

INFORMATION SECURITY - I



Edition 1
Year of Publication: 2016


© Confidentiality & Proprietary Information


This is a confidential document prepared by iNurture. This document, or any portion thereof, should not be made available to any persons other than the authorised and designated staff of the company/institution/vendor to which it has been submitted.


No part of this document may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of iNurture.


How to use the Self Learning Material


The pedagogy used to design this course is to enable you to assimilate the concepts and processes with ease. The course is divided into **Modules**. Each module is categorically divided into **Chapters**. Each chapter consists of the following elements:


 **Table of Contents:** Every chapter consists of a well-defined table of content. *For example: “1.1.8.(i)” should be read as “Module 1. Chapter 1. Topic 8. (Sub-topic i)” and 1.2.8. (ii) should be read as “Module 1.Chapter 2. Topic 8. (Sub-topic ii)”*


 **Aim:** ‘Aim’ refers to the overall goal to be achieved by going through the chapter.


 **Instructional Objectives:** ‘Instructional Objectives’ defines what the chapter intends to deliver.


 **Learning Outcomes:** ‘Learning Outcomes’ refers to what you will be able to accomplish by going through the chapter.


 **Advantages:** ‘Advantages’ describes the positive aspects of that particular method, theory or practice.


 **Disadvantages:** ‘Disadvantages’ describes the drawbacks of the particular method, theory or practice.


 **Summary:** ‘Summary’ contains the main points of the entire chapter.


 **Self-assessment:** ‘Self-assessment’ contains a set of questions to answer at the end of each topic.

 **e-References:** ‘e-References’ is a list of online resources that have been used while designing the chapter.

 **External Resources:** ‘External Resources’ is a list of scholarly books for additional source of knowledge.

 **Video Links:** ‘Video Links’ contain links to online videos that will help you to understand the concepts better.

 **Did you know?:** ‘Did you know’ is an interesting fact that helps improve your knowledge about the topic.

 **Activity:** ‘Activity’ is used to demonstrate the application of a concept. Activities can be online and offline.

Information Security - I

Course Description

The critical objective of this course is to enlighten every individual to know the importance of information and its security for an organisation. This course provides sufficient knowledge to understand the detailed structure of the information flow within/outside the organisation and provides the information to identify the points of vulnerabilities. It also briefs few security techniques such as firewalls, cryptography to avoid or control the information theft. This course briefs lot of security standards, policies and components of network security.

At the end of the course students will be able to understand how information security works in an organisation. Students will also be able to analyse various security threats in an organisation and can build recovery techniques accordingly.

This course is designed to serve as a stepping stone to build a career as a CISO (Chief Information Security Officer), Security Architect, Security Engineer, Security Manager, few fields in which one can explore many opportunities.

The **Information Security** Course contains **Five Modules**.

MODULE 1: INTRODUCTION TO INFORMATION SECURITY

Basics of Information Security, The Evolution of Information Security, Key information security concepts, Components of information system, Introduction to CNSS Security Model, Critical characteristics of information, Balancing information security and access, Approaches to information security implementation, Security Professionals and The Organisation

MODULE 2: USER IDENTITY AND ACCESS MANAGEMENT

Identity and access management concepts, Access management services, Account Authorisation and validation Management, Security auditing, Access control, Privilege Identity Management (PIM), Basic concepts of cryptography and network security, Encryption and Decryption, Applications of cryptographic hash functions, Requirements and security, Hash function based on cipher block chaining, Secure Hash Algorithm(SHA)

MODULE 3: SYSTEM AND SERVER SECURITY

System Security, Desktop and Server Security, Firewalls, Techniques of password cracking, Key Loggers, Viruses, Worms, Malwares, Spywares, Windows Registry

MODULE 4: INTERNET SECURITY & PREVENTION

Internet Security, Hacking Attacks, Approaches to Hacking, Planning for Hacking Incidents, Hacking Prevention Methods, Damage Limitation

MODULE 5: RISK ASSESSMENT AND CYBER LAWS

Risk Assessment, Vulnerability Assessment, Penetration Testing, Cyber Laws in India, Cyber Laws a global perspective, FAIR model

Table of Contents

MODULE 1

Introduction to Information Security

Chapter 1.1 Basics of Information Security	1
Chapter 1.2 Balancing Information Security and Access	21

MODULE 2

User Identity and Access Management

Chapter 2.1 Access Management	47
Chapter 2.2 Hashing and Cryptography	73

MODULE 3

System and Server Security

Chapter 3.1 System Security and Firewalls	115
Chapter 3.2 Viruses, Worms, Malwares and Spywares	149

MODULE 4

Internet Security and Prevention

Chapter 4.1 Internet Security	183
Chapter 4.2 Preventive Measures for Hacking Attacks	211

MODULE 5

Risk Assessment and Cyber Laws

Chapter 5.1 Risk Assessment	235
Chapter 5.2 Cyber Laws	271

Information Security - I

MODULE - I

Introduction to Information Security

Introduction to Information Security

Module Description

The main objective of this module is to show the importance of security over the organisation information. This module provides a brief about basic terminology, which will be acting as a base for the subsequent chapters along with the history and principles of the information security. This module describes the information system along with its components, also covers security measures based on the CNSS model along with key stakeholders of information system. This module also elaborates different approaches for implementing the information security.

By the end of this module, students will be able to understand different application, technical terms, key stakeholders and implementation methods involved in the information security. At the end of this chapter, student can analyse flow of information between different components of information system.

Chapter 1.1

Basics of Information Security

Chapter 1.2

Balancing Information Security and Access

Chapter Table of Contents

Chapter 1.1

Basics of Information Security

Aim.....	1
Instructional Objectives.....	1
Learning Outcomes.....	1
1.1.1 Introduction.....	2
1.1.2 The evolution of Information Security.....	2
(i) History	2
(ii) Security and its definition	3
(iii) Basic Principles.....	5
(iv) Information Security Applications	6
Self-assessment Questions.....	7
1.1.3 Key Information Security Concepts	7
Self-assessment Questions.....	10
1.1.4 Components of Information System	11
(i) Software	11
(ii) Hardware.....	12
(iii) Data.....	12
(iv) People.....	12
(v) Procedures.....	13
(vi) Networks	13
Summary	15
Terminal Questions.....	16
Answer Keys.....	17
Activity.....	17
Case Study	18
Bibliography.....	19
e-References	19
External Resources	19
Video Links	19



Aim

To provide the students with the knowledge of fundamentals of Information Security



Instructional Objectives

After completing this chapter, you should be able to:

- Explain the basic concepts and principles of Information Security along with its applications
- Elaborate the advantages of Information Security
- Define key terms and critical concept of Information Security
- Explain the characteristics of information system components to apply security concepts on the system



Learning Outcomes

At the end of this chapter, you are expected to:

- Outline the basic principles of Information Security with its applications so that the importance of Information Security is clearly known
- List some significant advantages of using Information Security.
- State the essential concept of Information Security.
- Recognise the strengths and weakness of information system components

1.1.1 Introduction

According to James Anderson, information security in an enterprise is a “well-informed sense of assurance that the information risks and controls are in the balance.”

Information is a critical and important asset of any organisation. Until the evolution of internet, protecting data was just a human task and very limited methods were available to protect data from unauthorised access. After a massive development of computing environment and their connectivity, protecting data from the intruders has become more critical. Emerging business trends like E-Commerce and M-Commerce has made information security as an important part of business continuation plan of most of the organisations.

Emerging demand for information security has created more business opportunities, i.e. many organisations have evolved in the market for protecting the data, many standards and protocols were created for data protection, many access methods were invented to authenticate and access the critical system, many third party gateways are designed to manage data protection and data loss. Still, the field has a lot of open challenges.

The present chapter focuses on various key terms used in the concept of information security, its applications, critical components of information security and advantages and disadvantages of it.

1.1.2 The evolution of Information Security

(i) History

History of any science begins with a need. Even the information security has taken its beginning with protecting the physical and software components of the first mainframe developed during World War II. This mainframe was filled with highly secure data. Access to it was done through multiple keys, facial verification, ID card verifications through security guards. This physical protection was enough, until mainframe was brought online during the 1960s.

During the 1960s the mainframes are interconnected through different centres by using research product “ARPANET” by Defence’s Advanced Research Project Agency (ARPA) (it is a base for internet evaluation). A very simple process of communication was set up between mainframe and communication centre. This interconnection has created a lot of protection issues, to deal with it in June of 1967; the Advanced Research Projects Agency employed a

task force to study the process of information systems. With the effort and recommendations of Task Force, a report was created and named as Rand Report R-609.9

Many operating systems were designed by including security in the operating system core; first among such operating systems are MULTICS. It is a time-sharing operating system developed in the mid-1960s by a consortium of General Electric (GE), Bell Labs and the Massachusetts Institute of Technology (MIT). Then UNIX joins the list with more password protecting features.

During late 1970s personal computer has made its entry. Personal computers are interconnected to data centres. Which made data and resources available in different locations, in simple terms can be called as decentralisation of data and resources. This evaluation has created networking in the 1980s.

In the 1990s, computers have become part of human life and are connected to each other through the internet (a global network). The Internet was now available even for the public, which has previously been with the government, academia and few industry professionals.

As the most critical defence department information was also a part of the internet, some de facto standards were in the need to protect them from external world through the internet. These de facto standards could provide limited security to the crucial data. Many protection problems, which are rising today, are because of the low priority given to security these days. One among such important cases is the email. This lack of complete data protection has given enough scope to security threats.

At present, millions of trillions of unsecured computers are part of the internet. Protecting personal data is contingent on information security. Now, many governments have understood that the information security is as important as the defence of a country. Cyber-attacks are making all organisations to safeguard their resources from the external world by employing proper security measures.

(ii) Security and its definition

The term security defines “something that secures or makes safe”. In other words, denying the access to someone who does not have required credentials to access the organisation information.

Security method needs to be deployed to protect the critical resources from adversaries, which would cause harm, intentionally or accidentally. The National security of any country

would be one **example** of it. It is a multi-layered system to protect the assets, resources, people and pride of the county. A complex multi-layered security system is also needed for achieving the safety of any organisation.

Different layers of security are needed for any organisation to protect their operations. They can be as follows:

- Physical security can be employed to protect physical items and objects from unauthorised access.
- Personnel security needs to protect the employee or a group of employees who are authorised to access operations of the organisation.
- Operations security is to protect the details of an operation or series of operations of an organisation.

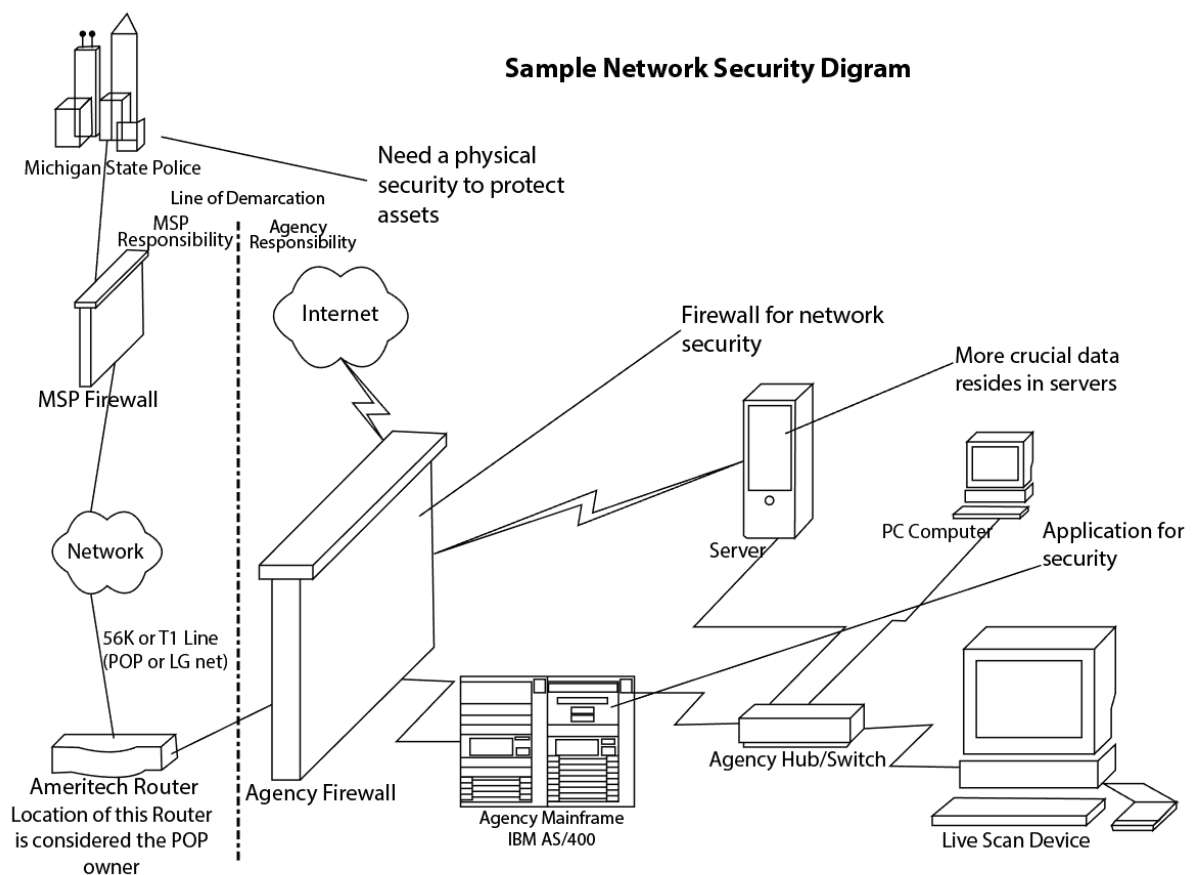


Figure 1.1.1 Simple Network Security

Communications security is needed to protect communication medium, technology and critical data of an organisation.

Network security is critical in protecting networking components & their connectivity and content, which follow through the network components.

Information security can be employed to protect the confidentiality, technology, storage process, transmission system and integrity and availability of information assets. It can be achieved by imposing different security policies, training & awareness and technology.

From figure 1.1.1, we can say that all physical assets need physical security, application level security can be used by using custom or dedicated application built for their security, network security can be used to protect intruders to penetrate the system through the internet and personal security can be used to access the PC of the network.



Advantages:

- Protects the data and resources of the organisations
- Provides secure and authenticated communication within and outside organisation
- Provides confidence and reliability to client about the organisation
- Provides a secure payment process for the users to do online transactions



Disadvantages:

- Increases the complexity of the communication
- Organisations are investing huge money for providing security for its upgradation.
- Decreases the productivity of the organisation as proving authenticity of the users every time.
- A dedicated team is required to monitor the security, giving training and modifying the access repeatedly.

(iii) Basic Principles

Information security stands strong based on three fundamental principles, which can be used to protect resources available in internetworking.

The principles are Confidentiality, Integrity and Availability.

- **Confidentiality** assures that the resources of an organisation can access only by authorised persons or objects.

Example: Every bank encapsulates a protection for customer details by providing PIN numbers to the ATM cards through which they can access their confidential details.

- **Integrity** assures consistency, accuracy and trustworthiness of data throughout organisational process transits. Integrity marks an assurance that, all the changes happened to data or resources are through authorised supervision only.

Example: banks protect the integrity of customer information by letting them set up alerts when their money is withdrawn from their account, irrespective of who made the transaction.

- **Availability** assures that resource or data is always available to authorised persons whenever they want to access them.

Example: Most of the banks are in a position to provide the account information to their customers at any point of time and place through various sources like internet banking, mobile banking, ATM services, etc.

(iv) Information Security Applications

Few applications of Information Security are:

- Physical and personal security can be provided by using biometric and retina scans.
- Firewalls, IDPs, honeypots, honeynets can be used for providing network security.
- Cryptography techniques are used to hide the original message, i.e., it provides communication security.
- Antivirus and anti-worms mechanisms can be used to protect the system from malicious software's.
- Secure Socket Layer provides the security at application level.
- Kerberos can be used for secure ticket processing.
- Secure electronic transactions (SET) can be used for securing the electronic transactions.
- Pretty Good Privacy can be used for encrypting and decrypting the emails.
- Digital signatures can be used for authenticating the messages or file transmissions.



Self-assessment Questions

- 1) Resources of the organisation can only be accessed by authorised users is termed as _____?
 - a) Authenticity
 - b) Availability
 - c) Durability
 - d) Confidentiality
- 2) When was ARPANET designed?
 - a) 1980's
 - b) 1960's
 - c) 1990's
 - d) 1950's
- 3) Which kind of operating system is MULTICS?
 - a) Batch Processing
 - b) Multiprogramming
 - c) Time sharing
 - d) Standalone
- 4) Firewall is an example for which level security?
 - a) Personal
 - b) Physical
 - c) Network
 - d) Communication

1.1.3 Key Information Security Concepts

Basic terms used in Information Security are as follows:

- **Attack:** Attack is an act that can cause damage or compromise to physical or logical resources of an organisation.

Attacks can be intentional or unintentional, active or passive and direct or indirect. Casually reading the sensitive data from the system without any damage can be considered as a passive attack, whereas doing harm or damage to the data can be treated as an active attack.

If a hacker tries to break information system, then it is an intentional attack, whereas damage due to natural disaster can be considered as an unintentional attack.

The hacker uses his/her personal computer for the attack in a direct attack, whereas the attack by other means is an indirect attack.

- **Exploit:** Any technique or method used to compromise a security system can be considered as an exploit.

An exploit may be a systematic process of security violation followed by an attacker, which focuses on the vulnerability in existing software or networking components or process related aspects to damage the security system or compromise the system.

- **Vulnerability:** A fault in a system or process or security mechanism, which opens a chance for an attacker to perform damage, can be considered as vulnerability.

For example, a glitch in the software package, weak network ports, house with limited security, etc.

Most of the vulnerabilities are detected, but many of them are undetected or newly emerged because of the large growing IT field every day.

Threat: A section of objects, which presents a danger to an asset or resource or information. Threats may be intentional or unintentional and create a heavy damage to the organisation.

For example, hackers intentionally threaten the unprotected security of information systems, whereas heavy storms unintentionally threaten buildings and their contents.

- **Resource:** It is an organisational asset which needs protection. An asset can be either logical or physical.

For example, Web site, information, or data are *examples* of logical assets, whereas a person, computer system, or other tangible objects are physical assets.

- **Access:** It is an ability of a person or an object to manipulate, modify or affect some other subject or object of the system. Authorised users are legal objects to access a system, but hackers act as an illegal objects to access a system. Access to a system can be regulated by using Access controls.
- **Damage:** It is harm or loss caused to the security system by stealing or damaging or modifying the existing resource from the system. The magnitude of damage happened to the system will be a clear measure for loss occurred to the organisation.

- **Threat Agent:** The specific instance or a person or incident, which causes the threat, can be considered as a threat agent.

For example, an individual hacker (he/she) can be considered as a threat agent. Similarly, all natural calamities, which disturb and cause damage to information, can also be considered as a threat agent.

- **Policy:** A policy is set of high level rules which give do's and don'ts of an organisation.
- **Protection Profile or Security Posture:** It is a set of all security measures and counter measures an organisation follows for securing the system can be considered as a Protection Profile. It includes policy, training & awareness and technology that an organisation follows or implements to safeguard their assets.

Subjects and Objects: A system or individual performs an attack is a subject, whereas if it suffers from attack then it is an object. A computer can be both subject and object. *For example*, if a hacker uses a computer to attack a system in that point hacker system is a subject, if another hacker hacks the same system then it becomes an object.

- **Control, Safeguard or Countermeasure:** Counter attack performed over an attack can be considered as a counter measure. This countermeasure can be a policy or Security mechanisms, which will reduce risk and improves the security of an organisation.
- **Risk:** It is the probability of damage or compromise happens to the system, which is unwanted to the organisation. Organisations always try to minimise risk.

Every organisation tries to calculate the risk, which it can tolerate with the existing countermeasure it has planned.

