Scanning is a set of procedures used to identify hosts, ports, and services on a target network. Scanning is considered part of the intelligence-gathering process an attacker uses to gain information about the targeted environment. Expect the information that is gathered during this phase to take a good amount of time to analyze, which will vary depending on how good you are at reading the resulting information. If you have performed your initial reconnaissance well, however, this process should not be complicated. Your knowledge will help you not only target your initial scans better, but also better determine how to decipher certain parts of the results. To successfully negotiate the scanning phase, you need a good understanding of networks, protocols, and operating systems.

3.8.3 Enumeration

The last phase before you attempt to gain access to a system is the enumeration phase. Enumeration is the systematic probing of a target with the goal of obtaining user lists, routing tables, and protocols from the system. This phase represents a significant shift in your process; it is the initial transition from being on the outside looking in to moving to the inside of the system to gather data. Information such as shares, users, groups, applications, protocols, and banners all

proved useful in getting to know your target, and this information is now carried forward into the attack phase.

Enumeration occurs after scanning and is the process of gathering and compiling usernames, machine names, network resources, shares, and services. It also refers to actively querying or connecting to a target system to acquire this information. Hackers need to be methodical in their approach to hacking. The following steps are an example of those a hacker might perform in preparation for hacking a target system:

- Extract usernames using enumeration
- Group information
- Passwords
- Hidden shares
- Device information
- Network layout
- Protocol information
- Server data
- Service information.
- Gather information about the host using null sessions.
- Perform Windows enumeration using the SuperScan tool.
- Acquire the user accounts using the tool GetAcct.
- Perform SNMP port scanning.

The objective of enumeration is to identify a user account or system account for potential use in hacking the target system. It isn‘t necessary to find a system administrator account, because most account privileges can be escalated to allow the account more access than was previously granted.

3.8.4 Gaining Access

Once you have completed the first three phases, you can move into the system-hacking phase. At this point, the process becomes much more complex: You can’t complete the system hacking phase in a single pass. It involves using a

methodical approach that includes cracking passwords, escalating privileges, executing applications, hiding files, covering tracks, concealing evidence, and then pushing into a more involved attack. Phase 3 is when the real hacking takes place. Vulnerabilities exposed during the reconnaissance and scanning phase are now exploited to gain access to the target system. The hacking attack can be delivered to the target system via a local area network (LAN), either wired or wireless; local access to a PC; the Internet; or offline. Examples include stack based buffer overflows, denial of service, and session hijacking. Gaining access is known in the hacker world as owning the system because once a system has been hacked, the hacker has control and can use that system as they wish. In order to gain access in a system, hacker's first attempt is to crack the password. In the enumeration phase, you collected a wealth of information, including usernames. These usernames are important now because they give you something on which to focus your attack more closely. You use password cracking to obtain the credentials of a given account with the intention of using the account to gain authorized access to the system under the guise of an authentic user.

3.8.4.1 Password Cracking Techniques

Popular culture would have us believe that cracking a password is as simple as running some software and tapping a few buttons. The reality is that special techniques are used to recover passwords. For the most part, you can break these techniques into five categories, which you will explore in depth later in this chapter; but let's take a high-level look at them now:

i. **Dictionary Attacks**: An attack of this type takes the form of a password-cracking application that has a dictionary file loaded into it. The dictionary file is a text file that contains a list of known words up to and including the entire dictionary. The application uses this list to test different words in an attempt to recover the password. Systems that use passphrases typically are not vulnerable to this type of attack.

ii. **Brute-force Attacks**: In this type of attack, every possible combination of characters is attempted until the correct one is uncovered. According to RSA Labs, "Exhaustive key search, or brute-force search, is thebasic technique for trying every possible key in turn until the correct key is identified".

iii. **Hybrid Attack**: This form of password attack builds on the dictionary attack, but with additional steps as part of the process. In most cases, this means passwords that are tried during a dictionary attack are modified with the addition and substitution of special characters and numbers, such as P@ssw0rd instead of Password.

iv. **Syllable Attack:** This type of attack is a combination of a brute-force and a dictionary attack. It is useful when the password a user has chosen is not a standard word or phrase.

v. **Rule-based Attack:** This could be considered an advanced attack. It assumes that the user has created a password using information the attacker has some knowledge of ahead of time, such as phrases and digits the user may have a tendency to use. In addition to these techniques, there are four types of attacks. Each offers a different, effective way of obtaining a password from a target:

vi. **Passive Online Attacks:** Attacks in this category are carried out simply by sitting back and listening—in this case, via technology, in the form of sniffing tools such as Wire shark, man-in-the-middle attacks, or replay attacks.

vii. **Active Online Attacks:** The attacks in this category are more aggressive than passive attacks because the process requires deeper engagement with the targets. Attackers using this approach are targeting a victim with the intention of breaking a password. In cases of weak or poor passwords, active attacks are very effective. Forms of this attack include password guessing, Trojan/spyware/key loggers, hash injection, and phishing.

viii. **Offline Attacks:** This type of attack is designed to prey on the weaknesses not of passwords, but of the way they are stored. Because passwords must be stored in some format, an attacker seeks to obtain them where they are stored by exploiting poor security or weaknesses inherent in a system. If these credentials happen to be stored in a plaintext or unencrypted format, the attacker will go after this file and gain the credentials. Forms of this attack include pre-computed hashes, distributed network attacks, and rainbow attacks.

ix. **Nontechnical Attacks**: Also known as non-electronic attacks, these move the process offline into the real world. A characteristic of this attack is that it does not require any technical knowledge and instead relies on theft, deception, and other means. Forms of this attack include shoulder surfing, social engineering, and

dumpster diving.