- **Cryptography:**

Art of hiding the original message from the intruders with mathematical or scientific methods.



Self-assessment Questions

- 5) Probability of damage is also known as _____.
a) Risk
b) Loss
c) Exploit
d) Error Rate
- 6) System which performs an attack is termed as _____.
a) Object
b) Source
c) Target
d) Subject
- 7) A passive attack is _____.
a) Just reads the information
b) Adds the content to information
c) Deletes the information
d) Misplaces the content
- 8) Counter measure is a _____.
a) Percentage of information damage
b) Counter attack for attack
c) Program to restrict intruders
d) Measurement for physical attacks
- 9) Method used to make security system to compromise can be termed as _____.
a) Client
b) Decoy
c) Object
d) Exploit

1.1.4 Components of Information System

An information system is not just a computer hardware it is a combination of multiple elements such as software, hardware, people, data, network and procedures. All these six basic elements enable the information to be input, processed, output and stored. All of these components have their strengths and weaknesses with respect to the information system. Each component has their own security requirements.

They are as shown in the figure 1.1.2:

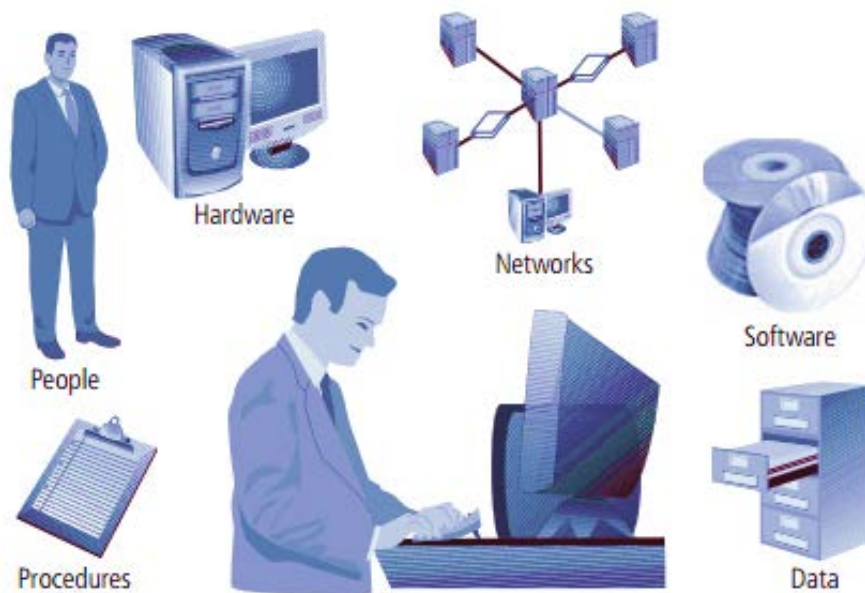


Figure 1.1.2: Components of an information system

As shown in the figure 1.1.2, the components of information systems are interconnected with each other. People of the organisation use software for their regular business activities. The software in turn interacts with hardware to save and process the data. Data is stored in different file systems such as database. All the systems and software's interact with each other by using the network. The stored data can be accessed by different people for their regular work using the organisation network. Through the network, people can interact with private networks.

(i) Software

This component is the most critical and crucial because most of the information flow happens through it. This component includes an operating system, application software and device utilities. IT industry has a high degree of possibilities to have bugs and other

fundamental problems in software. Most of the crucial information on any organisation flows through the software, which it uses for its daily needs. A small glitch in the software provides more scope for vulnerabilities, which makes the system more prone to attacks. In fact, our daily life is affected by most of the software's with bugs, Smartphone apps are the best *example* for it.

Software development in the market are done with very limited workforce and with the nasty deadlines, which creates software's with more holes in it. Most of the software development processes will consider the security of it as an external component rather than including it as a basic component, which makes the software more prone to security damages.

(ii) Hardware

Hardware is always a physical and visible asset of an organisation or an individual. The hardware provides a chance to mount software's over it and executes them, stores data, transports data and provides an interface for the adding and removing information from or into the system.

Most of the organisations provide physical security to the hardware such as lock and keys, providing access rights to only a few who are authorised employees of the organisation. Physical security may not be enough to protect the hardware because the hardware components are not provided with security measures and theft memory could cause information loss, therefore security at software level can be only protect it.

(iii) Database

Data is one of the vital resources for any organisation, so a greater level of effort is needed to protect it. Data would be the ultimate target for any intruders or attackers. Small loss of data will result in a huge damage to organisation growth. Protection at each level of data transfer is needed. Most of the software project management teams are neglecting the usage of the security measures provided by DBMS, which makes the database weak on security. Physical theft of the system will result in the loss of crucial data. So, take advantage of all the security levels available at software to protect data from the external world.

(iv) People

People who are working inside/outside of organisations are the powerful and weak to provide the security to organisation information assets. Every organisation must provide various kinds of access rights to the people by implementing the access control registers based on the

position of the employees. Every organisation must design and implement organisation policy about how to use the data, what are the penalties for misuse of information. Also, they have to conduct various kinds of training programs to educate and create the awareness in employees on various aspects like how to use the technology, what is the need for securing the information, etc.

(v) Procedures

Another aspect where most of the organisations are facing problem for providing the security to their information is due to their procedures. A procedure is nothing but a set of designed instructions to perform specific actions for organisational activities. If any organisation fails to provide the knowledge on importance of these procedures to their employees, then it can cause a great loss to the organisation. Every organisation must distribute the policies and the procedures for every individual without fail. Special training should be given to the employees to work with procedures.

(vi) Networks

In most of the cases, the external objects/intruder of the company tries to intrude into the system by using their network; hence it needs a great level of security to be implemented in this component. A small compromise in network security will create vulnerabilities, in turn, it may create damage. Here security can be implemented either at the entry level of the network with some filtration rules or allow the intruder to penetrate the system but implement a counter attack on the intruder system. Physical level security may not be much helpful at this level but cannot be neglected.



Self-assessment Questions

- 10) A collection of raw facts is known as _____.
 - a) Information
 - b) Database
 - c) DBMS
 - d) Data
- 11) Which of the following is a procedure?
 - a) Set of programs
 - b) Set of software's
 - c) Set of specific instructions
 - d) Set of Hardware
- 12) External objects intrude into the system through _____.
 - a) Procedures
 - b) Process
 - c) Network
 - d) Hardware
- 13) Which component of the security system does a virus or a worm attack?
 - a) Hardware
 - b) Software
 - c) JavaScript
 - d) Procedure
- 14) Which of the following are the biggest assets and weakest security glitch for any organisation?
 - a) People
 - b) Procedures
 - c) Hardware
 - d) Software
- 15) Which among the following options will create a scope for vulnerability?
 - a) Over usage of hardware
 - b) Compromise in network security
 - c) Training the employees about policies and procedures
 - d) Avoiding internet working



Summary

- Information is the important assets of any organisation even a small loss in data will create great damage to business activities.
- Every organisation must implement the security measurements at various levels, such as physical level, communication level, people level, Operational level security etc.
- Computer security is the key source for designing the information security since 1960's to present era.
- There are various tools to provide the security at every level. Like firewalls at the network level, biometric, password techniques at physical level are some examples.
- Every organisation must design the information policies and same to be distributed among the employees. Periodically organisation should conduct training and awareness programs to employees about policies, procedures, technologies to safeguard the various information assets of the organisation.
- Basic principles of data should retain at every transitional stage of the data.
- There are number key terms such as agent, asset, risk, vulnerability, exploit, subject and object.
- The main parts of any information system are hardware, software, people, network, data and procedures.



Terminal Questions

1. Elaborate on the history of information security.
2. What are the basic concept and principles of Information Security?
3. What is security? Why it is needed? List few applications of information security.
4. What are the strengths and weaknesses of information system components?



Answer Keys

Self-assessment Questions	
Question No.	Answer
1	d
2	b
3	c
4	c
5	a
6	d
7	a
8	b
9	d
10	d
11	c
12	c
13	b
14	a
15	b



Activity

Activity Type: Offline

Duration: 30 Minutes

Description:

Form groups and chart the importance of Information Security in current era.

Case Study

Myfootware Corporation is a new company that has started very recently. It was a footwear manufacturing industry. It has a lot of wings in their organisation they are as follows:

- Design section: where the designer are occupied and it is a very confidential area because it has designs which cannot be disclosed.
- Manufacturing section: where manufacturing happens most of the employees working here are illiterates and it includes contract employees also.
- Logistic and dispatch section: where most of the external people will be entering collect their stock.
- Management section: where all the official transaction does happen here and all confidential documents do exist here.
- A cafeteria: where all the employees, visitors will have refreshments here.

Now the management of MyFootware Corporation wants to install security systems at all the points of their industry. Now the managements is confused which kind of security system is feasible at which point.

1. Building an information Security for information system needed for Myfootware Corporation.
2. According to you, what are the best places to deploy the security system to stop the intruders?

Bibliography



e-References

- *Information Security*. Retrieved 5 Jan, 2017 from <https://www.us-cert.gov/sites/default/files/publications/infosecuritybasics.pdf>
- *History of Information Security*. Retrieved 5 Jan, 2017 from <https://www.villanova.edu/resources/iss/history-of-information-security/#.WHShX1N96M9>
- *Basic Security Concepts*. Retrieved 5 Jan, 2017 from <https://danielmiessler.com/study/infosecconcepts/#gs.dhhxVfg>

Image Credits

- Figure 1.1.1: http://www.gridgit.com/postpic/2012/04/sample-network-security-diagram_318703.png
- Figure 1.1.2:
http://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf



External Resources

- Stallings, W. (2000). *Network security essentials: applications and standards*. Upper Saddle River, NJ: Prentice Hall.
- Whitman, M. E., & Mattord, H. J. (2009). *Principles of information security*. Boston, MA: Thomson Course Technology.
- Zelkowitz, M. V. (2004). *Information security*. Amsterdam: Elsevier Academic Press.



Video Links

Topic	Link
Introduction to information Security	https://www.youtube.com/watch?v=yFRc-wpQc9c
Information Security	https://www.youtube.com/watch?v=eUxUUarTRW4
25 years of information security	https://www.youtube.com/watch?v=oIbl1jVUkJs



Notes:



Chapter Table of Contents

Chapter 1.2

Balancing Information Security and Access

Aim.....	21
Instructional Objectives.....	21
Learning Outcomes.....	21
1.2.1 Introduction.....	22
1.2.2 Introduction to CNSS Security Model.....	22
1.2.3 Critical characteristics of Information	27
(i) Confidentiality	28
(ii) Integrity	28
(iii) Availability.....	29
Self-assessment Questions.....	30
1.2.4 Balancing Information Security and Access	31
Self-assessment Questions.....	32
1.2.5 Approaches to Information Security Implementation.....	32
(i) Top-down Approach	32
(ii) Bottom-up Approach	33
Self-assessment Questions.....	34
1.2.6 Security Professionals and the organisation	35
(i) Senior Management.....	35
(ii) Information Security Project Team	36
(iii) Data Responsibilities	36
Self-assessment Questions.....	37
Summary	38
Terminal Questions.....	40
Answer Keys.....	41
Activity.....	42
Case Study	43
Bibliography.....	44
e-References	44
External Resources	44
Video Links	45



Aim

To equip the students with the knowledge of security measure and approaches that can be used to improve the security of the system within the organisation



Instructional Objectives

After completing this chapter, you should be able to:

- Explain full range of available security measures, according to the CNSS model
- Classify the key characteristics of information that must be protected by information security
- Describe the factors that must be considered when balancing information security and access
- Elaborate the approaches used to improve the security of the system
- Enumerate the information security roles of professionals within an organisation



Learning Outcomes

At the end of this chapter, you are expected to:

- Outline all the 27 aspects of security with respect to CNSS security model
- List the characteristics of information i.e. with respect to the CIA Triangle
- Recognise the imbalance that can occur when the needs of the end user are undetermined
- Outline key advantages and drawback of top-down and bottom-up approach
- Identify the range of professionals to support information security program
- Summarise how cipher block chaining can be used to construct a hash function
- Compute SHA-512 logic for a specific scenario

1.2.1 Introduction

The security system of an organisation is an uncompromised sector. This should be given high priority because of the effort made in building resources cannot be kept in the hands of the intruders. To build a strong security system, the need for security has to be analysed and planned. If required, expert advice should be sought to build a strong security system. The standard implementation model can be employed for building it. The final step is verifying and testing the implemented system with the existing standards, which is also important.

This chapter focuses on the importance of information and methods to safeguard the system. It analyses the importance of building security system and their implementation challenges. It also focuses on balancing between security system requirements and its implementations. The chapter concludes by discussing the types of people involved in building a strong security system.

After completing this chapter, students will be able to judge whether the system is secure or not. They can also explain whether it is balanced or has practical difficulties.

1.2.2 Introduction to CNSS Security Model

The Committee on National Security Systems (CNSS) states that “information security is the protection of information and its critical elements, including the systems and hardware that use, store and transmit that information”.

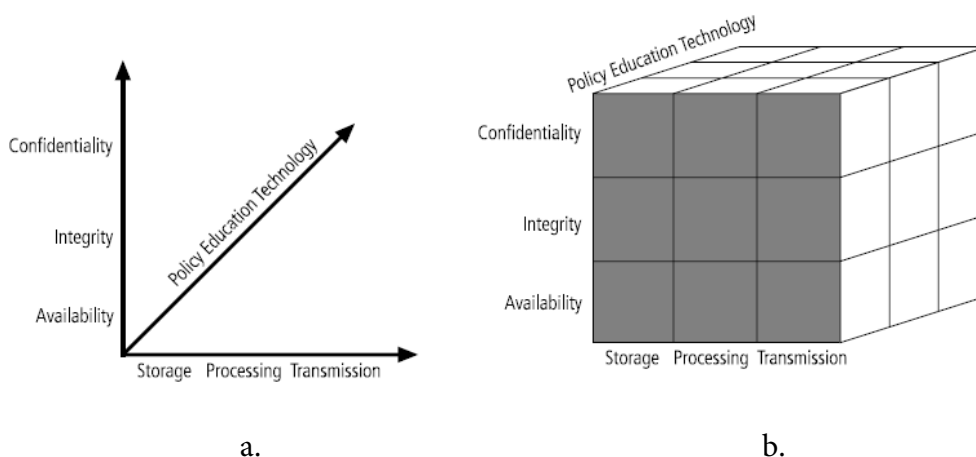


Figure 1.2.1 CNSS Security Model

CNSS document provides a base and complete information security model. It is a widely accepted evaluation standard for information systems security. It was designed by John

McCumber in 1991. It provides a graphical representation of the information security architectural approach. This graphical representation has a cube with 3 dimensions with 3 elements in each dimension as shown in Figure 1.2.1 (a). Hence, it is also known as McCumber Cube. The McCumber Cube has a total of 27 cells as shown in Figure 1.2.1 (b). The security solution of the organisation must be able to address all 27 small cells of the big cube. Let us consider the intersection of storage, availability, technology from Figure 1.2.1 (b), which checks whether the technology used for securing the storage is allowing the authorised user for accessing the storage any time? If the answer is yes, then we can move ahead and check next cell, if the answer is 'No' it mean that the solution must be corrected to make it available.

A verification table for security system can be prepared as shown in table 1.2.1. If all the questions of the questionnaire are having an answer as yes, then it indicates that the system is very secure, otherwise a discussion can be made to decide which factors can be neglected.

Table 1.2.1 Evaluation table for security system

Cube No.	X-Axis	X-Axis	X-Axis	Questionnaire	Yes/No
1	Storage	Confidentiality	Policy	Is the policy available for saving confidentiality of storage	
2	Processing	Confidentiality	Policy	Is the policy available for saving confidentiality of Processing	
3	Transmission	Confidentiality	Policy	Is the policy available for saving confidentiality of Transmission	
4	Storage	Confidentiality	Education	Is the confidentiality of storage educated	

5	Processing	Confidentiality	Education	Is the confidentiality of processing educated	
6	Transmission	Confidentiality	Education	Is the confidentiality of transmission educated	
7	Storage	Confidentiality	Technology	Is the technology protecting the confidentiality of storage	
8	Processing	Confidentiality	Technology	Is the technology protecting the confidentiality of processing	
9	Transmission	Confidentiality	Technology	Is the technology protecting the confidentiality of transmission	
10	Storage	Integrity	Policy	Is the policy available for saving the integrity of storage	
11	Processing	Integrity	Policy	Is the policy available for saving the integrity of processing	
12	Transmission	Integrity	Policy	Is the policy available for saving the integrity of Transmission	
13	Storage	Integrity	Education	Is the integrity of storage educated	

14	Processing	Integrity	Education	Is the integrity of processing educated	
15	Transmission	Integrity	Education	Is the integrity of transmission educated	
16	Storage	Integrity	Technology	Is the technology protecting the integrity of storage	
17	Processing	Integrity	Technology	Is the technology protecting the integrity of processing	
18	Transmission	Integrity	Technology	Is the technology protecting the integrity of transmission	
19	Storage	Availability	Policy	Is the policy available for of storage	
20	Processing	Availability	Policy	Is the policy available for of processing	
21	Transmission	Availability	Policy	Is the policy available for transmission	
22	Storage	Availability	Education	Is the availability of storage educated	
23	Processing	Availability	Education	Is the availability of processing educated	
24	Transmission	Availability	Education	Is the availability of transmission educated	

25	Storage	Availability	Technology	Is the technology making the storage available	
26	Processing	Availability	Technology	Is the technology making the processing available	
27	Transmission	Availability	Technology	Is the technology making the transmission all the time available	

When a security system built, after being evaluated based on the criteria described above is successful, then it is a very good security system. It is practically very challenging to build a system, which does not compromise the security system of the organisation.



Self-assessment Questions

- 1) What is CNSS model used for?
 - a) Planning the security system
 - b) Designing the security system
 - c) Evaluating the security system
 - d) Deploying the security system

- 2) Which of the following sets the specified valid dimension of McCumber Cube?
 - a) {storage, technology, transmission}
 - b) {storage, policy, confidentiality}
 - c) {storage, availability, integration}
 - d) {storage, processing, Transmission}

1.2.3 Critical characteristics of Information

Characteristics of information will decide the value of the information. If characteristics of information changes then sometimes it increases the value of it, but most of the times it decreases. A few characteristics of information affect information's value to users more than others do. Most of the times it depends on the circumstances; *for example*, in time critical applications or transactions, information will lose its complete value when it is not being delivered within the time line decided.

Even though security professionals and end users have a clear understanding of the characteristics of information, few tensions will arise if the end user wants unrestricted access to information. This could lead to threats even during the unrestricted access.

A critical characteristic of any information can be expressed by using C.I.A. (Confidentiality, Integrity and Availability) triangle; details of it are as shown in Figure 1.2.2.

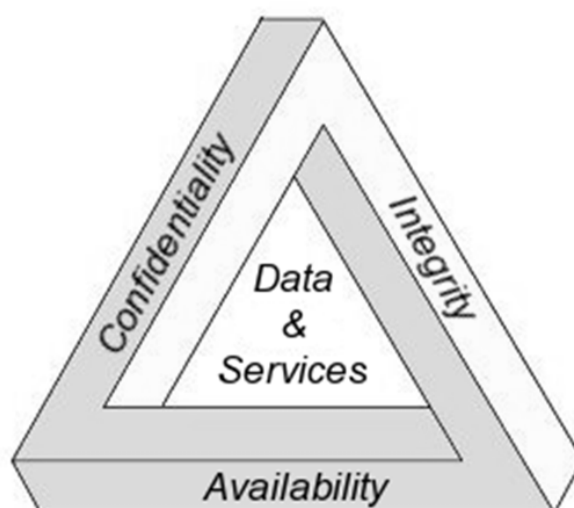


Figure 1.2.2: CIA Triangle

The figure shown above depicts that all the services and data of the organisation are protected by using these three attributes such as confidentiality, integrity and availability and these important attributes are described below:

(i) Confidentiality

Information confidentiality can be confirmed when the information is accessible only by authorised members or objects of the organisation. When an unauthorised user accesses the resources of the organisation, then it is considered as a security breach. Security professional always tries to protect the information access from the unauthorised users or objects. To protect the information confidentiality many measures need to be implemented, few of them are as follows:

The information is usually classified into two types i.e., critical and non-critical. More security needs to be enforced for the storage section of the organisation where critical documents are stored. The application should be designed and used in such a way that it ensures the proper security policy's execution and the proper education of all the users of the organisation about the security policy of the organisation.

Confidentiality of the information is one of the unique selling points of most of the organisations. Confidentiality in simple terms can be called as privacy. Most of the organisations consider their transaction, customer and employee details as most confidential; if they are disclosed by any means, then it is considered as a big security breach.

Most of the times, simple security glitches happen unintentionally, which needs to be taken care to ensure confidentiality. *For example*, sending email with confidential details to an outsider of the organisation by mistake, throwing away of documents containing important information without shredding it properly. Most of the time hackers will be waiting for such kind of mistakes, even if they find few details of the customers, they can reconstruct complete details from the available details. An employee of the organisation knows that if he carry's bulk content, he will be caught, but if he carry's small piece of information every day without any notice, one day he can reconstruct entire data. This kind of approach can be called as salami theft.

(ii) Integrity

The integrity of the information can be confirmed only when it is complete and uncorrupted. The integrity of the information is lost when the information was corrupted or distracted or damaged by any source. The integrity of information can even get disturbed during the transit of information from one system to another system through the network. Worms and viruses are an important source, which disturbs the integrity of information.

The integrity of information can be checked by closely monitoring the changes in the file attributes such as file size or hash value. By using special hashing algorithm hash value of the file will be calculated, then this hash value will be stored in a secure place. Change in hash value is an indication of the corruption of data which can be reconstructed by using data reconstruction algorithms.

The integrity of information can even get disturbed by the noise in transmission, low voltage transmissions, etc., if the errors are very minimum, then error correction algorithms can be used to reconstruct the original information.

(iii) Availability

Availability of information confirms that an authorised user or object will be given access to the required information in the required format without any obstacles or interruptions.

Example: most of the employees of the organisation of IT world will continue their work from home in some cases of emergency. To continue their work, they need access to most of the critical resources of the organisation from the external network. To provide the access their credentials are accepted and verified with the user's access permissions. If the credentials are matching, then the access will be given. Now, he is free to use his resources without any interruptions. It makes the system available and more secure too.



Self-assessment Questions

- 3) Which of the following attributes of information confirms that an authenticated user must access all the resources, which he is authorised to access?
 - a) Availability
 - b) Integrity
 - c) Confidentiality
 - d) Redundancy

- 4) Which of the following attributes of information confirms that only authorised users can assess the resources of the organisation?
 - a) Availability
 - b) Integrity
 - c) Confidentiality
 - d) Redundancy

- 5) Which of the following attributes of information confirms that information available is complete and uncorrupted?
 - a) Availability
 - b) Integrity
 - c) Confidentiality
 - d) Redundancy

- 6) Which of the following algorithm is not used for checking the integrity of information?
 - a) Hashing Algorithm
 - b) Error detection algorithms
 - c) Parity Check
 - d) Bubble sort algorithm

- 7) Throwing a document with important information, without proper shredding is a security glitch for which of the following characteristics of information?
 - a) Availability
 - b) Integrity
 - c) Confidentiality
 - d) Redundancy

1.2.4 Balancing Information Security and Access

It is highly impractical to expect or create a complete information security system to meet the current needs. Information security is a process and it cannot be a goal. The ideal security system will never allow anyone to access the resources of the organisation. Every organisation of the present era expects their system to be available to anyone, anywhere, anytime, through any means but this approach creates a danger or threat to the security system. So a balance between the security policies and the secure access is highly recommended now a days as shown in figure 1.2.3.

Factors which are to be considered for balancing the system are Access to the system, Protection level requirements, Legal problems on violation of policy, privacy requirements, cost of implementation and maintenance.

A reasonable balance between information security measures and access requests of users must be a key focus. This balance can be achieved only when a proper study on the need for restricting measures, the level of access rights and type of security measures required to be taken by the senior level management people of the organisation. If restrictions are highly required, then the user needs to be educated on the same needs, so that the balancing measures can be planned further.



Figure 1.2.3 Balance between security and access



Self-assessment Questions

- 8) Every organisation today expects the system to be accessible to _____.
a) Only a few prisons, only a few locations, only in specified time
b) Any prisons, only a few locations, only in specified time
c) Anyone, anywhere, anytime
d) Anyone, anywhere, only in specified time
- 9) Which of the following is true regarding the ideal security system?
a) Will allow everyone to access the system
b) Will restrict only few members
c) Will allow only admin to access the system
d) Will never allow anyone to access the system

1.2.5 Approaches to Information Security Implementation

Implementation of a security system of an organisation is not a simple task. It involves a lot of people and planning, managing them needs a lot of planning and the models to be followed. Among all such approaches, Top-down approach and Bottom up approaches are the best. Depending on the size, time and budget of the organisations, they can choose one among them. They can be explained as follows:

(i) Top-down Approach

In this approach, project requirement is decided by the top management team. Top management will decide the process, policy, goals and expected outcomes. The terms and policies decided will be passed to project development team. As the requirements are decided by the top management team, hence financial support is very high. The requirement of the CIO cannot be denied; hence the project execution will be much faster than the bottom up approach.

In a few cases, the project development life cycle will also be involved and complete study is conducted.

The main advantage of this approach is champions like Chief Information Officer (CIO) and Vice President- Information Technology (VP-IT) will directly involve in the project execution, hence finance deficit will be very minimum and mid-level employees will consider

the project as a high priority and speed up the execution process. End-users can be directly involved in this process. Key end-users can also be involved in process execution, which can be called as Joint Application Development (JAD). In this case, documentation will play a very vital role. So all the processes and procedures must be documented and employees of the respective organisation should be trained accordingly. An organisation which is about to start and is newly started can adopt this approach because very limited planning is needed and expert advice may not be needed, hence senior management can handle the implementation.

(ii) Bottom-up Approach

The complex security system of any organisation cannot be implemented without any plan or experts. This entire process cannot be done within a single day. An incremental process from deep roots could be the best recommendation for this approach. This kind of approach can be named as bottom-up approach.

The most crucial advantage of the bottom-up approach is that the expert can carry deep study of the information system. On a daily basis, within a few days, they understand the threats possible and the level of restriction required at initial stages and plans the security requirement for future problems. Based on the knowledge they collected for the existing system, a complete security system plan can be generated.

Unfortunately, organisational waiting and investing power, the end users participation is an important restriction for the bottom-up approach.

The organisational hierarchy and the bottom-up and top-down approaches are illustrated in Figure 1.2.4.

Organisations which are well established and running for very long duration can go for this approach because here expert study is very much required. Implementation of a security system in this kind of organisations can take a bit more budget and time for the implementation.

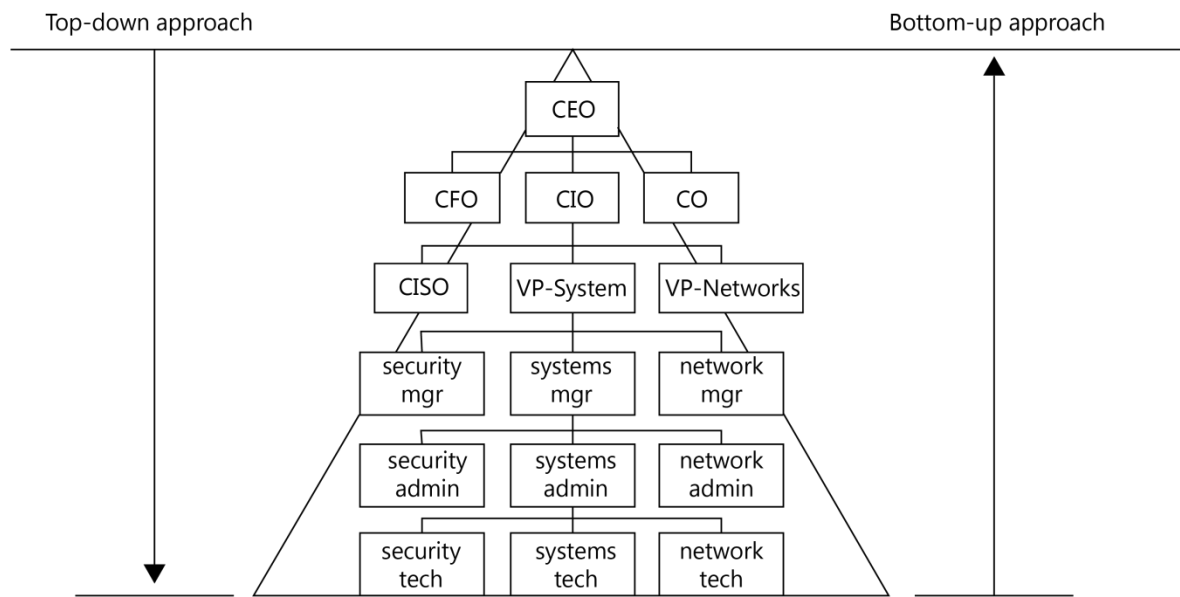


Figure 1.2.4. Organisational Hierarchy

Any of the approaches can be used for building the security system because none of them prefers to have a compromise in the security system. Thus, building a strong security system is the ultimate goal.



Self-assessment Questions

- 10) Which of the following property is not true with respect to bottom up approach?
 - a) Policies, procedures are decided by top management
 - b) A study on the existing systems is done day-by-day
 - c) Expert will study the complete system
 - d) Complete planning is done before implementation of the system

- 11) Which of the following is an advantage of bottom up approach of security system implementation?
 - a) Too much waiting time
 - b) Good expert advice
 - c) Inactive end user
 - d) Huge investment

1.2.6 Security Professionals and the organisation

Information security implementation inside the organisation includes support of different professionals. A key source for successful implementation of security is always senior management people. Of course, there are other administrative staffs that will take care of designing various procedures and policies and technical team for deploying the information security details.

The various responsibilities, roles for different professionals are given below:

(i) Senior Management

Senior management is a team employee who takes crucial decisions and plays a very important part in organisational development. Even security system implementation and policy design is done by senior management. Based on the size and distribution of organisation, the team size will increase and decrease.

Chief Information Officer (CIO): CIO is the senior technology officer also known as vice president of information or information technology or systems. The primary job of a CIO is implementing the strategic information plans by sharing the strategic plans of the organisation with the various professionals like the president, executive officer. After completion of strategic information plans, to empower the planning and systems management to support the activities of the organisation, CIO works along with other managers for designing the tactical and operational plans. He also enforces the order of execution.

Chief Information Security Officer (CISO): CISO's primary responsibility is identifying, organising and implementing the organisation's information security system. CISO is also known as the manager for IT, administrator for security. Chief information security officer reports to chief information officer. CISO also responsible for:

- Design and implement the security metrics
- Security Compliance program development
- Audit with the external and internal agencies
- Security incidents and response evaluation
- Technology updating
- Implemented security measures according to government standards.

(ii) Information Security Project Team

This project team includes a number of technical and non-technical persons who are having experience in one or more areas.

Information security project team member's roles are as follows:

- **Champion:** Senior executive officers, whose responsibility is project initiation and see that it supports, administratively and economically, at the organisation level.
- **Security policy developers:** People who know the organisation policies and values. The role of security policy developers is to design and deploy new policies, according to the needs of the organisation.
- **Team leader:** Also known as project manager, departmental line manager or staff unit manager. The responsibility of team leader is to understand the project management and technical requirements for information security.
- **Security professionals:** Trained, committed and educated people, who are professional in all aspects of technical and non-technical for providing the information security.
- **Risk assessment specialists:** These specialists assess various kinds of risks inside the organisation like financial, organisational assets and information security methods.
- **Systems administrators:** People whose key role is to provide and maintain the organisation information and also system administration within the organisation.
- **End users:** People who are going to use various kinds of organisational data for implementing or to work with organisational activities or applications. End users retrieve the information according to the department, access rights.

(iii) Data Responsibilities

The duties of various owners of data mentioned below:

- **Data custodians:** People who directly report and work with data owners. Duties of data custodians are identifying the storage for data depending on organisation size, maintenance, providing procedures and policies for information security aspect and implementing the backup and recovery procedures for organisational information assets.
- **Data owners:** People whose primary responsibility is protecting the organisational data. Data owners are the top-level management people. They usually create various access permissions to the different users based on the position inside the organisation.

Data owners work with subordinates to maintain the integrity and updating of data on a day-to-day basis.

- **Data users:** People whose responsibility is to use the organisational data for fulfilling the organisational activities and goals. Security of data in each level is important and should be done by every individual who are part of the organisation.

Collective working of all these professionals can only build a strong security system. Building a strong security system can be possible only with well-planned and organised process implementations. Most of the organisations have implemented this simple logic and they are quite successful in the business.



Self-assessment Questions

- 12) Project requirements are decided by CIO of the organisation in the case of a top-down approach to the security system implementation.
 - a) True
 - b) False
- 13) Which of the following positions cannot be considered as the senior management team for an organisation?
 - a) CIO
 - b) CISO
 - c) Vice President
 - d) Senior Programmer
- 14) Which of the following positions cannot be considered as information security project team for an organisation?
 - a) Team Leader
 - b) Vice President
 - c) Security Policy Developers
 - d) System Administrators
- 15) Which of the following is not a type of data ownership?
 - a) Data Owners
 - b) Data Custodians
 - c) Data Users
 - d) Data Creators



Summary

- The CNSS security model can be used for evaluating the security system built for any organisation, it has a 3x3x3 cube for representing {storage, processing and transmission} in x-axis, {confidentiality, integrity, availability} in the y-axis, {policy, education, technology} in the z-axis. Each small cube among 27 cubes should be addressed while building the security system
- Information is the critical component of any organisation safeguarding. It employs properties like Confidentiality, Integrity and availability by using the security system built within the organisation. It is called as a C.I.A triangle.
- Confidentiality: only authorised user must access critical resources.
- Integrity: Every information available must be complete and uncorrupted.
- Availability: information must be available to anyone, anywhere, anytime.
- The ideal security system cannot suffice the need to present the world so balanced security system makes the resources available anywhere, anyone, any time requirement of the industry.
- Implementation of the security system can follow top down or bottom up approach.
- Management will decide the requirements and team goes with it is top down approach.
- Experts will study the system and decide the requirements that can be considered as bottom-up approach.
- The information security implementation and management are done by many professionals inside the organisation. They are senior management people, information security project team and data management team.
- The senior management people are the key persons for deploying security of information.

- The Chief information security officer identifies the strategic plans of business based on that they will convert these plans to strategic information plans.
- The information security team consists of various technical and non-technical people like a champion, leader, team leader, security professional, developers etc.



Terminal Questions

1. Explain the CNSS Security Model.
2. “Every organisation must balance the information”, Explain.
3. Write a note on CISO, Data Owners, Data Custodians, Team Leader.
4. Compare and contrast top-down and bottom-up approaches.
5. Define CIA triangle. Explain the characteristics of information.



Answer Keys

Self-assessment Questions	
Question No.	Answer
1	c
2	d
3	a
4	c
5	b
6	d
7	c
8	c
9	d
10	a
11	b
12	a
13	d
14	b
15	d



Activity

Activity Type: Online/Offline

Duration: 30 Minutes

Description:

Discuss in groups about various pros and cons of top-down and bottom-up approach and figure out which approach is more suitable to keep the system secure.

Case Study

Myfootware Corporation is a new company started very recently. It is a footwear manufacturing industry. It has lot of wings in their organisation they are as follows:

- Design section: where all the designers are working on designs and it is a very confidential area because it has designs which cannot be disclosed.
- Manufacturing section: where manufacturing happens, most of the employees working here are illiterates and it includes contract employees.
- Logistic and dispatch section: where most of the external people will be entering and collecting their stock.
- Management section: where all the official transactions happen and all confidential documents exist here.
- A cafeteria: where all the employees, visitors will have refreshments.

Management of Myfootware decided to install biometric machines for the designing section, manufacturing section and employees are provided with access cards. They also provided the Logistic section with temporary id and security guard, management section with biometric doors. Security cams and biometric lockers were installed to store documents and cafeteria does not need any security. All the biometric machines installed in the organisation will accept only single finger scanning model.

Answer the questions:

1. Which section of the company has more security threat and how it is resolved?
2. In which section of the company, the balance of the security system is missing and why?
3. What are the secondary backup measures you suggest for each section (*example*: card missing, fingerprint not reading, etc.).

Bibliography



e-References

- *CNSS Security Model*. Retrieved 5 Jan, 2017 from <http://www.aplontech.com/index.php/articles-and-tutorials/it-security/73-cnss-security-model>
- *Critical characteristics of Information*. Retrieved 5 Jan, 2017 from <https://www.scribd.com/presentation/168581476/Critical-Characteristics-of-Information-In-Information-Security>
- *Balancing Information Security and Access*. Retrieved 5 Jan, 2017 from <http://www.ciscopress.com/articles/article.asp?p=1152146&seqNum=2>

Image Credits

- Figure 1.2.1.a: http://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf
- Figure 1.2.1.b: http://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf
- Figure 1.2.2: <https://blogs.technet.microsoft.com/seanearp/2007/08/01/layers-defense-in-depth-part-1/>
- Figure 1.2.3: <http://image.slidesharecdn.com/intelitandsixirrefutablelawsofsecurity-120419142131-phpapp01/95/six-irrefutable-laws-of-information-security-3-728.jpg?cb=1402397663>
- Figure 1.2.4: <http://slideplayer.com/slide/5166911/>



External Resources

- Sumner, M. (2005). *Enterprise resource planning*. Upper Saddle River, N, J.: Prentice Hall.
- Leon, A. (2008). *Enterprise resource planning*. New Delhi: Tata McGraw-Hill.
- Garg, V. K., & Venkitakrishnan, N. K. (2004). *Enterprise resource planning: concepts and practice*. New Delhi: Prentice-Hall of India Private Limited.



Video Links

Topic	Link
CNSS Security Model	https://www.youtube.com/watch?v=WjtchGSsc04
Critical Characteristics	https://www.youtube.com/watch?v=j8FT9WqmuDY
The evolving CISO role	https://www.youtube.com/watch?v=T0lXtSLPfPQ



Notes:



Information Security - I

MODULE - II

User Identity and Access Management

User Identity and Access Management

Module Description

E-commerce and M-commerce plays a vital role in the present business era. To attract the customers, organisations have started an online business by providing various attractive offers like discounts on the credit/debit card purchases, cash backs for immediate payments through net banking, etc. With this, the organisations face a great challenge in securing the user identification and bank information of every customer.

This module focuses on the user's identity mechanisms and various ways how the organisation implements the access management system for different users. It describes the authentication, authorisation, availability (AAA) concepts and explains the importance of security audits to improve the security system. This module also focuses on the classification of access controls and how the centralised access controls can be designed and implemented according to the organisation policies and standards. This module also explains the importance of encryption; different key terms used to work with cryptographic techniques, various kinds of cryptographic techniques and use of hash functions. It also provides the detailed information about symmetric and asymmetric encryption mechanisms to convert the readable information into unreadable information, so that, even if the intruders grab the user's information, they cannot get the right or correct message.

At the end of this module, the students will be able to understand the authentication and authorisation techniques, which are suitable for the organisation requirements and they can also identify the need of access controls for the organisation and implement them based on the requirements.