3.8.5 Privilege Escalation

Escalating privileges basically means adding more rights or permissions to a user account. Simply said, escalating privileges makes a regular user account into an administrator account. Generally, administrator accounts have more stringent password requirements, and their passwords are more closely guarded. If it isn‘t possible to find a username and password of an account with administrator privileges, a hacker may choose to use an account with lower privileges. In this case, the hacker must then escalate that account‘s privileges. This is accomplished by first gaining access using a non-administrator user account—typically by gathering the username and password through one of the previously discussed methods—and then increasing the privileges on the account to the level of an administrator. When you obtain a password and gain access to an account, there is still more work to do: privilege escalation. The reality is that the account you’re compromising may end up being a lower-privileged and less defended one. If this is the case, you must perform privilege escalation prior to carrying out the next phase. The goal should be to gain a level where fewer restrictions exist on the account and you have greater access to the system.

Every operating system ships with a number of user accounts and groups already present. In Windows, preconfigured users include the administrator and guest accounts. Because it is easy for an attacker to find information about the accounts that are included with an operating system, you should take care to ensure that such accounts are secured properly, even if they will never be used. An attacker who knows that these accounts exist on a system is more than likely to try to obtain their passwords.

There are two defined types of privilege escalation, each of which approaches the problem of obtaining greater privileges from a different angle:

- **Horizontal Privilege Escalation**: An attacker attempts to take over the rights and privileges of another user who has the same privileges as the current account.
- **Vertical Privilege Escalation**: The attacker gains access to an account and

then tries to elevate the privileges of the account. It is also possible to carry out a vertical escalation by compromising an account and then trying to gain access to a higher-privileged account.

One way to escalate privileges is to identify an account that has the desired access and then change the password. Several tools that offer this ability, including the following:

- Active@ Password Changer
- Trinity Rescue Kit
- ERD Commander
- Windows Recovery Environment (WinRE)
- Password Resetter

Once you gain access to a system and obtain sufficient privileges, it's time to compromise the system and carry out the attack. Which applications are executed at this point is up to the attacker, but they can either be custom-built applications or off-the-shelf software. Once an attacker has gained access to a system and is executing applications on it, they are said to own the system. An attacker executes different applications on a system with specific goals in mind:

- **Backdoors:** Applications of this type are designed to compromise the system in such a way as to allow later access to take place. An attacker can use these backdoors later to attack the system. Backdoors can come in the form of rootkits, Trojans, and similar types. They can even include software in the form of remote access Trojans (RATs).
- **Crackers:** Any software that fits into this category is characterized by the ability to crack code or obtain passwords.
- **Keyloggers:** Keyloggers are hardware or software devices used to gain information entered via the keyboard.
- **Malware:** This is any type of software designed to capture information, alter, or compromise the system.

3.8.6 Pilfering

The objective is to gain access to trusted systems by information gathering. Once Administrator equivalent status has been obtained, attackers typically shift their

attention to grabbing as much information as possible that can be leveraged for further system conquests.

3.8.7 Creating backdoors

The objective is to hide the fact of total ownership from the system administrators by erasing all tracks from logs. There are many ways to plant a backdoor on a system, but let's look at one provided via the PsTools suite. This suite includes a mixed bag of utilities designed to ease system administration. Among these tools is PsExec, which is designed to run commands interactively or non-interactively on a remote system. Initially, the tool may seem similar to Telnet or remote desktop, but it does not require installation on the local or remote system in order to work.To work, PsExec need only be copied to a folder on the local system and run with the appropriate switches. Let's take a look at some of the commands you can use with:

- The following command launches an interactive command prompt on a system named \\dbserver: psexec \\dbserver cmd.
- This command executes ipconfig on the remote system with the /all switch, and displays the resulting output locally:psexec \\ dbserver ipconfig /all.
- This command copies the program rootkit.exe to the remote system and executes it interactively: psexec \\dbserver -c rootkit.exe.
- This command copies the program rootkit.exeto the remote system and executes it interactively using the administrator account on the remote system: psexec \\dbserver -u administrator -c rootkit.exe.

As these commands illustrate, it is possible for an attacker to run an application on a remote system quite easily. The next step is for the attacker to decide what to do or what to run on the remote system. Some of the common choices are Trojans, rootkits, and backdoors. Other utilities that may prove helpful in attaching to a system remotely are the following:

- **PDQ Deploy:** This utility is designed to assist with the deployment of software to a single system or to multiple systems across a network. The utility is designed to integrate with Active Directory as well as other software packages.
- **RemoteExec:** This utility is designed to work much like PsExec, but it also makes it easy to restart, reboot, and manipulate folders on the system.

- **DameWare:** This is a set of utilities used to remotely administer and control a system. Much like the other utilities on this list, it is readily available and may not be detected by antivirus utilities. DameWare also has the benefit of working across platforms such as Windows, OS X, and Linux

3.8.8 Covering Tracks

Once you have penetrated as system and installed software or run some scripts, then next step is cleaning up after yourself or covering your tracks. The purpose of this phase is to prevent your attack from being easily discovered by using various techniques to hide the red-flags and other signs. During this phase, you seek to eliminate error messages, log files, and other items that may have been altered during the attack process. The objective is to lay trap doors in various parts of the system so as to ensure easy privileged access. Last on the intruders checklist is the creation of future opportunities to return to the compromised system, hopefully disguised from the purview of system administrators.