Chapter 2.1

Access Management

Chapter 2.2

Hashing and Cryptography

Chapter Table of Contents

Chapter 2.1

Access Management

Aim.....	47
Instructional Objectives.....	47
Learning Outcomes.....	47
2.1.1 Introduction.....	48
2.1.2 Identity and Access Management Concepts.....	48
(i) Directory Services.....	49
(ii) Identity Lifecycle Management Services	51
(iii) Access Management Services	51
Self-assessment Questions.....	52
2.1.3 Access Management Services	53
(i) Authentication	53
(ii) Authorisation.....	54
(iii) Federation and Trust	55
Self-assessment Questions.....	56
2.1.4 Account Authorisation and Validation Management.....	56
Self-assessment Question	57
2.1.5 Security Auditing	58
Self-assessment Questions.....	59
2.1.6 Access Control.....	60
(i) Mandatory Access Control	60
(ii) Discretionary Access Control.....	61
(iii) Role-based Access Control	62
(iv) Rule-based Access Control	63
2.1.7 Privilege Identity Management (PIM)	64
(i) Privileged Single Sign On (SSO)	65
Self-assessment Question	65
Summary	66
Terminal Questions.....	67
Answer Keys.....	68
Activity.....	68
Case Study	69

Bibliography.....	70
e-References.....	70
External Resources	70
Video Links	71



Aim

To provide the students with the knowledge of existing identity and access control management system and their auditing methods



Instructional Objectives

After completing this chapter, you should be able to:

- Explain the concept of User identity and lifecycle management in Information Security
- Describe various Access Management Services that can be used to manage security of the information
- Illustrate the requirement of account authorisation and validation process
- Explain the requirement of security auditing
- Classify four main categories of access control model
- Describe how privilege identity management is done to protect the user account from any loss or theft of sensitive information



Learning Outcomes

At the end of this chapter, you are expected to:

- Identify what is user identity management service and its importance
- Outline various Access Management Services to maintain security while accessing the information
- Examine the logical need of account authorisation and validation
- Outline the events to be registered for audit purpose
- List the mechanism of an access control model
- Outline the special requirements for privilege identity management and how to implement PIM

2.1.1 Introduction

Authentication of users and their authorisation to the resources, protects the organisation resources from the intruders. But, if a proper access allocation system for the resources is not introduced, then there is a chance of reducing the organisation's productivity in the name of security enforcement. It is also equally important to set the access control, validate them and audit them to make necessary changes in the security policies.

The main goal of this chapter is to provide different identity management and authentication services and their implementation challenges. It also helps in understanding how both authentication and authorisation can be audited and improved.

At the end of the chapter, students can estimate the level of authentication and authorisation need of any organisation, i.e. from small scale to large scale organisations.

2.1.2 Identity and Access Management Concepts

Every organisation is increasing their business opportunities by all possible ways. Every activity of the organisation is happening online. Most of the organisations are moving towards ERP and SAP implementations in their organisation because it increases the transparency and productivity of the organisation. During this process, the users of the system need different authentications at different levels, such as mail server, file server, application server, database server, SAP, ERP, etc. Even the customer of the organisation needs different authentication and authorisations for their activities. Therefore, standardisation of identity and access management is very important. It allows the organisation to go ahead with a single authentication system for the entire process.

Identity and access management system is one of the solutions for the challenges listed above. It is an identity management system, which manages the digital identity of all the organisation participants. It also manages business process flow, security policies and security regulations required for the organisation.

As a whole I&AM is a pack of the following services:

- Directory Services
- Identity Life Cycle Management Services
- Provisioning
- Access Management Services

If all services are considered as components of the system, their interactions are as shown in figure 2.1.1

Identity management services, access management services and provisioning services interact with directory services for user credentials and their authorisation details. The provisioning services will decide the authorisation of resource such as operating system, files, application, databases and other resources.

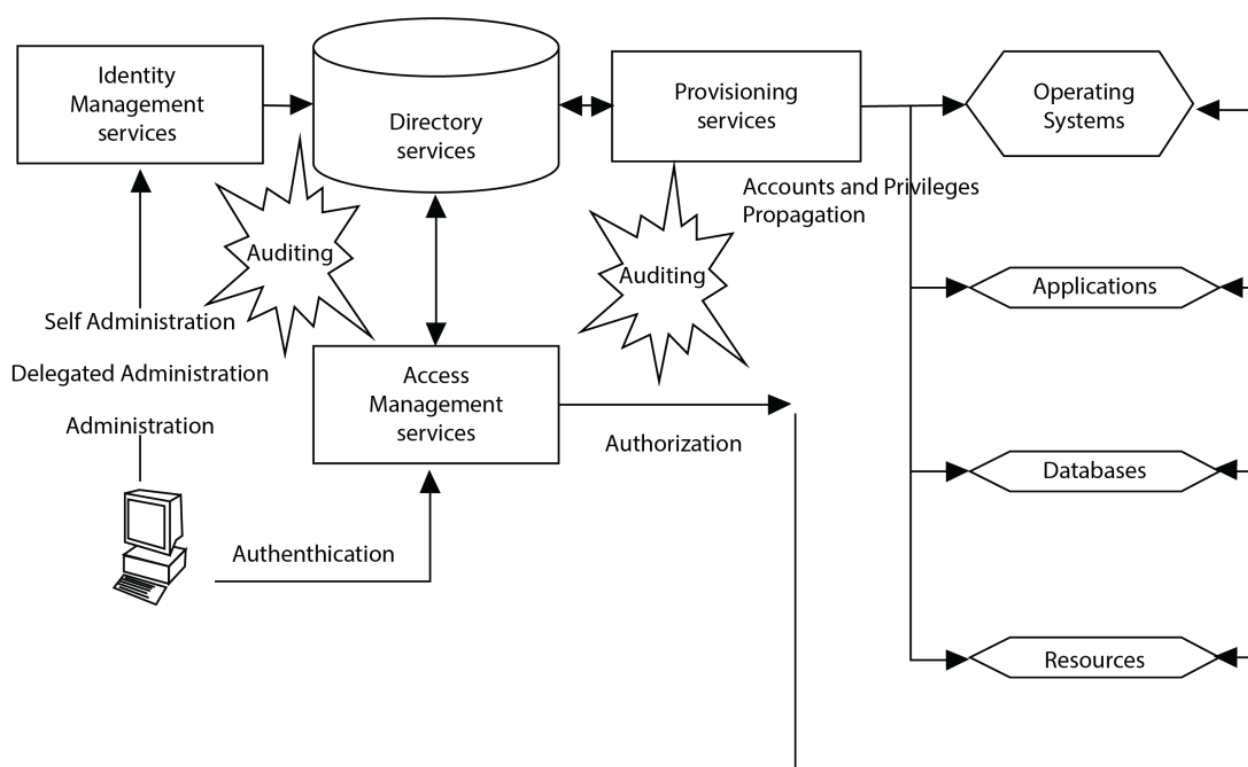


Figure 2.1.1: Identity and Access management services

(i) Directory Services

As shown in figure 2.1.1, the directory service is considered as a lookup service for user authentication details such as passwords, fingerprints, retina scans, etc. Directory services act as a core component of I & AM system, because it stores all authentication details in different formats of storage like a database, flat files, XML files and directories. Other components of I&AM system interact with the directory service by using the most reliable protocol, named as Lightweight Directory Access Protocol (LDAP).

LDAP is a directory service protocol, which runs above TCP/IP protocol. LDAP is used to search and modify directories. LDAP provides a benefit of extending directory storage and management of identity details.

Most of the organisation maintains small directories for each and every identification services. All these small heterogeneous directories are synchronised with a centralised directory named as meta directory. The main aim of meta-directory is to provide a single point authentication system for all the services of the organisation.

Meta directories use LDAP standard interface to collect authentication details from different heterogeneous data sources and synchronises with the centralised Meta directories. All the operations are illustrated in figure 2.1.2:

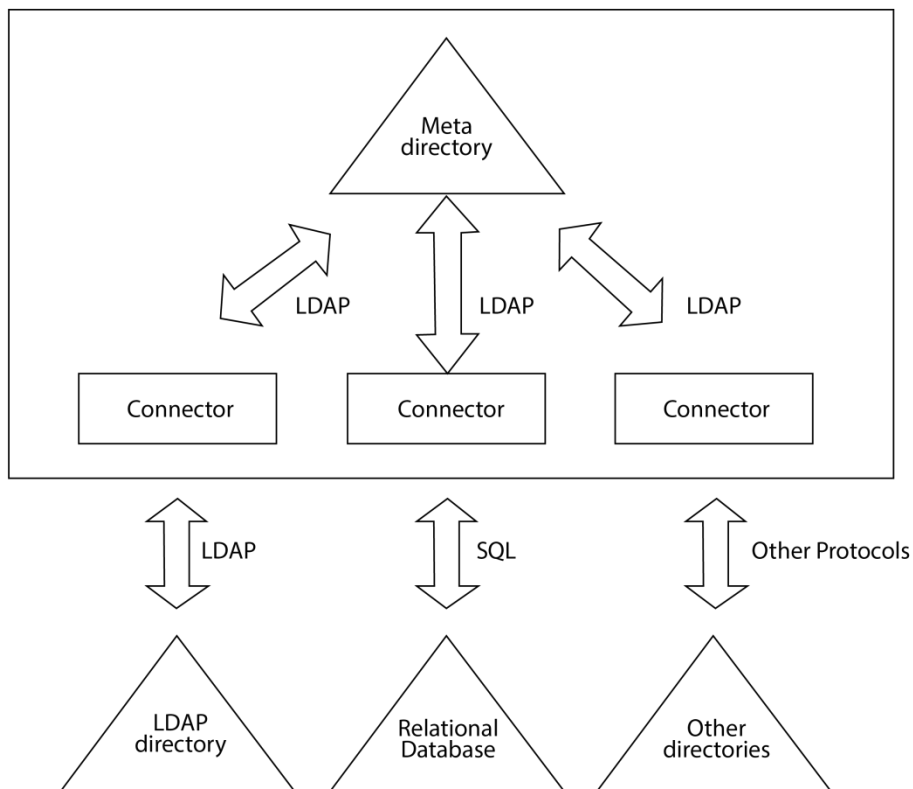


Figure 2.1.2 LDAP interface

Unification of different data sources is not so simple in the process of construction. In the process of standardisation, first a search needs to happen to identify all the heterogeneous data sources, only then a complete unified directory service can be implemented in the complete organisation.

(ii) Identity Lifecycle Management Services

Lifecycle management is a systematic process of modifying user profile, which includes their attributes, access rights, privileges and credentials based on the business requirements. This process can be done in different ways which are as follows:

- **Provisioning:** Provisioning is an automated process of modifying user account and securing the profile details. This automated process will manage user credential requirements of different applications and authorisations of the organisation. The automated process will be tuned based on the operational procedure of the organisation. Most of the provisioning applications are approval-based systems. i.e. every user creation, role creation, authentication and authorisation must be approved by the higher management.

Main operations of a provisioning application are:

- Creating user accounts
 - Assigning roles, responsibilities, authentications and authorisation's
 - Managing the credentials of all the users based on run-time requests
 - Management of approval system
- **Delegated administration:** Delegating the responsibility of user account management of a person or organisation to a third person can be named as delegated administration. In most of the organisations, third party vendors handle this process. This is most applicable to organisations, which works on a partnership basis.
 - **Self-service administration:** Administration of all user accounts by the organisation employees themselves without trusting an external agency can be considered as self-administration.

(iii) Access Management Services

Access management services are mainly for monitoring, controlling and auditing of access to resources within or outside the organisation.

The major focus of this process is on managing:

- Authentication of users
- Authorisation of resources

- Security auditing

Authentication and authorisation will be discussed in detail in section 2.1.3. Auditing is explained under section 2.1.5.



Self-assessment Questions

- 1) Which among the following services will store the user credential details of an organisation?
 - a) Directory Services
 - b) Provisioning Services
 - c) Access Management Services
 - d) Administrative Services
- 2) A service which provides one time authentication is _____.
 - a) Single Sign On
 - b) Single Sync On
 - c) Secure Single On
 - d) Secure Single Organisation
- 3) Which of the following protocol provides a communication between Meta directory and different data sources?
 - a) Lightweight Directory Accessibility Protocol
 - b) Lightweight Database Acceptance Protocol
 - c) Lightweight Directory Access Protocol
 - d) Lightweight Database Acceptance Protocol
- 4) Which of the following directory management techniques uses an automated tool?
 - a) Delegate
 - b) Self-Service
 - c) Manual
 - d) Provisioning

2.1.3 Access Management Services

Access management is a very critical process in the security system of an organisation. This focuses on managing the regular activities of an organisation, which ensures the smooth execution of security system. It also focuses on auditing of the security system based on the existing security standards available and certifies the organisation based on their security system implementation.

Overall responsibilities of access management services can be classified as:

(i) Authentication

Authentication refers to the user or entity identity verification process. Depending on the sensitivity of resources, user identities can be verified. By considering the following parameters, we can decide the security policies.

- Ease of integration
- Ease of use
- Multiple application support
- Manageability
- Cost

We can classify the authentication methods based on software and hardware.

Software authentications are:

- Username and password
- One-time password
- PINs
- Electronic passport

Hardware authentications are:

- Biometric
- Smart cards
- Hardware token

X-509 is an authorised organisation which issues and manages the digital certificates for users or organisations. X-509 certificate contains information about the identity of user or organisation to which a certificate is issued and the identity that issued it.

Most of these techniques are not completely secure. During user authentication over a network, cryptographic procedures are used for secure data transfers over networks.

Most of the organisations prefer to have a single login system for all the services of the organisation. Technically, it is known as Single Sign On (SSO). Most of the I&AM are moving towards this system. In this system, the user is authenticated once the user credentials are transported across all the systems and applications. It is very difficult to implement this system because different applications will have different user authentication systems and different storage systems. Most of the database systems available have already moved to SSO. Most of the organisations provide a helpdesk activity to resolve the access control problems, which can be resolved by using SSO.

(ii) Authorisation

Authorisation is the process of checking whether the user has permission to access the different resources available within or outside the organisation or network. Authentication is the prerequisite for authorisation. Many algorithms are available to authenticate the users and some of them are as follows:

- Discretionary Access Control
- Mandatory Access Control
- Role-based Access Control
- List-based Access Control
- Token-based Access Control
- Rule Set Based Access Control

Of all these, the Discretionary Access Control, Mandatory Access Control, Role-based Access Control are popular, remaining have a very limited importance. Complete details about access controls will be covered in section 2.1.6.

- **Discretionary Access Controls:** In this process, the administrator decides a predefined resource authentication of the users and it will be executed.
- **Mandatory Access Controls:** Predefined securities are allocated to all the resources. On a need basis, permission to the resources will be given to the users, which can be altered based on the request and approval system.
- **Role-based Access Controls:** In this mechanism, users are allocated with some roles and accesses to the resources are defined for the given roles. If the role is changed then, their access will also be changed.

- **A list based Access Control:** Every user will be provided with their authenticated resources. The list will be modified, if the user needs access to more number of resources.
- **Token-based Access Control:** Every user has to raise a token for the resources and on approval by the superiors, the resources are allocated to the users.
- **Rule set based Access Controls:** An open access control framework runs in the Linux kernel, which has predefined algorithm for authenticating and managing their authentications, based on the request.

(iii) Federation and Trust

The core portion of any access control mechanism is trust. Any algorithm will fail, if the trust fails. As the size of the organisations is growing and the employees count is growing, point of trust is very difficult to manage; hence we go through a systematic process. An agreement of trust can be used to establish a secure communication between different organisations. This process is being used today to gain the business. Most of the third party vendors are allowed into the system for a specific task from the overall task of the organisation. Some organisations prefer to use the trust as a factor for sharing the resources.



Self-assessment Questions

- 5) Which among the following is a hardware authentication tool?
- a) Username and password
 - b) Personal Identification Numbers
 - c) One Time Passwords
 - d) Biometric Machines
- 6) In which of the following access control methods, authentication is done based on the resource?
- a) Discretionary Access Control
 - b) Mandatory Access Control
 - c) Role Based Access Control
 - d) Rule Based Access Control
- 7) ACL is an implementation which is controlled by ____.
- a) Discretionary Access Control
 - b) Mandatory Access Control
 - c) Role Based Access Control
 - d) Rule Based Access Control
- 8) Which of the following access controls assigns the authentication based on the responsibilities of the employee of the organisation?
- a) Discretionary Access Control
 - b) Mandatory Access Control
 - c) Role Based Access Control
 - d) Rule Based Access Control

2.1.4 Account Authorisation and Validation Management

Authorisation is one of the organisation security level aspects, which follows with authentication.

Every organisation must carry out authorisation process for each and every individual to perform the specific type of actions. Authorisation is the logical access of organisational data with access control rights and organisation policies. Authorisation enforces each person to do actions based on their limit of access. This limit of access to the resources is listed in a document file which can be called as Access Control List (ACL). This list becomes the base for the organisational validation process. All the users of the organisation are validated based on this list.

For example, if the user is having the authorisation only to read the information, then the user can only read the information and cannot perform the write or update operation. When the same user, though they do not have the permission to write, then to implement the

writing operation, the validation of ACL happens and informs the user about the rights of the user and the same to be loaded in log register for auditing purpose.

Every user must know what kind of the components, resources, data and services he/she is eligible to access, based on that user action are decided. Every user must read the organisation policies which include standards about the authentication, authorisation and actions to be taken for the violations of them.

Like authentication, authorisation is also a continuous process in the organisation. The authorisation controls need to be updated, based on the role changes of the user within the organisation.

Policies of organisation forces to use the dual authorisation mode, i.e. every operation performed by the user are approved by another user. For external users, this entire transaction appears as a single transaction. This kind of approval system creates an extremely powerful authentication system. However, it is very difficult to implement the two levels of approvals for emergency activities due to the time-consuming process.

After successful implementation of authorisation process, then frequently audit log should be checked for violations. The validation should be done for every user activity to verify whether the user is accessing the services or data according to the access control rights given to them.



Self-assessment Question

- 9) Restriction on the organisational resources by the user is known as ____.
- | | |
|-------------------|------------------|
| a) Authentication | b) Authorisation |
| c) Availability | d) Integrity |

2.1.5 Security Auditing

Auditing is nothing more than a verification of process execution based on the decided standards. Every organisation creates various security policies to run their organisational activities.

An organisation's security policy guides about:

- How to build the security system.
- Security elements identification, to provide tight security based on the organisational requirements.
- Provides the details regarding the creation of access control list (ACL) to the users and decides their accessibilities to the resources.

Once the organisation establishes the security system, it must perform the security audits frequently to ensure the standard.

A security audit is a systematic evaluation process for measuring the strength of security policies and the security system of an organisation based on existing security standards like ISO-27000 and NIST. To perform the audits, the organisation must implement the centralised log system for every user. Security auditors perform the auditing by conducting interviews, collecting the data from the users, operating system settings, examine the security policies, various security checking points and network architecture. After the Security audit, finally the audit team provides a detailed certificate to the organisation about the audit visit and immediate actions need to be taken for the identified errors. Every organisation must perform the internal audits to enhance the quality parameters using internal auditors.

An organisation must provide the required resources to the auditor for auditing purpose. Audit or performing the Security audit can be done in three steps:

- Open meeting with auditee (organisation).
- Suitable audit procedure documentation against the selected reference model.
- In-depth examination of the implemented system for increasing the quality aspect.

Many of the events of the organisation are verified during the security audit. Below listed events are few:

- What is the current state of the security system and how it is working?
- Whether users are accessing the information according to the ACL?

- Whether the access log is recording the type of user and type of access and it is reviewed?
- Whether the operating system and business applications are up-to-date?
- Have the basic applications built by considering the future security?
- Whether all the cryptographic techniques are working fine to encrypt the data?
- Whether any disaster recovery plans are present in the organisation?
- Is there any procedure for backup? Whether it is up-to-date?
- Whether the business applications are tested for bugs?

It is always advisable to conduct internal and external audit periodically and verify the stability of the system. It is even recommended to get certified for the audit.