3.8.8.1 Disabling Auditing

One of the best ways to prevent you from being discovered is to leave no tracks at all. And one of the best ways to do that is to prevent any tracks from being created or at least minimize the amount of evidence. When you're trying not to leave tracks, a good starting point is altering the way events are logged on the targeted system. Disabling auditing on a system prevents certain events from appearing and therefore slows detection efforts. Remember that auditing is designed to allow for the detection and tracking of selected events on a system. Once auditing is disabled, you have effectively deprived the defender of a great source of information and forced them to seek other methods of detection. In the Windows environment, you can disable auditing with the audit poll command included. Using the NULL session technique you saw during your enumeration activities, you can attach to a system remotely and run the command as follows:

auditpol \\<ip address of target> /clear

You can also perform what amounts to the surgical removal of entries in the Windows Security Log, using tools such as the following:

- Dumpel
- Elsave
- WinZapper
- CCleaner
- Wipe
- MRU-Blaster
- Tracks Eraser Pro
- Clear My History

3.8.8.2 Data Hiding

There are other ways to hide evidence of an attack, including hiding the files placed on the system such as EXE files, scripts, and other data. Operating systems such as Windows provide many methods you can use to hide files, including file attributes and alternate data streams. File attributes are a feature of operating systems that allow files to be marked as having certain properties, including read-only and hidden. Files can be flagged ashidden, which is a convenient way to hide data and prevent detection through simple means such as directory listings or browsing in Windows Explorer. Hiding files this way does not provide complete protection, however, because more advanced detective techniques can uncover files hidden in this manner.

3.8.8.3 Alternate Data Streams (ADS)

A very effective method of hiding data on a Windows system is also one of the lesser-known ones: Alternate Data Streams (ADS). This feature is part of the NTFS file system and has been since the 1990s, but since its introduction it has received little recognition; this makes it both useful for an attacker who is knowledgeable and dangerous for a defender who knows little about it. Originally, this feature was designed to ensure interoperability with the Macintosh Hierarchical File System (HFS), but it has since been used for other purposes. ADS provide the ability to fork or hide file data within existing files without altering the appearance or behavior of a file in any way. In fact, when you use ADS, you can hide a file from all traditional detection techniques as well as dir and Windows

Explorer. In practice, the use of ADS is a major security issue because it is nearly a perfect mechanism for hiding data. Once a piece of data is embedded and hidden using ADS, it can lie in wait until the attacker decides to run it later.

The process of creating ADS is simple:

triforce.exe > smoke.doc:triforce.exe

Executing this command hides the file triforce.exe behind the file smoke.doc. At this point, the file is streamed. The next step is to delete the original file that you just hid, triforce.exe. As an attacker, retrieving the file is as simple as this:

Start smoke.doc:triforce.exe

This command has the effect of opening the hidden file and executing it. As a defender, this sounds like bad news, because files hidden this way are impossible to detect using most means. But by using some advanced methods, they can be detected. Some of the tools that can be used to do this include the following:

- SFind—A forensic tool for finding streamed files
- LNS—Used for finding ADS streamed files
- Tripwire—Used to detect changes in files; by nature can detect ADS

An AD is available only on NTFS volumes, although the version of NTFS does not matter. This feature does not work on other file systems.

3.8.9 Denial of Service (DoS)

The objective is to use the readily available exploit code to disable a target. Essentially, a DoS attack disrupts or completely denies service to legitimate users, networks, systems or other resources. The intent of any such attack is usually malicious in nature and often takes little skill because of the requisite tools are readily available.

3.9 Let us Sum-up

When becoming an ethical hacker, you must develop a rich and diverse skill set and mind-set. Through a robust and effective combination of technological, administrative, and physical measures, organizations have learned to address their given situation and head off major problems through detection and testing. Technology such as virtual private networks (VPNs), cryptographic protocols,

intrusion detection systems (IDSs), intrusion prevention systems (IPSs), access control lists (ACLs), biometrics, smart cards, and other devices have helped security become much stronger, but still have not eliminated the need for vigilance. Administrative countermeasures such as policies, procedures, and other rules have also been strengthened and implemented over the past decade. Physical measures include devices such as cable locks, device locks, alarm systems, and other similar devices. Your new role as an ethical hacker will deal with all of these items, plus many more. As an ethical hacker you must not only know the environment you will be working in, but also how to find weaknesses and address them as needed. You will also need to understand the laws and ethics involved, and you also must know the client's expectations. Understand the value of getting the proper contracts in place and not deviating from them. Hacking that is not performed under contract is considered illegal and is treated as such. By its very nature, hacking activities can easily cross state and national borders into multiple legal jurisdictions. Breaking outside the scope of a contract can expose you to legal harm and become a career-ending blunder.

3.10 Further Readings

1. Study Material "Post-Graduate Diploma in Cyber Security Information System (PGDCS-06), Certificate in e-Governance and Cyber Security", Uttrakhand Open University, Haldwani, made available under a Creative Commons Attribution Share-Alike 4.0 Licence (International),
2. http://creativecommons.org/licenses/by-sa/4.0/
3. http://www.guru99.com/what-is-hacking-an-introduction.html
http://bedaone.blogspot.in/p/chapter-1-introduction-to-ethical.html

3.11 Assignments

1. Explain the various components of CIA Triad. Explain each of them.
2. What are the various types of hackers? Explain each of them briefly?
3. Enumerate and explain various phases involved in penetration testing. Briefly explain each of them.