Self-assessment Questions

- 10) A security audit compares the actual results with ____.
- | | |
|---------------------------------|--------------|
| a) Expected results | b) Audit log |
| c) Specified security standards | d) ACL |
- 11) For the security audit, _____ should provide the resources to accompany.
- | | |
|---------------------|------------|
| a) Internal auditor | b) Auditor |
| c) Clients | d) Auditee |

2.1.6 Access Control

An access control is a process of defining the relationship between authorisation of users and the resources of the organisation. All the access control mechanisms majorly focus on the below mentioned few points:

- Easy to authenticate users with resources
- Minimum time in modifying the authentications
- Confidentiality and integrity of the system must be assured
- Intruder of the system should not access any resources
- Easy management of audit information

There are three major access control mechanisms they are as under:

- Mandatory access control
- Discretionary access control
- Role based access control

Remaining access control mechanisms like Rule based access control are used very insignificantly.

(i) Mandatory Access Control

Execution of the Mandatory Access Control (MAC) is a very simple strategy.

All the resources of the organisation are classified into different authentication levels based on their sensitivity, protection requirements and confidentiality.

For example, let printer is one resource and 'X', 'Y' be the users of the organisation. In the clearance or an authorisation list of the printer, if only 'X' is included, then 'X' can use the printer, whereas 'Y' cannot use it, since 'Y' is not included in the list.

All the users will be provided with a clearance, based on their responsibilities, i.e. all the users are authorised to access all the resources, which have fewer authentications than their authentication level.

If the user's responsibilities are changed, then their clearance list will also change. It is very easy for managing the clearance of all the users by using the directory services.

It is very difficult to alter a clearance list by intruders. The user can make changes to only those resources that they are eligible to change.

The disadvantage of this approach is that it is very restrictive. As the administrator alone needs to modify the list of clearances, until he does that, the user cannot access the resource. Most of the MAC approaches are coupled with approval system, which further increases the delay.

(ii) Discretionary Access Control

Execution of the Discretionary Access Control (DAC) is quite simple. To explain the DAC, we can use Lampson's Matrix.

This matrix is a table which provides the mapping between the users and resources. The first column of this matrix has all usernames and the first row has all the resources available, as shown in the table 2.1.1.

Table 2.1.1: Example for Lampon's Matrix of a simple organisation

	Database Server	Application Server	Printer	Internet	File Server
Mr. X	Allowed to Read	Allowed	Allowed	Allowed	Only read
Mr. Y	Allowed to Read & write	Allowed	Not Allowed	Not Allowed	Read and write
Ms. Z	Allowed to Read	Allowed	Not Allowed	Allowed	Only read

All the entries of the table, except the first row and first column show their user authorisation details.

The administrator of the organisation, who is considered as owner of resources will authenticate all the users. Whenever any user needs to access any new resources, then the dedicated list is verified and an allotment is made.

Access Control List is the best *example* of this approach.

The biggest disadvantage of this approach is that, every resource for the user authentication must be decided well in advance, which is very difficult for any organisation because, for most of the organisations, this is very dynamic.

If an intruder modifies this list, he can access any resource of the organisation. Hence, it must be extremely protected.

If the list and resources of the organisation increase the size of the authentication list at one point, it becomes unmanageable.

Partial allocation of the resource is not possible with this approach.

(iii) Role-based Access Control

In this method, a new system is introduced called roles. Roles are created and all the users are allotted to different roles. Resources are authenticated based on the roles, rather than users. If the user roles are changed, then their resource authentication will also change.

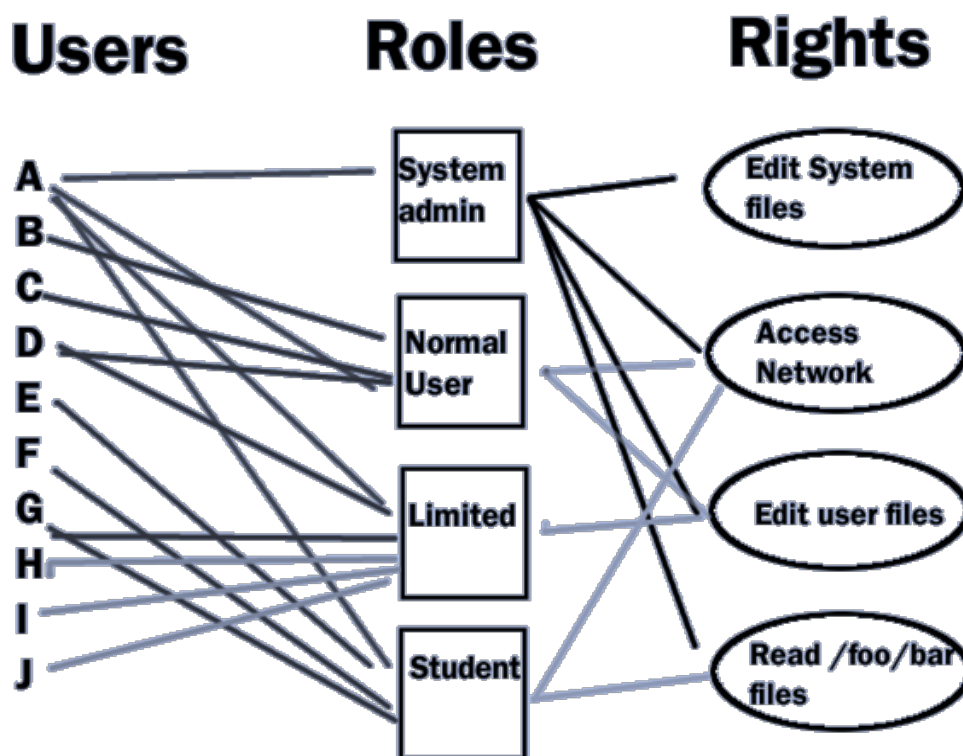


Figure 2.1.3: Example of Role based Access Control

From the figure 2.1.3, all the users from A to J are divided into different roles like admin, normal user, limited and student. These roles have been given authorisation to the files and

network. If any new user joins the system, then he must be allotted to the concern roles, because roles has been already allotted with authorisation for resources.

As the roles are hierarchical, child roles will inherit the basic role responsibilities of their parents, hence they also inherit the resource authentications. System administrator's productivity can be increased by review and revocation of permissions.

RBAC family constitutes four conceptual models:

- RBAC0 just groups the user based on the roles and authenticates the resources based on the roles;
- RBAC1 includes role hierarchy to RBAC0;
- RBAC2 adds dynamic constraints to RBAC0;
- RBAC3 includes all aspects of RBAC1 and RBAC2.

In DAC if any new resources are brought into the system, then all the concern user lists must be modified. Even in MAC, the resource clear list must include all the user names. Whereas, in case of RBAC, allotting the resource to the role is sufficient.

RBAC makes a very few changes in the organisation's database, when any new resource or users are brought into the system. Whereas, DAC and MAC will have a huge number of changes in database with dynamic changes of the organisation.

(iv) Rule-based Access Control

The business change will trigger the access change. If business demands new rules, then based on that the access controls are modified.

Most of the business needs expects the users to have a new resources allocated to them to fill the business requirements. The user can be part of any role, if access control is given to complete role, then all the members of the role can access them, which is not feasible for the security system. To avoid this process, a rule is created based on the business needs and allotments are made according to that.

Most of the rule based systems are coupled with role based system. In case of any special requests, few members of the system will be given access based on the new rule generated.

Implementations of the access control are feasible only if business changes are very minimum.



Self-assessment Questions

- 12) In Lampson's Matrix, first row is considered as ____.
- a) All the users
 - b) All the resources
 - c) All the access rights
 - d) All the authentication levels
- 13) Which of the following are hierarchical?
- a) Access rights
 - b) Authentication
 - c) Resources of the organisation
 - d) Roles of the organisation
- 14) Among the entire Role Based Conceptual model, which one of them focuses on the Role hierarchy?
- a) RBCM0
 - b) RBCM1
 - c) RBCM2
 - d) RBCM3

2.1.7 Privilege Identity Management (PIM)

In most of the organisations, super account management is very difficult and it is almost unmanageable.

Many of the super users of organisations like CIO, CEO, have limited training on its resource utilisation and authorisation. Giving the complete access rights to them may lead to misuse of the system. This misuse of authorisation can lead to loss or theft of data, sensitive information or may introduce malware into the system.

Risks of unmanaged PIMS:

- Intruders majorly focus on the privileged account which is not used for a long duration to intrude the system.
- In most of the cases of organisation, sensitive data thefts are through privileged user accounts.
- As the super user account has higher privileges, attacking the super user account gives a provision for compromising the network and opens vulnerabilities in the system.

Care to be taken in the implementation of PIM:

- An organisation must create and implement security policy which explains a procedure to be followed in the creation and managing of super user accounts.
- Do's and Don'ts of the super user account must be created, distributed and trained.
- Make use of special tools available for PIM such as provisioning tools.

(i) Privileged Single Sign On (SSO)

Most of the organisations are moving to the single sign-on system to avoid multiple passwords for multiple systems. Single sign-on will provide a comfortable environment for remembering a single password to access all the systems, but it includes a security glitch for a privileged account. If any intruder attacks the system through the SSO password, he can login to all the applications of the system and create damage to the system so to avoid this most of PIM use different SSO systems, which work, based on Multiple Factor Authentication (MFA) or 2 Factor Authentication (2FA).

In 2FA, users need at least two authentication procedures, to get access to the system. **For example**, internet banking with username, password and OTP.

In this MFA, use of two or more authentication procedures are needed to access the required system. **For example**, net banking applications use the username, password along with one time passwords and transaction passwords to complete the transaction.

Single sign on system binded with token system is much advisable for protecting the system. In this system, as soon as the privileged user accesses the system with his user name and password, the system administrator will get a notification. After the confirmation, the administrator will issue a token to go ahead.

Single sign on system for a privileged user is very much helpful, but a high degree of protection needs to be employed to prevent the misuses.



Self-assessment Question

15) For an intruder, which of the following accounts are most appropriate to compromise the network?

- | | |
|--------------------------------|----------------------------|
| a) Customer account | b) Normal employee account |
| c) Privileged employee account | d) Intruder account |



Summary

- Identification and access management is a systematic process of identifying the user by providing the authentication and authorise them to the resources.
- LDAP is a protocol used as an interface between different data sources with a centralised storage system called Meta directory.
- Identity life cycle management services focus on how user authentications are created and managed. It can be done by using provisioning tools, delegation approach or self-management.
- Access management services focus on managing the authentication, authorisation and audit of the security systems designed within the organisations.
- Access management services identifies the need of security, type of authentication suits for organisation needs, which algorithm to be used to assign user authorisations to resources and which information needs to be recorded for the security audit.
- Federation and trust is an important attribute on which sharing of resources between the organisation rely on.
- Account authorisation and validation management majorly focus on how user accounts are authorised to perform the specific tasks or operations if there is any authorisation violations and what are the actions to be taken on the people.
- An organisation must perform the security audits to know the performance of their organisation security system.
- An organisation must provide the resources needed to perform the audits like people, policies and standards, details about the security components, etc.
- Access controls are the different approaches available for assigning authorisations to resources with the users.
- Discretionary access controls: where the owner will decide the authorisations
- Mandatory access controls: where resources are assigned on authorisation level and users are provided with clearance to them.

- Role-based access controls: users are grouped by roles and roles are authorised.
- To access and misuse the organisation information, the main source for the attackers is the unused user accounts and the top-level management accounts.
- Privileged user authentication management needs to be much stronger than the regular user account.



Terminal Questions

1. Describe the concept of User identity and lifecycle management in Information Security.
2. What are the various Access Management Services that can be used to manage security of the information?
3. Explain the logical need of account authorisation and validation.
4. Explain the requirement of security auditing.
5. Describe the four main categories of access control model.



Answer Keys

Self-assessment Questions	
Question No.	Answer
1	a
2	a
3	c
4	d
5	d
6	b
7	a
8	c
9	b
10	c
11	d
12	b
13	d
14	b
15	c



Activity

Activity Type: Offline

Duration: 30 minutes

Description:

Identity and access management (I&AM) solution has to securely support more and more users (partners, employees, customers) and many types of sensitive applications in changing the technical environments. Discuss.

Case Study

Myfootware Corporation is a new company started very recently. It was a footwear manufacturing industry. It has a lot of wings in their organisation, which are as follows

- Design section: where the designers are occupied and it is a very confidential area because it has designs, which cannot be disclosed. Only designers can access and modify the file server meant for design files but no access to the production server.
- Manufacturing section: where manufacturing happens most of the employees working here are illiterates and it includes contract employees. They can read the content of the design file server to manufacture the footwear, but they can modify production server content.
- Logistic and dispatch section: where most of the external people will be entering to collect their stock. They should not have any access to file server, but needs an access to the production server.
- Management section: where all the official transaction does happen and all confidential documents do exist here. They have full access to the document server, but have read access to design and production servers.

By considering above criteria's answer the following questions:

1. Create a mandatory access control list for all the sections.
2. Suggest the access control method to be followed by all the sections.
3. Suggest the measures to be taken for implementing single sign on for all the sections.
4. Management section does not have permission to write at production and design servers. Do you think is it a wise policy if not suggest and justify your policy.

Bibliography



e-References

- *Access Control*. Retrieved 5 Jan, 2017 from http://liris.cnrs.fr/romuald.thion/file/s/RT_Papers/Thion07%3ACyber%3AAccess.pdf
- *Privilege Identity Management*. Retrieved 5 Jan, 2017 from http://www.ibm.com/support/knowledgecenter/SSRQBP_1.0.1.1/com.ibm.ispim.doc_1.0.1.1/Pim_Guide/cpt/pim_oview.html
- *Security Auditing*. Retrieved 5 Jan, 2017 from <http://searchsecurity.techtarget.com/IT-security-auditing-Best-practices-for-conducting-audits>

Image Credits

- Figure 2.1.1: <https://www.sans.org/reading-room/whitepapers/services/identity-access-management-solution-1640>
- Figure 2.1.2: <https://www.sans.org/reading-room/whitepapers/services/identity-access-management-solution-1640>
- Figure 2.1.3: http://lh4.ggpht.com/_0hUssIIWt_o/Syl2TpMYHRI/AAAAAAAAAAU/X872p5_OlsY/s1600/Role%20Based%20Access%20Control%20In%20Action.png



External Resources

- Whitman, M. E., & Mattord, H. J. (2009). *Principles of information security*. Boston, MA: Thomson Course Technology.
- Stallings, W. (2003). *Network security essentials: applications and standards*. Upper Saddle River, NJ: Pearson Education.
- Peltier, T. R., Peltier, J., & Blackley, J. A. (2005). *Information security fundamentals*. Boca Raton, FL: Auerbach Publications.



Video Links

Topic	Link
Access Control	https://www.youtube.com/watch?v=SE5KFDPh8-M
Privilege Identity Management	https://www.youtube.com/watch?v=dFY77_fR6NU&list=PL1Wa7oNYE2s6vcSi6jGJvrgR5LOBdokTp
Audits and Risks	https://www.youtube.com/watch?v=WgupVAiaV-Y



Notes:



Chapter Table of Contents

Chapter 2.2

Hashing and Cryptography

Aim.....	73
Instructional Objectives.....	73
Learning Outcomes.....	73
2.2.1 Introduction.....	75
2.2.2 Basic Concepts of Cryptography and Network Security.....	75
Self-assessment Questions.....	77
2.2.3 Encryption and Decryption	77
(i) Types of Encryption and Decryption Techniques	80
(ii) Process of Encryption and Decryption Techniques	84
(iii) Applications of Encryption and Decryption	89
Self-assessment Questions.....	90
2.2.4 Applications of Cryptographic Hash Function	90
(i) Message Authentication	91
(ii) Digital Signature.....	93
(iii) Other Applications	94
Self-assessment Questions.....	95
2.2.5 Requirements and Security	95
(i) Security Requirements for Cryptographic Hash Functions.....	96
(ii) Brute-force attacks	96
(iii) Cryptanalysis	97
Self-assessment Questions.....	97
2.2.6 Hash Function Based on Cipher Block Chaining	98
Self-assessment Questions.....	100
2.2.7 Secure Hash Algorithm (SHA).....	100
Self-assessment Questions.....	105
Summary	106
Terminal Questions.....	107
Answer Keys.....	108
Activity.....	109
Case Study	110

Bibliography.....	111
e-References.....	111
External Resources	112
Video Links	113



Aim

To provide the students with the knowledge of hashing and Cryptography in Information Security



Instructional Objectives

After completing this chapter, you should be able to:

- Define the terminology used for basic encryption and decryption
- Elaborate the process of encryption and decryption with its working, mechanism and its applications
- Elaborate the application of cryptographic hash functions
- Explain why a hash function used for message authentication needs to be secured
- Elaborate attacks on hash function
- Describe how cipher block chaining can be used to construct a hash function
- Analyse the operation of SHA-512 algorithm with respect to its working mechanism



Learning Outcomes

At the end of this chapter, you are expected to:

- State various terminologies and background of encryption and decryption
- Differentiate between symmetric-key encryption technique and asymmetric key encryption technique
- Simulate the process of Encryption and decryption techniques
- Identify the need and use of encryption and decryption
- Outline the application of cryptographic hash functions
- Identify why a hash function used for message authentication needs to be secured
- Identify the different attacks on hash functions

- Summarise how cipher block chaining can be used to construct a hash function
- Compute SHA-512 logic for a specific scenario

2.2.1 Introduction

With the proliferation of internet into every possible human activity, the information that is being exchanged between the systems increase exponentially. This necessitates that the users and the initiators of this information understand the importance of information security. The aim of information security is to prevent unauthorised intrusion into the system and protect the data integrity. Information security also lays down protocols that will ensure that the data is not accessible nor is it understood by an intruder. Information Security also defines a process that would authenticate the source of the data/information and verify the sender of the same.

The issues listed above are covered in this chapter. Student will learn about encryption and decryption, which will hide the original message from the intruders. Student will also be covering the concept of hashing, which will authenticate the message transmitted over the internet.

At the end of this chapter, students will be able to understand the importance of the encryption and decryption for hiding the message and hashing for authenticating the transmitted message.

2.2.2 Basic Concepts of Cryptography and Network Security

Due to advancement in the internet, there is an inherent threat for every organisational data or information. It must be protected from unauthorised persons or intruders. Most of the organisations are following various techniques to provide the security for their information like using the access control mechanism for different users, deploying the various software's at different places like firewalls, IDPS, honey pots, honey nets etc. Despite of tight security measures, several organisations are still struggling to protect their data.

Despite tough security measures, if the information gets hacked, ensuring that the information is in a format which cannot be understood by the hacker. So, the concept of cryptography was introduced, which converts the input text into a meaningless format.

Organisations are now using the cryptography concepts for securing their information.

Cryptography is the combination of two Greek words Krypto, means "hidden," and graphene, means "to write," i.e. converting the readable information to unreadable information or hiding the meaning of information by converting one format to another.

There are five primary functions of cryptography today they are:

- **Privacy/confidentiality:** It refers to that only the correct users should get the message content.
- **Authentication:** It is the process of identifying the person.
- **Integrity:** Integrity means there are no changes in the received message. It is same as the original message.
- **Non-repudiation:** It is the assurance that someone cannot deny or change the original message.
- **Key exchange:** It is the mechanism to share the keys between sender and receiver.

The terminology used for cryptosystems are:

- **Algorithm:**
A step-by-step procedure for solving the given problem.
- **Plain text:**
The original message created by the sender is known as the plain text. It is in the readable format.
- **Cipher text:**
The encrypted data, which is received by the receiver. The Cipher text is the scrambled format of the plaintext. This is very difficult to read.
- **Encryption algorithm:**
A procedure used by the sender for converting the plain (readable) text to cipher (unreadable) text. The inputs for this algorithm is plain text and encryption key and output is the cipher text.
- **Decryption algorithm:**
An algorithm used by the receiver to convert the data from cipher text to plain text.
- **Encryption key:**
It is the key used by the sender to convert the plain text to cipher text along with the encryption algorithm.
- **Decryption key:**
This is the key used by the receiver along with the decryption algorithm to receive the original information from a cipher text.
- **Key space:**
The value range used to create the keys is known as the key space.
- **Steganography:**
Hiding the information in one file inside another file is known as steganography.



Self-assessment Questions

- 1) Which of the following is the process of converting the cipher text to plain text?
 - a) Encryption
 - b) Decryption
 - c) Hash
 - d) Substitution
- 2) Which of the following is the technique to hide the information?
 - a) DES
 - b) Steganography
 - c) RSA
 - d) Key Space

2.2.3 Encryption and Decryption

In the encryption and decryption process (sequence shown in the figure 2.2.1), the sender encrypts the message using a key and transmits the cipher text or encrypted document to the recipient, who can retrieve the plain text by using the decryption key.

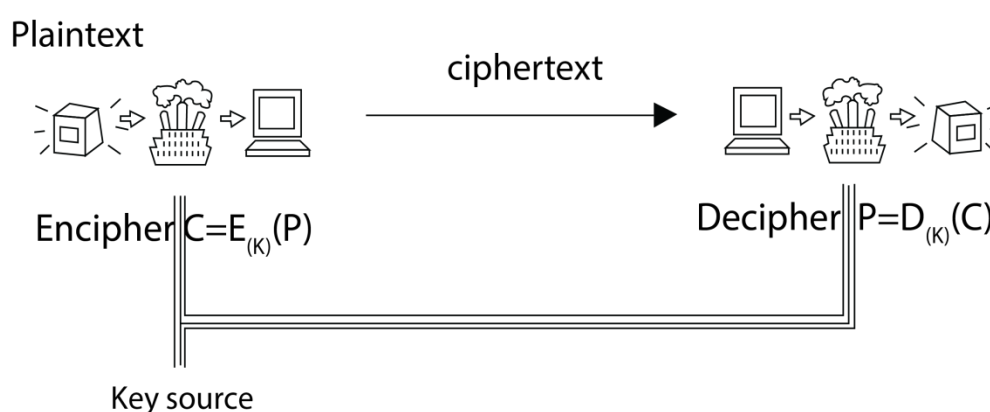


Figure 2.2.1. Encryption and Decryption

In the above diagram:

- To convert the plain text to cipher text, the encryption equation $C=E(K)(P)$ is used, where C =Cipher text, $E(K)$ =Encryption Key and P =Plain text.
- To convert the cipher text to plain text, the Decryption equation $P=D(K)(C)$ is used, where C =Cipher text, $D(K)$ =Decryption Key and P =Plain text.

Let us take a simple **example**

Consider the plain text is 123456 and the encryption algorithm adds 3 to each digit and decryption algorithm subtracts 3 from each digit. What would be the resultant cipher text?

Plain text(P) =123456

Key(k)=3

Encryption Algorithm: Add (3) to each digit for encryption

1+3 2+3 3+3 4+3 5+3 6+3

4 5 6 7 8 9

So Cipher text(C)= 456789

Decryption

4-3 5-3 6-3 7-3 8-3 9-3

1 2 3 4 5 6

Here Decryption Algorithm: subtract (3) from each digit of cipher text

So Plain text(P)=123456

Cryptographic systems can be classified using three components:

1. **Sequence and type of operation used for generating the cipher text:**

All cryptographic techniques are designed using either transposition or substitution methods. Transposition method is used for rearranging the entire terms in the message. Whereas, substitution method is used to substitute one word, line or character with the other.

Substitution Cipher:

In the substitution cipher method, one character in the plain text is replaced with the other character or by symbols or numbers.

It is more powerful if we repeat the same procedure again and again to generate the cipher text, i.e. Output of first operation becomes the input for second operation. Consider the following method:

Plain Text: a b c d e f g h i j k l m n o p q r s t u v w x y z

In the case of substitution method shown above, every character is substituted with its 4th character from the right hand side.

For example,

If the input text is 'information', then by using the above method, the cipher text would be:

MRJSVQEXMSR.

Transposition Cipher:

The transposition cipher rearranges the character position in the plain text to get the cipher text. This is also very easy technique when compared to the substitution cipher, which is difficult to decipher the cipher text.

Consider the following key positions: 1->6, 2->3, 3->1, 4->5, 5->2, 6->4 using this convert the plain text to cipher text

Input (plain text): SAVE-THE-EARTH-IT-WILL-SAVE-YOU.

Divide the input into 6 letter blocks

Key positions decided

Table 2.2.1: key positions

Present Position	Transposition
1	6
2	3
3	1
4	5
5	2
6	4

Then the input becomes:

Table 2.2.2: working of transposition

6 5 4 3 2 1	6 5 4 3 2 1	6 5 4 3 2 1	6 5 4 3 2 1	6 5 4 3 2 1	1
S A V E - T	H E - E A R	T H - I T -	W I L L - S	A V E - Y O	U
T V S - A E	R - H A E E	- - T T H I	S L W - I L	O E A Y V -	U

Give the numbering for each block from right to left and change the position according to the key positions by using table 2.2.1. The final result of each block would be as shown in table 2.2.2

Cipher text: TVS-AER-HAEE--TTHISLW-ILOEAYV-U

2. Number of Keys used:

The cryptographic algorithms can be classified based on the number of keys used. Based on the number of keys used, we can classify the cryptographic algorithms as symmetric key and asymmetric key. In the symmetric key technique for encryption and decryption, the same key will be used and it is known as a private key.

In asymmetric key technique two keys are used for encryption and decryption - one is a private key and other is a public key.

3. Plain Text processing:

Cryptographic algorithm can also be classified based on the Plain text processing. In this, the classification is based on how the encryption algorithm processes the plain text (whether as a character or word or block).

(i) Types of Encryption and Decryption Techniques

Based on the number of keys used by encryption and decryption algorithms, they can be divided into two types. Algorithm with same key for encryption and decryption and different keys for encryption and decryption.

Symmetric key encryption: It is also known as private key encryption. In the symmetric key encryption process, both sender and receiver use the same key for encryption and decryption. The key used in this encryption is known as private key or secret key. There are several algorithms that are working by using this concept like DES, AES, Triple DES.

Figure 2.2.2 illustrates symmetric encryption working process

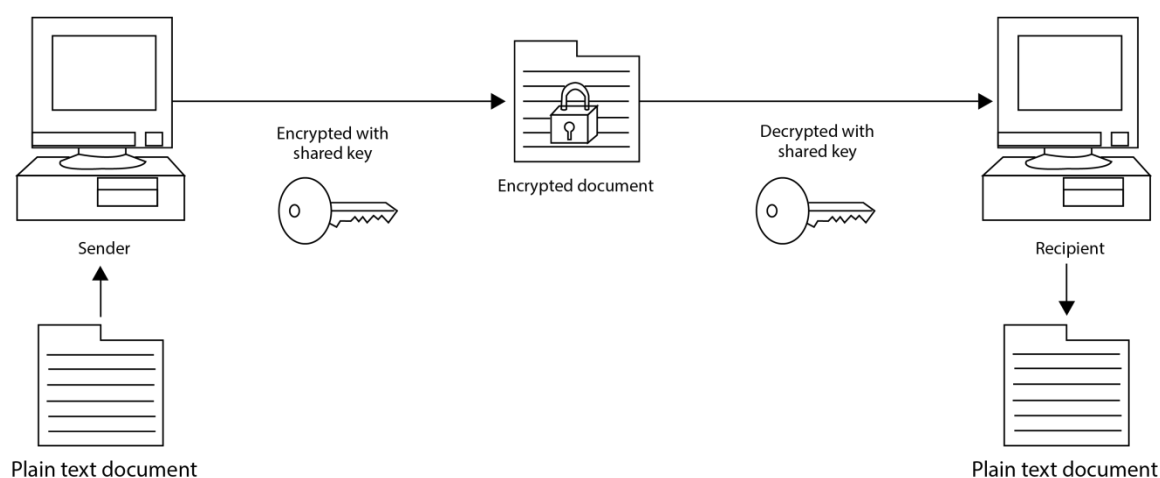


Figure 2.2.2: Symmetric encryption process

In symmetric encryption, first the sender converts the plain text or original message to the cipher text or encrypted text using the private key or a secret key or shared key by using an encryption algorithm. Then, the sender sends the encrypted document to the receiver. At the receiver end, the receiver collects the encrypted document and decrypts it using the same key which the sender used, using a decryption algorithm to get the plain text from cipher text.

The following are the precautionary steps to be taken to build strong symmetric key encryption process:

- The shared key should be sent secretly, securely and to be shared prior to the encryption process.
- As the same key used by the parties it is recommended to change the key frequently.
- The strong security system should be identified and built to share the keys between the parties, otherwise there is a chance that the intruder may grab it.

Challenges:

Challenges with symmetric key are listed below:

- **Key creation:**
Generation of the key is an important concept in the symmetric key encryption process. There should be a mutual understanding between the parties to create the key, which should be transmitted to the other before the encryption process.

- **Trust:**

Trust plays an important role in the symmetric key encryption algorithm because there is a chance that either sender or receiver might lose their key unintentionally, in the worst case if an eavesdropper finds the same key, then definitely he/she can get the message content.

Example of symmetric encryption algorithm: Data Encryption Standard (DES), triple DES, Advanced Encryption Standard (AES), etc.

**Advantages:**

- It is simple and widely used technique.
- Much faster in their execution.
- Since the key is not distributed along the text, the chance of decrypting the data is very less.

**Disadvantages:**

- Secret key sharing between the parties is cumbersome.
- Authenticity of the message cannot be assured.

Asymmetric Encryption Algorithm:

It is also known as public key encryption. Unlike symmetric algorithm, the asymmetric key algorithm uses two keys - private key and public key. Private keys are known only to the respective users, whereas the public key is known to everyone in the group or a communication process. In this algorithm, a combination of private and public key is used.

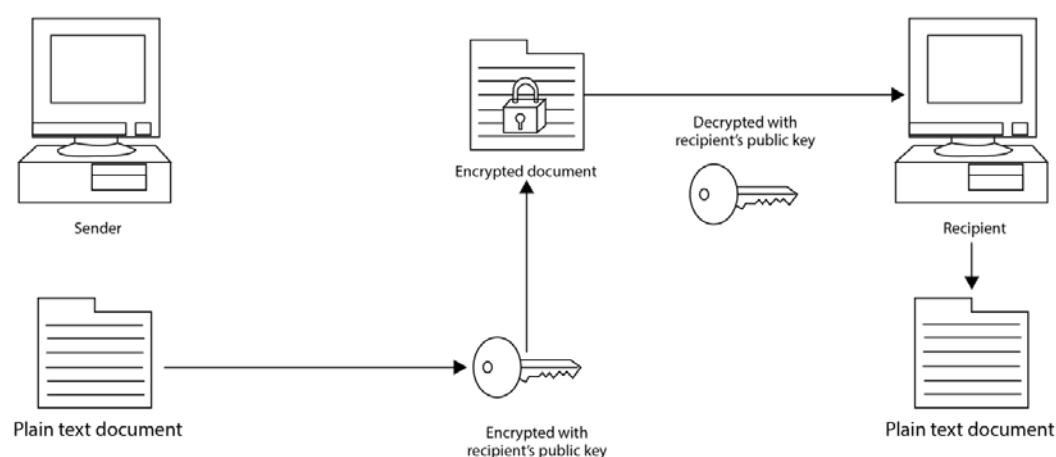


Figure 2.2.3: Asymmetric key encryption process

As shown in the figure 2.2.3, the sender encrypts the plain text using the public key of the receiver. The encrypted document is transferred to the recipient. To get the original message at the receiver side, the receiver uses the private key of their own to decrypt the message.

Salient features of the asymmetric encryption are:

- For each user, two dissimilar keys are assigned, one is private key which is only known to the user and a public key which is known to everyone in the group and going to a common place which is known as a public key repository. Using this, anyone can gain the public key of others.
- The two keys are calculated using some mathematical equations and some relation exists between the private and public keys of the same party.
- The keys are interrelated. It is impossible to calculate the private key of a person using public key, which is available publicly.
- For the entire encryption and decryption process, a same set of keys should be used, i.e. either two keys of the sender or receiver, i.e. if the message is encrypted using a sender private key, then the public key of the sender should be used to decrypt or if the sender uses receiver public key for encryption, then receiver private key should be used for decryption.
- As the key length is large, the processing time is high as compared to the symmetric key encryption process.

Challenges:

One of the biggest challenges with an asymmetric encryption is: if the sender is using the public key of the receiver and if that is changed or replaced with other third party key, then the message is going to reach to the intruder. So a solution to this is to use the Public Key Infrastructure (PKI), which is a third party tool to maintain public keys securely.

Example of asymmetric encryption algorithm: RSA, Diffie - Hellmen

**Advantages:**

- No key distribution is needed.
- Private key assures the authenticity of the message.

**Disadvantages:**

- It is slow in their execution
- Uses more computer resources.
- Loss of private key causes unwanted overhead.

But today most of the persons are using a combination of both symmetric and asymmetric keys, which is known as hybrid techniques.

(ii) Process of Encryption and Decryption Techniques

The process of encryption and decryption has four major components such as:

1. Plain text
1. Cipher text
2. Secret key and public key
3. Algorithm

Various algorithms which come under symmetric encryption and asymmetric encryption techniques are described as below:-

Symmetric encryption algorithms:

DES Algorithm:

DES algorithm is used for encryption of plain text and decryption of a cipher text. DES algorithm has following properties they are:

- **Plain Text:** The overall message is divided into 64 bit blocks. If any block does not have sufficient text, then extra bits are padded at the end of the plain text. Each block is processed individually by the DES Algorithm
- **Cipher Text:** Each block of 64 bit plain text is converted into 64 bit cipher text.
- **Initial and final Permutation:** This phase exchange different bit positions of the text with other bit positions
- **Round Key Generator:** Round Key Generator will accept 56 bit key and produces 16 keys by exchanging the positions of 56 bits of initial key. Each key generated will be of 48 bit length.
- **Round 1 to 16:** Each round accepts input from the previous round or initial permutation and performs the XOR operation with the corresponding key.

Encryption Algorithm:

DES Encryption Algorithm execution is as shown in figure 2.2.4

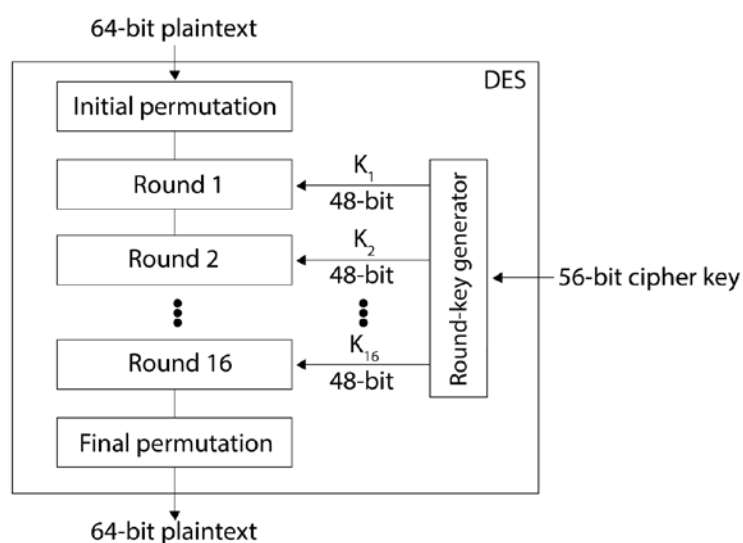


Figure 2.2.4: DES algorithm

Plain text is submitted for Initial permutation, which produces the result by swapping different bit positions and is submitted to round 1.

Key generation module produces 16 keys from initial key.

While (round number is less than 16)

{

Split text to Left_{round number} (32 bits) and Right_{round number} (32 bits)

Left_{round number} and Right_{round number} are submitted to mixer module.

Output of mixer module is submitted to swapper module which swaps left part with the right part

Output of swapper module is submitted to the next round

}

Output of round 16 is submitted to final permutation, which swaps the bit positions and produces cipher text

Decryption Algorithm

Decryption algorithm works in reverse order of Encryption Algorithm, i.e. Cipher text is submitted to final permutation.

Then it completes all the rounds from round 16 to round 1 and submits the result of round 1 to initial permutation, which produces the plain text.

AES Algorithm

DES was invented before 30 years. It faces a lot of security threats because the key length is very small. Hence, DES was not much recommended for advanced security operations. To overcome this threat, AES was designed by using DES algorithm as a base as shown in figure 2.2.5

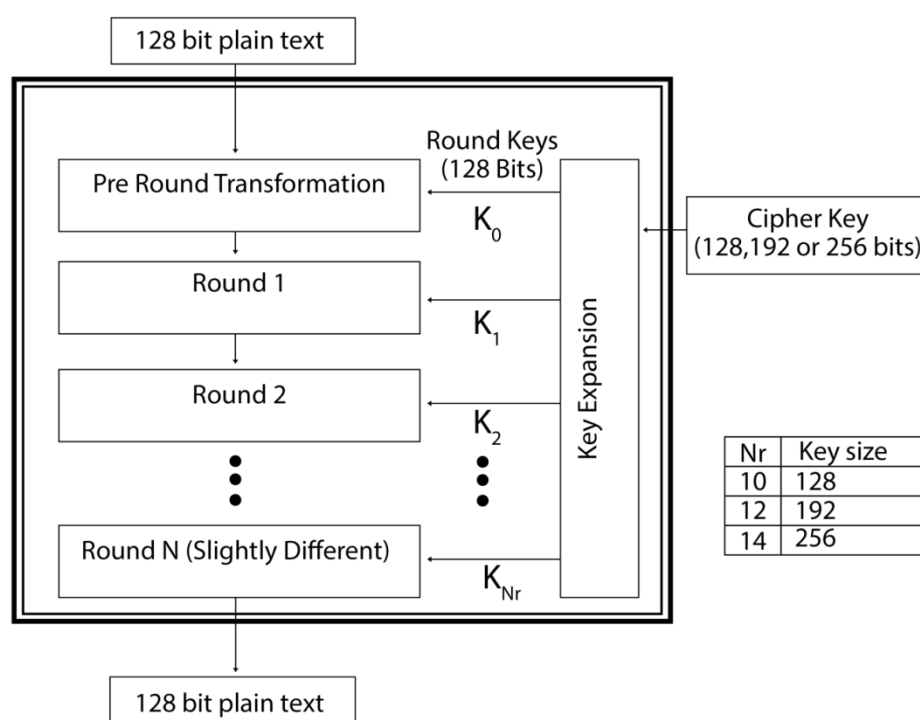


Figure 2.2.5: AES algorithm

Even though AES uses DES as the base algorithm, it has its own features they are:

- Plain text is divided in 128 bit blocks. If any block does not have sufficient bits, then extra bits are padded to the text at the end of the message.
- Based on the key length used, the number of rounds is decided.
 - If key length is 128 bits (i.e. 16 bytes) then the number of rounds is 10. This version is named as AES128
 - If the key length is 192bits (i.e. 24 bytes) then the number of rounds is 12. This version is named as AES192
 - If key length is 256 bits (i.e. 32 bytes) then the number of rounds is 14. This version is named as AES256

128 bit plain text is passed through initial permutations and positions of the text are changed based on the permutations decided.

The text passes through all the rounds by performing round operations with keys generated by the key generation module.

After completing all the rounds text is passed to final permutation and cipher text is produced. The process of decryption will be the reverse procedure to the encryption process.

RSA ALGORITHM:

RSA public key algorithm was developed in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman. This algorithm is used to send the information securely over a non-secure medium. In RSA algorithm, the plain text is encrypted using a public key and encrypted data is decrypted using a private key.