Unit 4: Computer Forensics 4

Unit Structure

4.1 Learning Objectives

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

- Define Computer Forensic
- Know the history and evolution of Computer forensics
- Describe various types of cyber crimes
- Understand benefits of computer forensics
- Know about forensics readiness
- Implement forensics readiness plan

4.2 Introduction

Computer forensics is the art of recovering and analyzing the contents found on Computer devices such as desktops, notebooks, tablets, smart phones, etc. It was little-known a few years ago. However, with the growing incidence of cyber-crime adoption of computer devices, this branch of forensics has gained momentum in the recent years, augmenting what was conventionally limited to the recovery and analysis of biological and chemical evidence during criminal investigations. This has been used an important technology used many investigating agencies for detection of cyber-criminal activities and evidences. In this unit we will discuss the evolution and of computer forensics technology, its benefits and applications.

4.3 Definition of Computer Forensics

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it. It is the use of specialized techniques for recovery, authentication and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, and

authentication of data by technical analysis or explanation of technical features of data and computer usage. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel. Similar to all forms of forensic science, computer forensics is comprised of the application of the law to computer science. Computer forensics deals with the preservation, identification, extraction,and documentation of computer evidence. Like many other forensic sciences, computer forensics involves the use of sophisticated technological tools and procedures that must be followed to guarantee theaccuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing. So Computer Forensic is the use of specialized techniques for recovery, authentication, and analysis of computer data, typically of data which may have been deleted or destroyed.

4.4 Cyber Crime

Computer crime or cybercrime is any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Dr.Debarati Halder and Dr. K. Jaishankar define Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare.

Computer forensics is traditionally associated with criminal investigations and, as you would expect, most types of investigation center on some form of computer crime. This sort of crime can take two forms. (a) Computer based crime and (b) Computer facilitated crimes.

4.4.1 Computer Based Crime

This is criminal activity that is conducted purely on computers, for example cyber-bullying or spam. As well as crimes newly defined by the computing age it also includes traditional crime conducted purely on computers (for example, child pornography).

4.4.2 Computer Facilitated Crime

Crimes conducted in the "real world" but facilitated by the use of computers. A classic example of this sort of crime is fraud: computers are commonly used to communicate with other fraudsters, to record/plan activities or to create fraudulent documents.

Not all Computer forensics investigations focus on criminal behavior; sometimes the techniques are used in corporate (or private) settings to recover lost information or to rebuild the activities of employees.

4.5 Evolution of Computer Forensics

It is difficult to pinpoint the first “computer forensic” examination or the beginning of the field for that matter. But most experts agree that the field of computer forensics began to evolve more than 30 years ago. The field began in the United States, in large part, when law enforcement and military investigators started seeing criminals get technical. Government personnel charged with protecting important, confidential, and certainly secret information conducted forensic examinations in response to potential security breaches to not only investigate the particular breach, but to learn how to prevent future potential breaches. Ultimately, the fields of information security, which focuses on protecting information and assets, and computer forensics, which focuses on the response to hi-tech offenses, started to intertwine.

Over the next decades, and up to today, the field is evolving. Both Government and private organizations and corporations have followed suit – employing internal information security and computer forensic professionals or contracting such

professionals or firms on an as- needed basis. Significantly, the private legal industry has more recently seen the need for computer forensic examinations in civil legal disputes, causing an explosion in the e- discovery field.

4.6 Stages of Computer Forensics Process

The overall computer forensics process is sometimes viewed as comprising four stages:

1. **Acquire**: Identifying and Preserving
2. **Analyze**: Technical Analysis
3. **Evaluate:** What the Lawyers Do
4. **Present:** Present Computer evidence in a manner that is legally acceptable in any legal proceedings.

4.7 Benefits of Computer Forensics

With the ever increasing rate of cyber-crimes, from phishing to hacking and stealing of personal information not only confined to a particular country but the globally at large, there is a need for forensic experts to be available in public and private organizations. To be able to handle this, it's vital for network administrator and security staff of networked organizations to have this course in practice making sure that they have the laws pertaining to this on their fingertips. This would ensure that should need for the service avail itself, then they would come in and rescue the situation.

The survival and integrity of any given network infrastructure of any company or organization strongly depends on the application of computer forensics. They should be taken as the main element of computer and network security. It would be a great benefit for a company if it has knowledge of all the technical and legal aspects of this field. Should the company's network be under attack and the intruder caught in the act, then an understanding about computer forensics will be of help in provision of evidence and prosecution of the case in the court of law.

New laws aimed at the protection of customer's data are continuously being developed. Should they lose data, then naturally the liability goes to the company. Such cases, if they occur will automatically result in the company or organization

being brought to the court of law for failure to protect personal data, this can turn out to be very expensive. But through the application of forensic science, huge chunks of money can be saved by the firms concerned. A lot of money is lately being spent on network and computer security. Software for vulnerability assessment and intrusion detection has passed the billion dollar mark, this is according to experts. It simply means that there is a necessity in investment in either employing an expert in computer forensic in the firms, or having part of their staff trained into this venture so as to help in detection of such cases should they arise.

4.8 Uses of Computer Forensics

There are few areas of crime or dispute where computer forensics cannot be applied. Law enforcement agencies have been among the earliest and heaviest users of computer forensics and consequently have often been at the forefront of developments in the field.

Computers may constitute a 'scene of a crime', for example with hacking or denial of service attacks or they may hold evidence in the form of emails, internet history, documents or other files relevant to crimes such as murder, kidnap, fraud and drug trafficking.

It is not just the content of emails, documents and other files which may be of interest to investigators but also the 'metadata' associated with those files. A computer forensic examination may reveal when a document first appeared on a computer, when it was last edited, when it was last saved or printed and which user carried out these actions.