The Rivest-Shamir-Adleman (RSA) algorithm is used to generate the private and public keys. The algorithm is as follows:

- Let m is the original message which should be decrypted
- Choose p and q where p, q are prime numbers
- Compute $n = p * q$
- Compute $\phi(n) = (p - 1) * (q - 1)$
- Choose e such that $1 < e < \phi(n)$ and m^e and $\phi(n)$ are coprime. i.e. $\gcd(e, \phi(n))=1$
- Compute a value for d such that $(d * e) \% \phi(n) = 1$.
- Now Public key is (e, n)
- The private key is (d, n)
- Now cipher text $c = m^e \bmod n$
- For decrypting message $m = c^d \bmod n$

Execution of this algorithm starts with choosing two prime numbers. The product of these two prime numbers will be ' n ' which is known to both sender and receiver. Choose the ' e ' value, based on the condition listed in the algorithm, which is known to sender only.

As sender knows ' e ' and ' n ' values, he computes the receiver's public key. By using ' d ' and ' n ' values, the receiver will compute the private key.

Based on the equations listed above, encryption and decryption will take place.

Diffie- Hellmen key exchange:

Security of encryption and decryption majorly depends on the key. If the key is not exchanged securely, then the entire effort goes in vain. Diffie Hellmen key exchange algorithms are the most popularly used algorithms for secure key exchange between the sender and the receiver. The secure key that was sent secretly will be used for further encryption and decryption process.

Algorithm is as follows:

Consider two persons X and Y who wish to create a shared key and agreed for p and base g, where p is a prime number and g is a random integer, such that $g < p$ and g are the primitive root of p.

- X chooses secret key a and sends to Y using $A = g^a \text{ mod } p$
- Y chooses secret key b and sends to X using $B = g^b \text{ mod } p$
- X computes secret key using $s = B^a \text{ mod } p$
- Y computes secret key using $S = A^b \text{ mod } p$

Now, as a result, both X and Y will have the exchanged secret key value. And further, this secret key value will be used for symmetric encryption. So, by using the above procedure, two parties shares the secret key securely.

(iii) Applications of Encryption and Decryption

Few applications of encryption and decryption are:

- Most of the persons are using this for exchanging or transferring their content from one end to the other.
- All the online shopping sites and banking enterprises are using it to secure the user data.
- Set-top boxes, modems, smart cards and SIM cards, all use it to encrypt sensitive data.
- Digital rights management systems are using it to prevent unauthorised use of data or duplication of copyrighted material.
- Single Sign On system also uses encryption and decryption to transfer the passwords between the parties.
- All mobile banking transactions are encrypted and decrypted based on the needs.
- Most of the Databases store the data in encrypted format.
- Most of the social engineering sites are preserving the user's data in the encrypted format only.



- ### 2.2.4 Applications of Cryptographic Hash Function

Hash functions use complicated mathematical steps to produce the output strings. It includes XOR operations, shifting of bits, modules operation and so on.

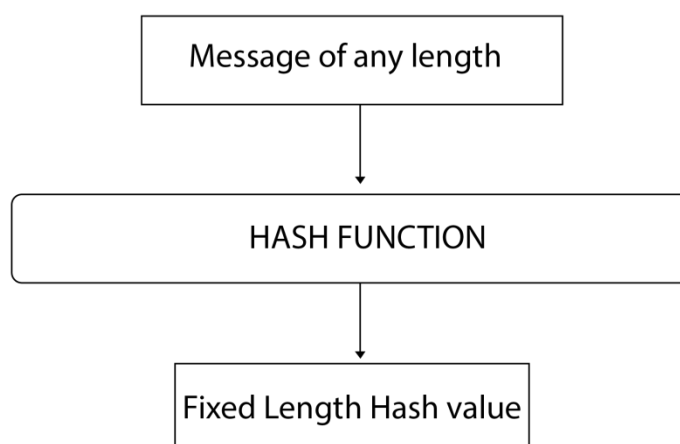


Figure 2.2.6: Basic hash function

The cryptographic hash function is one type of hash function, which takes a detailed message as an input and produces simple alphanumeric strings. This string can be named as message digest or hash value or digital footprint or digest or checksum.

It possesses few basic properties such as:

- It is very easy to calculate hash value of any text, but by using a hash value, it is highly impossible to calculate the original message.
- No two messages provided to hash function results in same hash value.
- Any two messages having very minimal changes will also have a different message digest.

This concept would be extremely useful for authenticating the messages, which are transferred through the internet or network. When a message is received from the sender, the receiver has no assurance that he has received messages from the sender. The concept of cryptographic hash function will resolve these issues.

This concept has been used in different places in network security.

(i) Message Authentication

Message authentication should confirm few aspects such as

- Whether the message is from a valid source
- Whether message has not been modified by any intruder

To assure these points, the Messages Authentication Code (MAC) algorithm has been introduced, also known as keyed hash function. Its execution can be explained as follows:

MAC is a symmetric key cryptographic technique, i.e. both sender and receiver will use the same key for the overall process. MAC uses existing standard hashing function for the overall process like MD2, MD5, etc.

MAC algorithm accepts original message and symmetric key as the inputs. By using both inputs, a message digest is calculated. This message digest will be transmitted along with the original message as proof of authentication, as shown in figure 2.2.7.

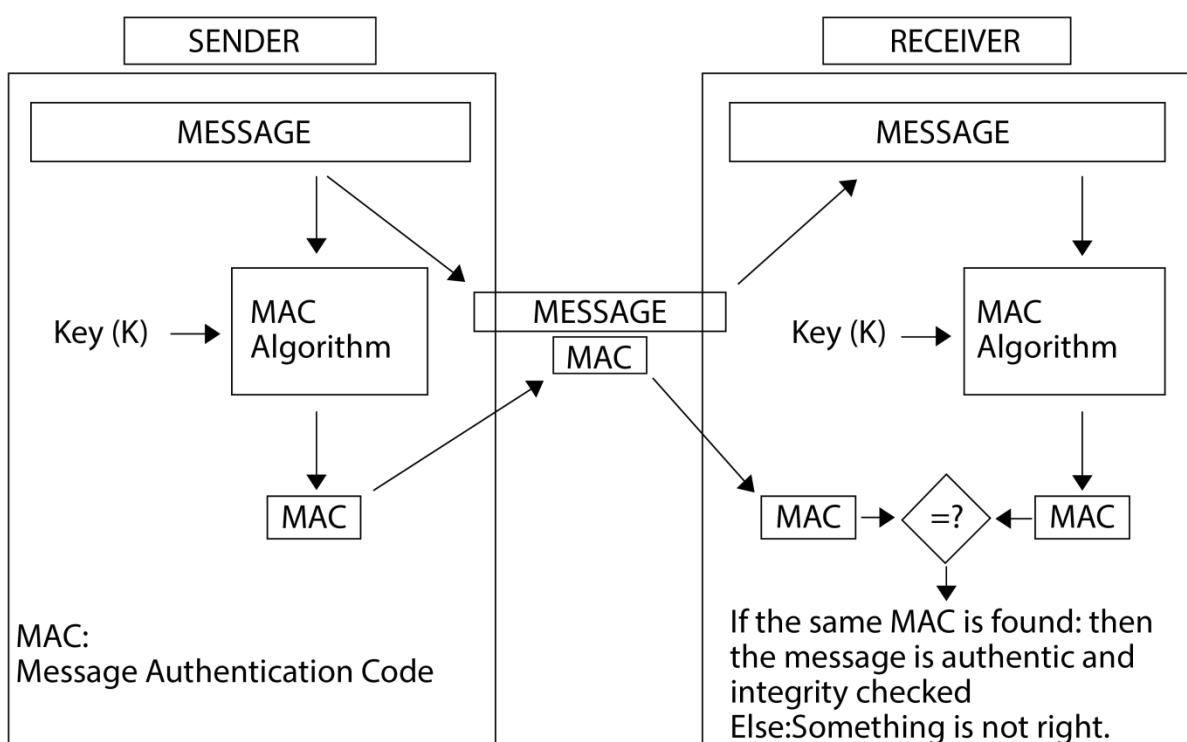


Figure 2.2.7: Message authentication code

At the receiver side, on receiving the message MAC value is recomputed by using the same algorithm used by the sender with symmetric keys. If the digest produced is same as the senders digest value, then it is considered as the original message, without intruder modifying the message. If message digest values are not same, then it indicates that either the message is not from valid source or message is modified by intruders.

Limitations of MAC:

- As MAC uses a symmetric key, the algorithm cannot be secure until the key exchange is not revealed in the external world.
- Even though the intruder has not changed the message, there is a chance that the receiver can modify the message and claims that the sender has sent the same message. MAC cannot provide any proof for this because even if the sender calculates the MAC value, it will be same as receiving wrongly computed values. Hence, nothing can be traced out.

(ii) Digital Signature

To avoid the disadvantages of MAC, digital signature has been introduced. As handwritten or typed documents are combined with signature as a proof of authentication. Similarly, digital documents are attached with digital signatures as a proof of authentication.

Digital signatures are created by using personal or entity digital data. Sender or receiver or third party can verify it. Digital signatures are calculated by using asymmetric key procedure, i.e. private–public keys are used in this algorithm, as shown in figure 2.2.8.

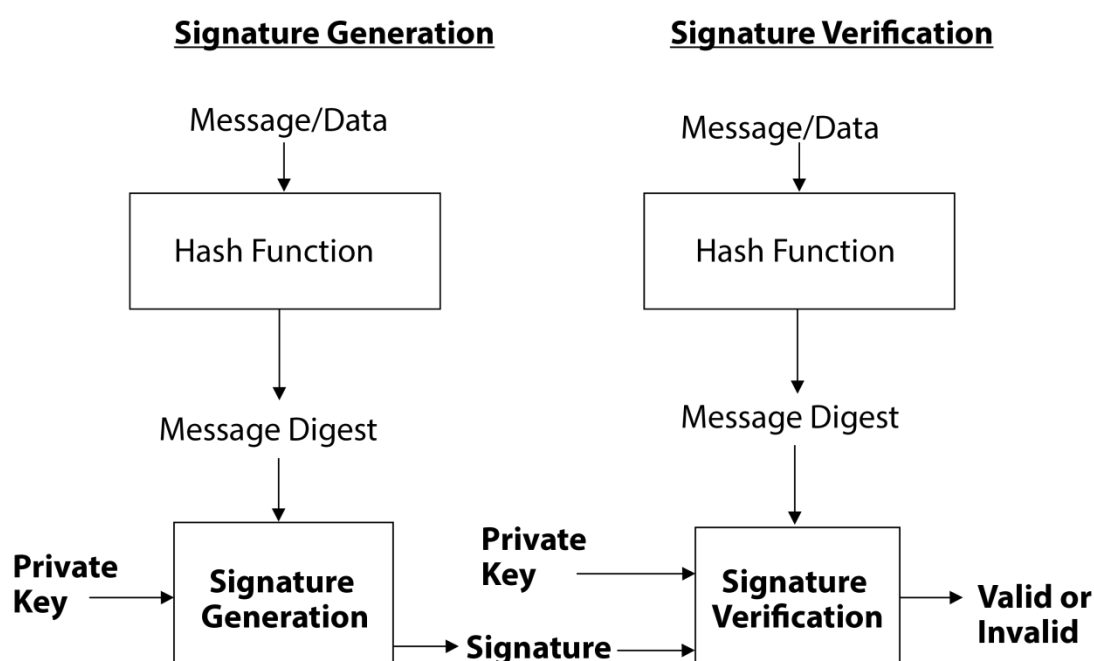


Figure 2.2.8: Digital signature

- The sender/ signer will feed his original message to an existing hash function and gets a hash value.
- Signers hash value along with their private key are fed to signature algorithm and produces a file with data and digital signature.
- At verifier/receiver side, the data is submitted to the same hash function used by the sender and digital signature along with the public key of the sender. This is fed to the verification algorithm.
- If the result produced by both hashing and verification algorithms are same, then we can consider it as a valid and uninterrupted document.

(iii) Other Applications

Password Protection: In spite of saving the direct password, it is recommended to save the message digest of the password, which will protect the password intrusion. This system is very useful for secure sign on application for transferring the user credentials.

Error detection of the message: Before transmitting the message over the network its hash value is calculated. Data and hash values are transmitted to the receiver, who intern uses data as input to hash function, produced results are compared to the received hash value if they are same then message is not altered, else it is changed and is considered as an error in the message. Either it is trying to correct or discard the message or the same is informed to the sender.

Most of the confidential information documents which needs authentication are attested with digital signatures.

Hash functions are used for data compressions as well.

Holograms and QR codes are generated by hashing the original information.



Self-assessment Questions

- 7) In cryptography MAC Stands for _____.
a) Message Authentication Code b) Member Authentication Code
c) Message Authorisation Code d) Member Authorisation Code
- 8) A digital signature is a _____.
a) Handwritten signature b) Photo of signature
c) Encryption information d) Cyclic redundant check
- 9) What is the message digest used for?
a) To preserve the integrity of the message
b) To transfer the message to the receiver
c) To create the message by the sender
d) To communicate with sender and receiver

2.2.5 Requirements and Security

A strong security system always expects few requirements of the system. They are as follows:

- All types of security features must be set up such that they are extremely strong
- Complete control of the security that is managed by a single person is not recommended
- Network of the system must be made strong with firewalls, honeypots and other security standards
- Conduct internal and external security audits periodically
- The users of the system must never reveal their passwords to anyone and it should be changed frequently
- Use strong encryption and decryption algorithms
- A strong key exchange system must be used for key exchange
- Length of the keys must be considerably longer
- All the documents sent or accepted must be digitally signed

(i) Security Requirements for Cryptographic Hash Functions

The Security of any hash function purely relies on the extra stuff added in the process and algorithm itself. If the algorithm is not strong, then its logic can be predicted and misused such kind of attacks are called as birthday attacks.

Key length alone governs the security of the hash function. If the length of the key is small, then it can be cracked by using brute force attacks.

Pre-image resistance: The value produced by the hash functions should be in such a way that the message cannot be predicted from it. If it can be predicted, it means it is vulnerable to pre-image attacks.

Second pre-image resistance: If the hash function produces same hash value for two messages, as shown in figure 2.2.9, it means that it is weak in collision resistance and is vulnerable to second pre-image attacks.

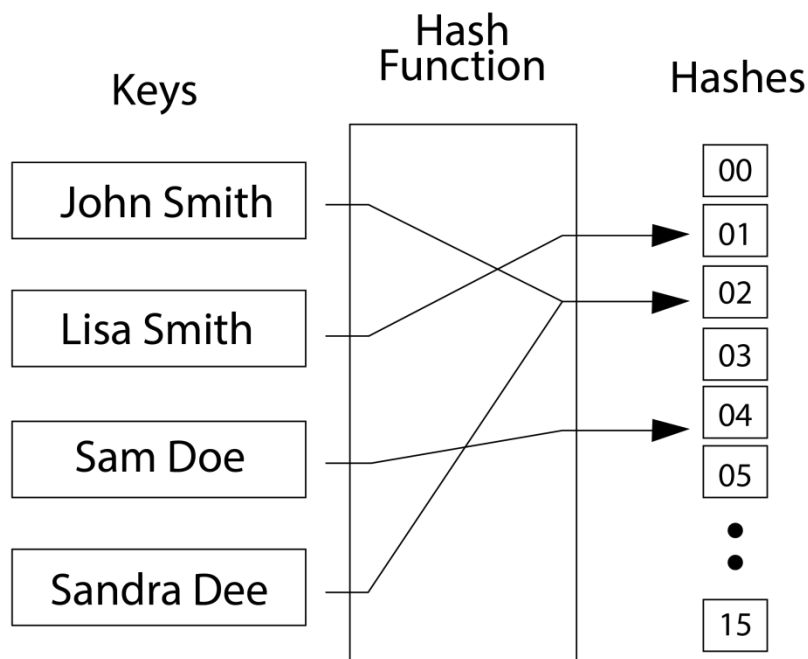


Figure 2.2.9. Example of lack of collision resistant

(ii) Brute-force attacks

It is an attack applied by using trial and error methods for breaking passwords, encryption keys and hash function logics and so on. It is a very time consuming process, but successful. To

avoid this attack, all types of key must have a considerable length and should not stay for long duration. Most of the organisation insists their employees to use a strong password, which should contain a combination of characters, special characters and numbers. This makes it very difficult for the attackers to break the passwords.

If the lengths of the keys are small, then they are prone to brute force attacks.

(iii) Cryptanalysis

It is a type of attack done by studying the ciphers, cipher text or crypto system with an aim of finding the weakness in the system, such that the plain text can be extracted from the cipher text without knowing keys or the logic of the algorithm. This analysis many times provide the details about the structure of key and with this, the number of key possibilities will reduce considerably and then brute force attack can be applied with less key combinations.

Sometimes this attack focuses on:

- Knowing part of the plain text from which remaining can be guessed.
- Obtain the logic of the algorithm by trying with different messages with different key combinations.



Self-assessment Questions

- 10) If hash values calculated twice for the same message are same, then it called as _____.
a) Image resistance of hash b) Pre-image resistance
c) Second pre-image resistance d) Pre-resistance
- 11) A brute force attack is _____.
a) Logical method b) Trial and error method
c) Compromise method d) Guess method

2.2.6 Hash Function Based on Cipher Block Chaining

Cipher Block Chaining (CBC):

Cipher block chaining is used for encrypting the plain text to cipher text by using a single key called as initialising vector.

In cipher block chaining the overall data is divided into equal sized blocks and if last block has less content, then it is padded with extra bits to make the length same.

Let $P_1, P_2, P_3, \dots, P_n$ be the different blocks of plain text. An initialisation vector S_0 is a secret key used to start the process.

Main logic of CBC works as shown in the figure 2.2.10. First block of plain text is XOR with initialising vector S_0 and the result is used as an input to encryption algorithm E_K , which produces C_1 as cipher text, which is used as a key for encrypting the next block P_2 and this process continues until the entire plain text is converted as cipher text blocks $C_1, C_2, C_3, \dots, C_n$.

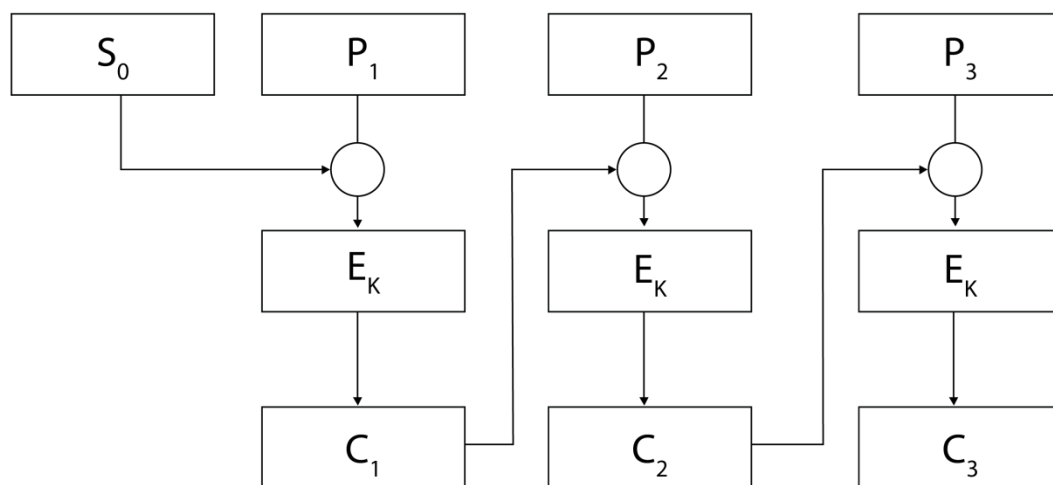


Figure 2.2.10 Logic of CBC

The main advantages of this approach is:

- Even though the two blocks have same content, they still produce different cipher text, resulting to avoid birthday attack. Birthday attack is an attack that predicts the logic of the algorithm by analysing the output of the hash function.

- More keys are not required because the cipher text of previous block can act as a key for the next block.

The same logic of the CBC can be used for hashing, but major difference is, in the case of encryption and decryption, the result would be entire $C_1, C_2, C_3, \dots, C_n$. Whereas, in the case of hashing, the final result C_n is considered as the message authentication code (MAC).