More recently, commercial organizations have used computer forensics to their benefit in a variety of cases such as:

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Forgeries
- Bankruptcy investigations
- Inappropriate email and internet use in the work place

- Regulatory compliance

4.9 Objectives of Computer Forensics

We all will agree to the fact that we are depending more on more on Information & Communication Technology (ICT) tools and internet for digital services to an extent that today we talk online using chat application, we depend on email to communicate with relatives and office, we stay in touch with our friends and update status using social engineering platforms like Facebook, etc., we work online by staying connected to our office/ client using internet, we shop online, we teach online, we learn online, we submit our bill online today. Our dependency on Computer and Internet have increased so much that we are “online” most of the time. Therefore, there is an increased need of protecting our information from being misused by following Information security guidelines. However, if the security of our computer is compromised, computer forensics comes handy for post- incident investigation.

The objectives of Computer forensics are to provide guidelines for:

- Following the first responder procedure and access the victim’s computer after incident.
- Designing procedures at a suspected crime scene to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication.
- Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Provide guidelines for analyzing digital media to preserve evidence, analyzing logs and deriving conclusions, investigate network traffics and logs to correlate events, investigate wireless and web attacks, tracking emails and investigate email crimes.
- Producing computer forensic report which provides complete report on computer forensic investigation process.
- Preserving the evidence by following the chain of custody.
- Employing the rigorous procedures necessary to have forensic results stand up to scrutiny in a court of law.
- Presenting Computer forensics results in a court of law as an expert witness.

4.10 Role of Forensics Investigator

Following are some of the important duties of a forensic investigator:

- Confirms or dispels whether a resource/network is compromised.
- Determine extent of damage due to intrusion.
- Answer the questions: Who, What, When, Where, How and Why.
- Gathering data in a forensically sound manner.
- Handle and analyze evidence.
- Prepare the report.
- Present admissible evidence in court.

4.11 Forensics Readiness

There are several reasons for this field's growth; the most significant being that computers are everywhere. You'd be hard pressed to find a household today without at least one computer. And it is not just computers that computer forensic examiners get involved with. Computer forensic examiners analyze all types of technical devices. Look around you while you walk down the street – people are on their cell phones, using iPods, PDAs, and text messaging. Computer forensic examiners analyze all of these electronic devices! Cyber forensics is a rapidly changing field. There are new technologies coming out daily that are becoming smaller, but storing more and more data. This leads to why cyber forensics is import. In computer related crimes, such identity fraud, it is becoming easier to hide data. With the proper analysis of digital evidence, better security can be made to protect computer users, but also catch those who are committing the crimes. Organizations have now realized the importance of being prepared to combat cyber criminals with their forensic readiness plan ready.

4.11.1 Forensics Readiness

Forensic readiness is the ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation. In a business context there is the opportunity to actively collect potential evidence in the form of log files, emails, back-up disks, portable computers, network traffic records, and telephone records, amongst others. This evidence may be collected in advance of

a crime or dispute, and may be used to the benefit of the collecting organization if it becomes involved in a formal dispute or legal process.

4.11.2 Goals of Forensic Readiness

Some of the important goals of forensics readiness are:

- To gather admissible evidence legally and without interfering with business processes;
- To gather evidence targeting the potential crimes and disputes that may adversely impact an organization;
- To allow an investigation to proceed at a cost in proportion to the incident;
- To minimize interruption to the business from any investigation; and
- To ensure that evidence makes a positive impact on the outcome of any legal action.

4.11.3 Benefits of Forensic Readiness

Forensic readiness can offer an organization the following benefits:

- Evidence can be gathered to act in an organization's defense if subject to a lawsuit;
- Comprehensive evidence gathering can be used as a deterrent to the insider threat (throwing away potential evidence is simply helping to cover the tracks of a cyber- criminal);
- In the event of a major incident, an efficient and rapid investigation can be conducted and actions taken with minimal disruption to the business;
- A systematic approach to evidence storage can significantly reduce the costs and time of an internal investigation;
- A structured approach to evidence storage can reduce the costs of any court-ordered disclosure or regulatory or legal need to disclose data (e.g. in response to a request under data protection legislation);
- Forensic readiness can extend the scope of information security to the wider threat from cyber-crime, such as intellectual property protection, fraud, extortion etc.;
- It demonstrates due diligence and good corporate governance of the company's information assets;
- It can demonstrate that regulatory requirements have been met;
- It can improve and facilitate the interface to law enforcement if involved;

- It can improve the prospects for a successful legal action;
- It can provide evidence to resolve a commercial dispute;
- It can support employee sanctions based on digital evidence

4.11.4 Steps for Forensic Readiness Planning

The following ten steps describe the key activities in forensic readiness planning:

1. Define the business scenarios that require digital evidence;
2. Identify available sources and different types of potential evidence;
3. Determine the evidence collection requirement;
4. Establish a capability for securely gathering legally admissible evidence to meet the requirement;
5. Establish a policy for secure storage and handling of potential evidence;
6. Ensure monitoring is targeted to detect and deter major incidents;
7. Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched;
8. Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence;
9. Document an evidence-based case describing the incident and its impact.
10. Ensure legal review to facilitate action in response to the incident.

Let us now discuss in brief each of the ten steps.

1. **Define the business scenarios that require digital evidence:** The first step in forensic readiness is to define the purpose of an evidence collection capability. The rationale is to look at the risk and potential impact on the business from the various types of crimes and disputes. What is the threat to the business and what parts are vulnerable? This is, in effect, a risk assessment, and is performed at the business level.

The aim is to understand the business scenarios where digital evidence may be required and may benefit the organization the event that it is required. In general the areas where digital evidence can be applied include:

- Reducing the impact from computer-related crime;
- Dealing effectively with court orders to release data;
- Demonstrating compliance with regulatory or legal constraints;
- Producing evidence to support company disciplinary issues;

- Supporting contractual and commercial agreements; and
- Proving the impact of a crime or dispute.

In assessing these scenarios, this step provides an indication of the likely benefits of being able to use digital evidence. If the identified risks, and the potential benefits of forensic readiness, suggest a good return on investment is achievable, then an organization needs to consider what evidence to gather for the various risk scenarios.

2. **Identify available sources and different types of potential evidence:** The second step in forensic readiness is for an organization to know what sources of potential evidence are present on, or could be generated by, their systems and to determine what currently happens to the potential evidence data. Computer logs can originate from many sources. The purpose of this step is to scope what evidence may be available from across the range of systems and applications in use. Some basic questions need to be asked about possible evidence sources to include.

- Where is data generated?
- What format is it in?
- How long is it stored for?
- How is it currently controlled, secured and managed?
- Who has access to the data?
- How much is produced?
- Is it archived? If so where and for how long?
- How much is reviewed?
- What additional evidence sources could be enabled?
- Who is responsible for this data?
- Who is the formal owner of the data?
- How could it be made available to an investigation?
- What business processes does it relate to?
- Does it contain personal information?

Email is an obvious example of a potential rich source of evidence that needs careful consideration in terms of storage, archiving & auditing and retrieval. But this is not the only means of communication used over the internet, there is also

instant messaging, web-based email that bypasses corporate email servers, chat-rooms and newsgroups, even voice over the internet. Each of these may need preserving and archiving. The range of possible evidence sources includes:

- Equipment such as routers, firewalls, servers, clients, portables, embedded devices etc.
- Application software such as accounting packages etc for evidence of fraud, ERP packages for employee records and activities (e.g. in case of identity theft), system and management files etc;
- Monitoring software such as intrusion detection software, packet sniffers, keyboard loggers, content checkers, etc;
- General logs such as access logs, printer logs, web traffic, internal network logs, internet traffic, database transactions, commercial transactions etc;
- Other sources such as: CCTV, door access records, phone logs, pabx data etc;
- Back-ups and archives.

3. **Determine the Evidence Collection Requirement:** It is now possible to decide which of the possible evidence sources identified in step 2 can help deal with the crimes and disputes identified in step 1 and whether further ways to gather evidence are required. This is the evidence collection requirement. The purpose of this step is to produce an evidence requirement statement so that those responsible for managing the business risk can communicate with those running and monitoring information systems through an agreed requirement for evidence. One of the key benefits of this step is the bringing together of IT with the needs of corporate security. IT audit logs have been traditionally configured by systems administrators independently of corporate policy and where such a policy exists there is often a significant gap between organizational security objectives and the 'bottom-up' auditing actually implemented. The evidence collection requirement is moderated by a cost benefit analysis of how much the required evidence will cost to collect and what benefit it provides (see above). The critical question for successful forensic readiness is what can be performed cost effectively. By considering these issues in advance and choosing storage options, auditing tools, investigation tools, and appropriate procedures it is possible for an organization to reduce the costs of future forensic investigations.

4. **Establish a capability for securely gathering legally admissible evidence**

to meet the requirement: At this point the organization knows the totality of evidence available and has decided which of it can be collected to address the company risks and within a planned budget. With the evidence requirement understood, the next step is to ensure that it is collected from the relevant sources and that it is preserved as an authentic record. At this stage legal advice is required to ensure that the evidence can be gathered legally and the evidence requirement can be met in the manner planned. For example, does it involve monitoring personal emails, the use of personal data, or 'fishing trips1' on employee activities? In some countries, some or all of these activities may be illegal. Relevant laws, in the areas of data protection, privacy and human rights, will inevitably constrain what can actually be gathered. Some of the guidelines are:

- Monitoring should be targeted at specific problems.
- It should only be gathered for defined purposes and nothing more;
- Staff should be told what monitoring is happening except in exceptional circumstances.

Physical security of data such as back-up files or on central log servers is important from the data protection point of view, and also for secure evidence storage. As well as preventative measures such as secure rooms and swipe card access it is also prudent to have records of who has access to the general location and who has access to the actual machines containing evidence. Any evidence or paperwork associated with a specific investigation should be given added security by, for example, storing in a safe. Additional security of logs can also be achieved through the use of WORM storage media.

5. Establish a policy for secure storage and handling of potential evidence: The objective of this step is to secure the evidence for the longer term once it has been collected and to facilitate its retrieval if required. It concerns the long-term or off-line storage of information that might be required for evidence at a later date. A policy for secure storage and handling of potential evidence comprises security measures to ensure the authenticity of the data and also procedures to demonstrate that the evidence integrity is preserved whenever it is used, moved or combined with new evidence. In the parlance of investigators this is known as continuity of evidence (in the UK) and chain of custody (in the US). The continuity of evidence also includes records of who held, and who had access to, the

evidence (for example from swipe control door logs). A significant contribution to the legal collection of evidence is given by the code of practice on the legal admissibility and weight of information stored electronically, published by the British Standards Institution. This document originated from a perceived need for evidence collection in the paperless office. The problem it addressed is if all paper documents are scanned, can the paper sources be thrown away without loss of evidential usability? The current edition broadens the scope to all information management systems, Ad hoc opportunistic searches, without justification, for potentially incriminating activities or communication such as those where information is transmitted over networks such as email systems for example. It points out that methods of storage, hardware reliability, operation and access control, and even the programs and source code, may be investigated in order to determine admissibility. A closely related international standard is being developed as ISO 15801. The required output of this step is a secure evidence policy. It should document the security measures, the legal advice and the procedural measures used to ensure the evidence requirement is met. Upon this document rests the likely admissibility and weight of any evidence gathered.

6. **Ensure monitoring and auditing is targeted to detect and deter major incidents:** In addition to gathering evidence for later use in court, evidence sources can be monitored to detect threatened incidents in a timely manner. This is directly analogous to Intrusion Detection Systems (IDS), extended beyond network attack to a wide range of behaviors that may have implications for the organization. It is all very well collecting the evidence.

This step is about making sure it can be used in the process of detection. By monitoring sources of evidence we can look for the triggers that mean something suspicious may be happening. The critical question in this step is when should an organization be suspicious? A suspicious event has to be related to business risk and not couched in technical terms. Thus the onus is on managers to explain to those monitoring the data what they want to prevent and thus the sort of behavior that IDS might be used to detect for example. This should be captured in a ‘suspicion’ policy that helps the various monitoring and auditing staff understand what triggers should provoke suspicion, who to report the suspicion to, whether heightened monitoring is required, and whether any additional security measures

should be taken as a precaution. Each type of monitoring should produce a proportion of false positives. The sensitivity of triggers can be varied as long as the overall false positive rate does not become so high that suspicious events cannot be properly reviewed. Varying triggers also guards against the risk from someone who knows what the threshold on a particular event is and makes sure any events or transactions he wishes to hide are beneath it.

7. **Specify circumstances when escalation to a full formal investigation (which may use digital evidence) is required:** Some suspicious events can be system generated, such as by the rule-base of an IDS, or the keywords of a content checker, and some will be triggered by human watchfulness. Each suspicious event found in step 6 needs to be reviewed. Either an event will require escalation if it is clearly serious enough, or it will require enhanced monitoring or other precautionary measures, or it is a false positive. The purpose of this step is to decide how to react to the suspicious event. The decision as to whether to escalate the situation to management will depend on any indications that a major business impact is likely or that a full investigation may be required where digital evidence may be needed. The decision criteria should be captured in an escalation policy that makes it clear when a suspicious event becomes a confirmed incident. At this point an investigation should be launched and policy should indicate who the points of contact are (potentially available on a 24x7 basis) and who else needs to be involved. As with steps 3 and 6, the network and IT security managers and the non-IT managers need to understand each other's position. What level of certainty or level of risk is appropriate for an escalation? What strength of case is required to proceed? A preliminary business impact assessment should be made based on whether any of the following are present:

- Evidence of a reportable crime
- Evidence of internal fraud, theft, other loss
- Estimate of possible damages (a threshold may induce an escalation trigger)
- Potential for embarrassment, reputation loss
- Any immediate impact on customers, partners or profitability
- Recovery plans have been enacted or are required; and
- The incident is reportable under a compliance regime.

8. **Train staff, so that all those involved understand their role in the digital**

evidence process and the legal sensitivities of evidence: A wide range of staff may become involved in a computer security incident. The aim of this step is to ensure that appropriate training is developed to prepare staff for the various roles they may play before, during and after an incident. It is also necessary to ensure that staff is competent to perform any roles related to the handling and preservation of evidence. There will be some issues relevant to all staff if they become involved in an incident. The following groups will require more specialized awareness training for example:

- The investigating team;
- Corporate HR department;
- Corporate PR department (to manage any public information about the incident);
- 'owners' of business processes or data;
- Line management, profit center managers;
- Corporate security;
- System administrators;
- IT management;
- Legal advisers; and
- Senior management (potentially up to board level).

At all times those involved should act according to 'need to know' principles. They should be particularly aware whether any staff, such as 'whistle blowers' and investigators, need to be protected from possible retaliation by keeping their names and their involvement confidential. Training may also be required to understand the relationships and necessary communications with external organizations that may become involved.

9. Present an evidence-based case describing the incident and its impact: The aim of an investigation is not just to find a culprit or repair any damage. An investigation has to provide answers to questions and demonstrate why those answers are credible. The questions go along the lines of who, what, why, when, where and how. Credibility is provided by evidence and a logical argument. The purpose of this step is to produce a policy that describes how an evidence-based case should be assembled. A case file may be required for a number of reasons:

- To provide a basis for interaction with legal advisers and law enforcement;
- To support a report to a regulatory body;
- To support an insurance claim;
- To justify disciplinary action;
- To provide feedback on how such an incident can be avoided in future;
- To provide a record in case of a similar event in the future (supports the corporate memory so that even if there are changes in personnel it will still be possible to understand what has happened);
- To provide further evidence if required in the future, for example if no action is deemed necessary at this point but further developments occur.

10. Ensure legal review to facilitate action in response to the incident: At certain points during the collating of the cyber-crime case file it will be necessary to review the case from a legal standpoint and get legal advice on any follow-up actions. Legal advisers should be able to advice on the strength of the case and suggest whether additional measures should be taken; for example, if the evidence is weak is it necessary to catch an internal suspect red handed by monitoring their activity and seizing their PC? Any progression to a formal action will need to be justified, cost- effective and assessed as likely to end in the company's favour. Although the actual decision of how to proceed will clearly be post-incident, considerable legal preparation is required in readiness. Legal advisors should be trained and experienced in the appropriate cyber laws and evidence admissibility issues. They need to be prepared to act on an incident, pursuant to the digital evidence that has been gathered and the case presented in step 9. Legal advice should also recognize that the legal issues may span legal jurisdictions e.g. states in the US, member states in the EU. Advice from legal advisers will include:

- Any liabilities from the incident and how they can be managed;
- Finding and prosecuting/punishing (internal versus external culprits);
- Legal and regulatory constraints on what action can be taken;
- Reputation protection and PR issues;
- When/if to advice partners, customers and investors;
- How to deal with employees;
- Resolving commercial disputes; and

- Any additional measures required.

4.12 Issues Facing Computer Forensics

The issues facing computer forensics examiners can be broken down into three broad categories: technical, legal and administrative

4.12.1 Technical Issues

a. **Encryption –** Encrypted data can be impossible to view without the correct key or password. Examiners should consider that the key or password may be stored elsewhere on the computer or on another computer which the suspect has had access to. It could also reside in the volatile memory of a computer (known as RAM) which is usually lost on computer shut-down; another reason to consider using live acquisition techniques, as outlined above.

b. **Increasing storage space –** Storage media hold ever greater amounts of data, which for the examiner means that their analysis computers need to have sufficient processing power and available storage capacity to efficiently deal with searching and analyzing large amounts of data.

c. **New technologies –** Computing is a continually evolving field, with new hardware, software and operating systems emerging constantly. No single computer forensic examiner can be an expert on all areas, though they may frequently be expected to analyze something which they haven't previously encountered. In order to deal with this situation, the examiner should be prepared and able to test and experiment with the behavior of new technologies. Networking and sharing knowledge with other computer forensic examiners is very useful in this respect as it's likely someone else has already come across the same issue.

d. **Anti-forensics –** Anti-forensics is the practice of attempting to thwart computer forensic analysis. This may include encryption, the over- writing of data to make it unrecoverable, the modification of files' metadata and file obfuscation (disguising files). As with encryption, the evidence that such methods have been used may be stored elsewhere on the computer or on another computer which the suspect has had access to. In our experience, it is very rare to see anti-forensics tools used correctly and frequently enough to totally obscure either their presence or the presence of the evidence that they were used to hide.

4.12.2 Legal Issues

Legal issues may confuse or distract from a computer examiner's findings. An example here would be the 'Trojan Defense'. A Trojan is a piece of computer code disguised as something benign but which carries a hidden and malicious purpose. A lawyer may be able to argue that actions on a computer were not carried out by a user but were automated by a Trojan without the user's knowledge; such a Trojan Defense has been successfully used even when no trace of a Trojan or other malicious code was found on the suspect's computer. In such cases, a competent opposing lawyer, supplied with evidence from a competent computer forensic analyst, should be able to dismiss such an argument. A good examiner will have identified and addressed possible arguments from the "opposition" while carrying out the analysis and in writing their report.

4.12.3 Administrative Issues

a. **Accepted standards –** There are a plethora of standards and guidelines in computer forensics, few of which appear to be universally accepted. The reasons for this include: standard-setting bodies being tied to particular legislations; standards being aimed either at law enforcement or commercial forensics but not at both; the authors of such standards not being accepted by their peers; or high joining fees for professional bodies dissuading practitioners from participating.

b. **Fit to practice –** In many jurisdictions there is no qualifying body to check the competence and integrity of computer forensics professionals. In such cases anyone may present themselves as a computer forensic expert, which may result in computer forensic examinations of questionable quality and a negative view of the profession as a whole.

4.13 Let us Sum-up

Computer forensics is the practice of collecting, analyzing and reporting on Computer data in a way that is legally admissible. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel. Computer crime, or cybercrime, is any crime that involves a computer and a network. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare.

The survival and integrity of any given network infrastructure of any company or organization strongly depends on the application of computer forensics. Forensic readiness is the ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation.

Monitoring should be targeted at specific problems. Physical security of data such as back-up files or on central log servers is important from the data protection point of view, and also for secure evidence storage.

A policy for secure storage and handling of potential evidence comprises security measures to ensure the authenticity of the data and also proceduresto demonstrate that the evidence integrity is preserved whenever it is used, moved or combined with new evidence.

The aim of an forensic investigation is not just to find a culprit or repair any damage. An investigation has to provide answers to questions and demonstrate why those answers are credible. At certain points during the collating of the cyber-crime case file it will be necessary to review the case from a legal standpoint and get legal advice on any follow-up actions.

4.14 Further Readings

1. Digital Forensics, (PGDCS-07), Study Materials of Uttarakhand Open University, Haldwani, for Post-Graduate Diploma in Cyber Security,
2. Robert Rowlingson Ph.D , qinetiq Ltd., A Ten Step Process for Forensic Readiness, International Journal of Digital Evidence, Winter 2004, Volume 2, Issue 3.
3. ICT and Education, Fundamental of ICT in education, By Dr. T. Manichander.
4. http://einvestigations.com/computer-forensics/expert-witness/
5. http://searchsecurity.techtarget.com/definition/computer-forensics
6. https://www.linkedin.com/pulse/computer-forensic-egharevba-etinosa- aca-acfe-amscce-clrmp-ifrs-cert.
7. https://forensiccontrol.com/resources/beginners-guide-computer- forensics.

4.15 Assignments

1. Name the four stages of computer forensic process.
2. Outline the uses of computer forensics.
3. Mention the objectives of computer forensics?
4. Write the role of a forensics investigator?
5. What are the benefits of forensic readiness?
6. Explain various steps involved in forensic readiness planning.