The process of MAC construction by using CBC logic is as follows in figure 2.2.11

- Divide the message into same sized blocks of plain text P_1, P_2, \dots, P_n . Add extra bits of the last block to make the size same.
- Perform XOR between initialising vector (IV) with the first block of plain text P_1 . The result is used as an input for a hashing function (E_K) and the resultant message digest is used as a key for the next block.
- This process continues, until all blocks of data completed and MAC will be the result after completing the process.

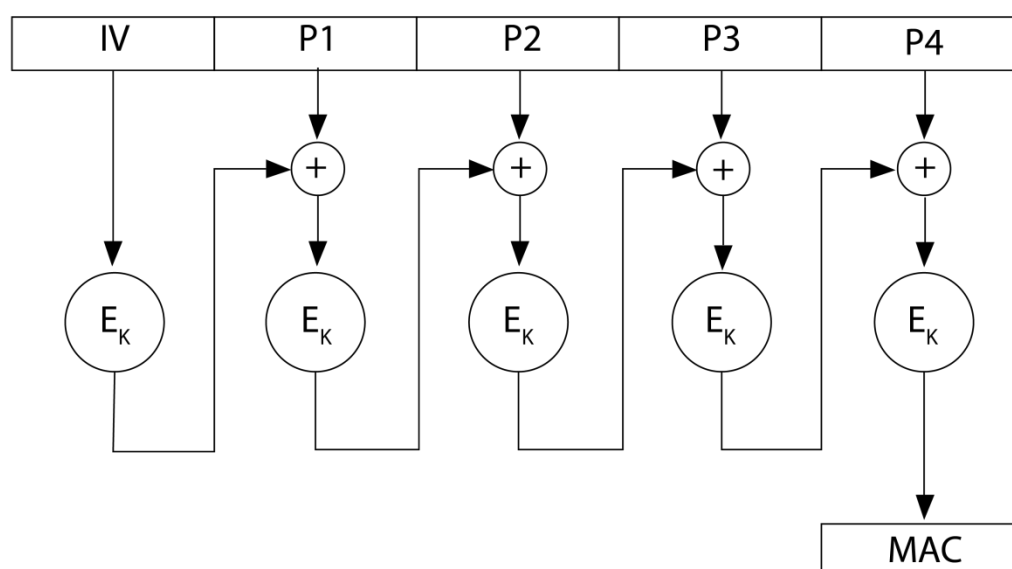


Figure 2.2.11: Hashing based on cipher block chaining

The main advantage of using CBC for hashing would be:

- The same length message digest is produced for messages of any length
- It becomes more difficult for the cryptanalysis to analyse the data
- It is almost difficult for a birthday attack and bruit force attack to crack this message digest



Self-assessment Questions

- 12) Hash function in cryptography takes an arbitrary block of data as input and returns ____.
- a) Variable Length Message
 - b) Zero Length Message
 - c) Fixed Length Message
 - d) Two Digit Key
- 13) By seeing the cipher text, if an attacker getting the information about encryption algorithm, then such kind attack can be called as ____.
- a) Brute Force Attack
 - b) DOS Attack
 - c) Man in the middle Attack
 - d) Birthday Attack

2.2.7 Secure Hash Algorithm (SHA)

Secure Hash Algorithm is a cryptographic hash function designed and published by NIST as a U.S. Federal Information Processing Standard:

It has 4 versions they are as under:

- SHA-0: It is an 160 bit hash function designed in 1993, but withdrawn very soon because of significant flaw and published with updated version SHA-1.
- SHA-1: It is a 160-bit hash function, which resembles MD5 algorithm. It was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. Because of its weakness, it is no longer used as a security standard after 2010.
- SHA-2: It is a family of two hash functions SHA-256 and SHA-512 designed by NSA. Even the logic of hashing is same, they differ in word size as SHA-256 uses 32-bit words and SHA-512 uses 64-bit words. Few truncated versions do exist in this family, which are known as SHA-224, SHA-384, SHA-512/224 and SHA-512/256.
- SHA-3: It is a family of hash functions with the same length as SHA-2 but completely different logic for execution was designed. It uses a hash function, namely Keccak. The standard released in this version is FIPS PUB 180, FIPS PUB 180-1 and FIPS PUB 180-2. NIST has updated Draft FIPS Publication 202 which a difference from Secure Hash Standard (SHS).

SHA-1:

Physical properties of SHA-1 are as follows:

- SHA-1 accepts data of a length that is < 264 bits and produces an output which is of 160 bits. This output is also called a message digest.
- It divides overall message as blocks of 512 bits.
- Maximum data allowed is 264 bits. SHA-1 is defined for a file with size more than 264 bits.
- Length of the message is added at the end of the message.
- The overall process is divided into 5 states, namely A, B, C, D and E.
- Each state performs 16 operations.
- Each operation has a few bit rotations and number of rotations are different for different states.
- The size of each state is 32 bits.
- Additions module 232 is used for performing additions.

Working of SHA-1:

The overall message is divided into equal sized message blocks, i.e. 512 bits, out of which last 64 bits are for the length of the message, if the message size is not equal to 512 bits, 1 is padded to the message rest of the bits are filled with 0 and at last message length is added.

Now, the message will be in the form of $512 \text{ bits} * n$, where n is number of blocks of the message.

Then process all the blocks one by one as shown in the figure 2.2.12

SHA-1 functions and operates, as shown in figure 2.2.12, in 32-bit words and produces a 32 bit output word.

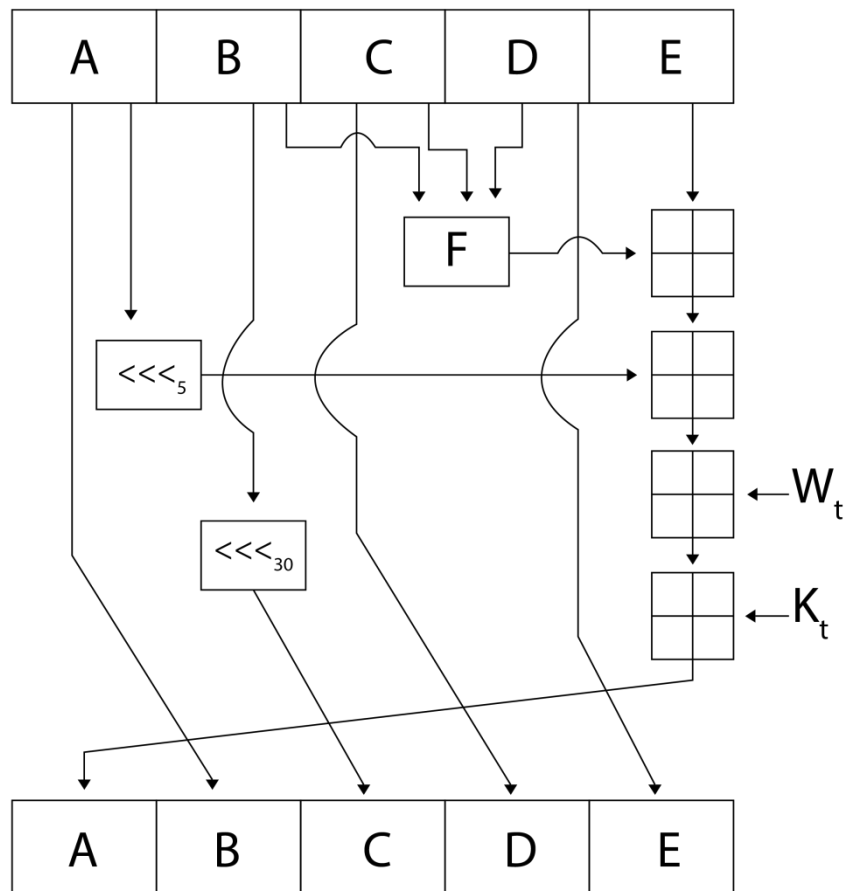


Figure 2.2.12 Working of SHA-1

One iteration within the SHA-1 compression function:

A, B, C, D and E are 32-bit words of the state:

F is a nonlinear function that varies as follows;

- \lll_n denotes a left bit rotation by n places; n varies for each operation; W_t is the expanded message word of round t ; K_t is the round constant of round t ;
- \boxplus denotes addition modulo 232, which is used for performing additions.

SHA-512

To increase the complexity of the hash value, SHA-1 has been restructured and SHA-512 is produced. It has same logic as SHA-1, but the numbers will differ such as:

- SHA-512 accepts message less than 2128 bits length and produces a message digest of 512 bits.
- Uses initialisation vector or key size as 512 bits.
- It divides over message as blocks of 1024 bits. Among 1024 bits, the last 128 bits are allocated for message length.
- Maximum data allowed is 2128 bits.
- The overall message is divided into 8 states and each state performs 10 operations.
- The size of each state is 64 bits.
- Addition modulo 264 is used for modulo operations.

Working of SHA-512:

The overall message is divided into equal sized message blocks, i.e. 1024 bits, of which the last 128 bits are for the length of the message. If the message size is not equal to 1024 bits, then 1 is padded to the message and rest of the bits are filled with 0 (at the last positions of the message).

Now, the message will be in the form of 1024 bits*n, where n is number of blocks of the message.

Then process all the blocks one by one, as shown in the figure 2.2.13.

SHA-512 uses functions and operates on 512-bits key and 1024 bit message to produce 512 bit output. First function takes input as first block (M1) and initialisation vector (H0) and produces a 512 bit output (H1) which will be passed as input to the second function. The second function accepts a second block (M2) and output of first function (H1) and produces a hash value (H2), which will be passed to the next function. This process continues until all the message blocks are completed.

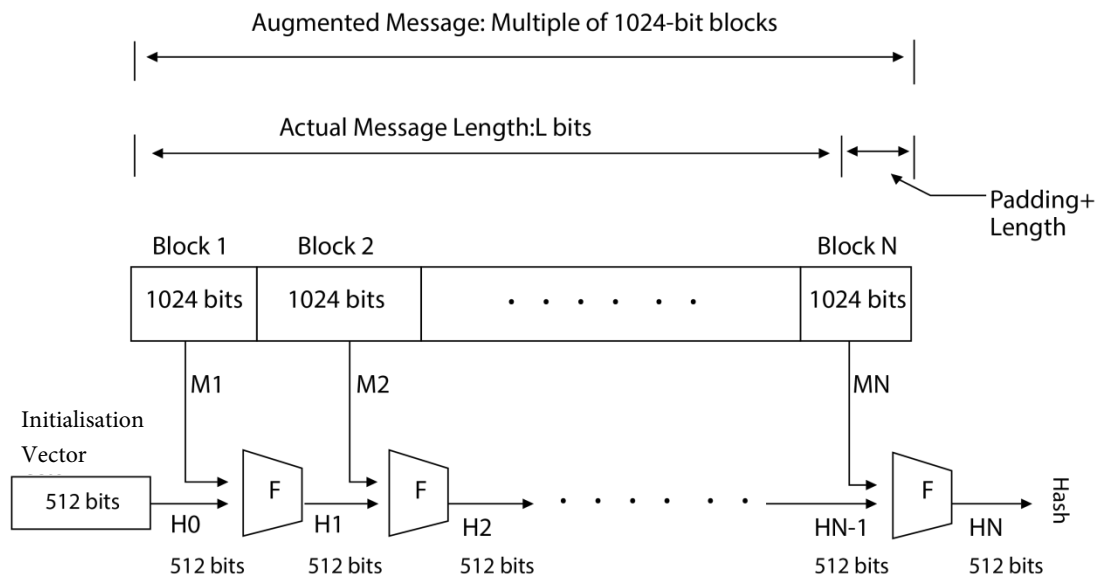


Figure 2.2.13 Working of SHA-512

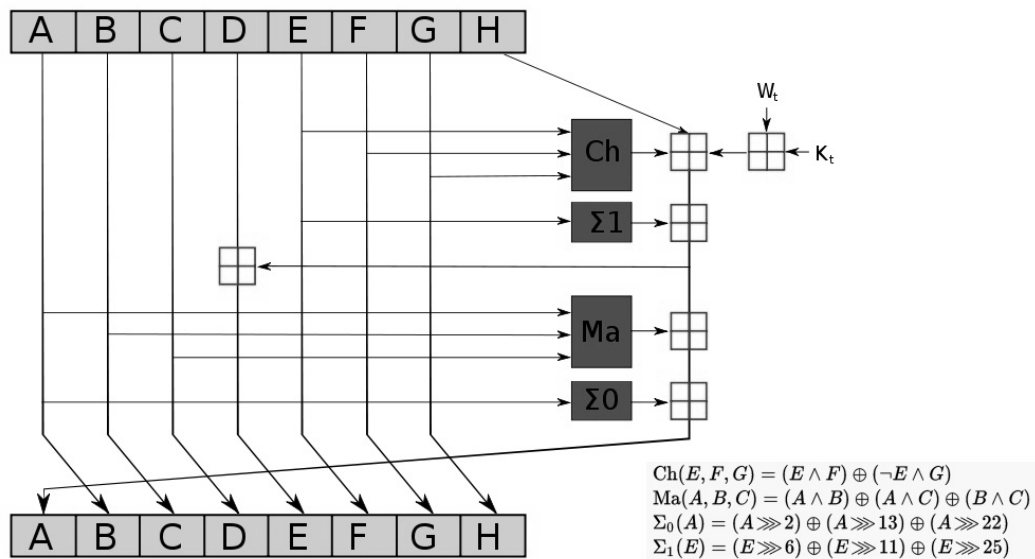


Figure 2.2.14 Operation of SHA 512

One iteration in a SHA-512 family compression function is shown in figure 2.2.14.

A, B, C, D, E, F, G and H are different states of one function. Each state consumes 64 bits, Each state accept some portion of text from block of text and performs few operations like change of bit positions, addition, modulo and swap. Output of few states is being transferred to other states like A is transferred to B, B is transferred to C,....., as shown in figure 2.2.14.

Since SHA-512 is free from all the attacks that SHA-1 was facing, it is used in many security applications.



Self-assessment Questions

- 14) The length of an initialisation vector in SHA-512 is ____.
- | | |
|------------|-------------|
| a) 32 bits | b) 128 bits |
| c) 64 bits | d) 512 bits |
-
- 15) Number of rounds in SHA-512 is ____.
- | | |
|-------|-------|
| a) 60 | b) 30 |
| c) 80 | d) 20 |



Summary

- Encryption and Decryption help to convert the message into an unreadable format, so that the intruders cannot access it.
- Encryption is a process of converting the file into an unreadable format so that only intended recipient can understand and use it.
- Encryption can be symmetric or asymmetric. Symmetric encryption uses single key, whereas asymmetric encryption uses a pair of private and public keys. Mathematical algorithms are used to generate these keys.
- Symmetric key encryptions are safe, if the key exchange is done in a secured way.
- Asymmetric key encryption encrypts the file by using the public key of the sender and decrypts by using the private key of the receiver.
- Cryptographic hashing algorithms are used for producing hash key based on the content of the file. This can be used for authenticating the file. This process can be used for MAC, digital signatures, error detection and password protection.
- MAC cannot provide complete authentication, hence the digital signature is used for message authentication.
- Basic security requirements have to be fulfilled to avoid birthday attacks, brute force attacks and cryptanalysis attacks.
- SHA is a secure hashing algorithm used for calculating the hashing value for the file data. SHA is a most suitable hash function, which could able to tolerate lots of security attacks.



Terminal Questions

1. What are the terminologies used for basic encryption and decryption?
2. What is the difference between symmetric-key encryption technique and asymmetric key encryption technique?
3. Explain RSA algorithm in detail.
4. What are the different attacks on hash function? List few applications of cryptographic hash functions.
5. Explain how cipher block chaining can be used to construct a hash function.
6. With a neat diagram, explain the working of SHA-512.



Answer Keys

Self-assessment Questions	
Question No.	Answer
1	b
2	b
3	c
4	a
5	d
6	b
7	a
8	c
9	a
10	b
11	b
12	c
13	d
14	d
15	c



Activity

Activity Type: Online

Duration: 30 Minutes

Description:

Research and present how encryption and decryption is done in bank systems.

Case Study

Myfootware Corporation is a new company started very recently. It was a footwear manufacturing industry. It has a lot of wings in their organisation they are as follows:

Design section: Where the designer is occupied and is a very confidential area because it has designs, which cannot be disclosed. Each design created is transferred to design server by encrypting it with the public key of design section and private key shared only with management section for approvals.

Manufacturing section: Where manufacturing happens. For an authenticity in the manufacturing industry, a hologram is added to every product that is manufactured.

Logistic and dispatch section: All the approved orders and procured raw material details are secretly shared with logistic section by management section.

Management section: All the documents shared or received by the management section expect a digital signature. Most of the marketing people working in this department expect the quotation, which will be delivered with digital signature.

By considering the above criteria, answer the following questions:

1. Why does the design section need asymmetric key encryption? Can it be managed with shared key encryption? Justify.
2. Does every employee of the management section require independent digital signature? If yes, suggest a simple digital signature algorithm which reduces the cost of digital signature.
3. Every hologram produced by manufacturing section includes company information as a point of authenticity. So, justify which hashing technique would be better to minimise the message digest value?

Bibliography



e-References

- *Cryptography*. Retrieved 5 Jan, 2017 from <http://www.cs.iit.edu/~cs549/lectures/CNS-1.pdf>
- *Encryption and Decryption*. Retrieved 5 Jan, 2017 from <http://www.cs.iit.edu/~cs549/lectures/CNS-1.pdf>
- *Symmetric and Asymmetric encryption algorithms*. Retrieved 5 Jan, 2017 from <http://searchsecurity.techtarget.com/answer/What-are-the-differences-between-symmetric-and-asymmetric-encryption-algorithms>

Image Credits

- Figure 2.2.1: <http://www.cs.iit.edu/~cs549/lectures/CNS-1.pdf>
- Figure 2.2.2: http://books.gigatux.nl/mirror/securitytools/ddu/images/0321194438/graphics/09fig02_alt.jpg
- Figure 2.2.3: http://books.gigatux.nl/mirror/securitytools/ddu/images/0321194438/graphics/09fig02_alt.jpg
- Figure 2.2.4: <http://www.tuicool.com/articles/Ub6rui>
- Figure 2.2.5: <http://www.seminarsonly.com/computer%20science/Confidential%20Data%20Storage1.jpg>
- Figure 2.2.6: http://vignette1.wikia.nocookie.net/computersecuritypsh/images/5/5f/Hash_Function.png/revision/latest?cb=20110323192006
- Figure 2.2.7: <https://upload.wikimedia.org/wikipedia/commons/thumb/0/08/MAC.svg/661px-MAC.svg.png>
- Figure 2.2.8: http://vignette2.wikia.nocookie.net/itlaw/images/e/e2/Snapshot_2009-07-29_20-53-38.gif/revision/latest?cb=20090730035532
- Figure 2.2.9: https://upload.wikimedia.org/wikipedia/commons/thumb/5/58/Hash_table_4_1_1_0_0_1_0_LL.svg/240px-Hash_table_4_1_1_0_0_1_0_LL.svg.png
- Figure 2.2.10: <http://slideplayer.com/slide/5128231/>
- Figure 2.2.11: <https://www.cs.rit.edu/~ark/fall2012/482/module05/CbcMac.png>
- Figure 2.2.12: <https://en.wikipedia.org/wiki/SHA-1>

- Figure 2.2.13: <https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture15.pdf>
- Figure 2.2.14: <https://en.wikipedia.org/wiki/SHA-2>



External Resources

- Whitman, M. E., & Mattord, H. J. (2003). *Principles of information security*. Boston, MA: Thomson Course Technology.
- Stallings, W. (2000). *Network security essentials: applications and standards*. Upper Saddle River, NJ: Prentice Hall.
- Pachghare, V. K. (2009). *Cryptography and information security*. New Delhi: PHI Learning.



Video Links

Topic	Link
Block cipher modes of operation	https://www.youtube.com/watch?v=aflVXL8N_WI
Cryptographic Hash Function	https://www.youtube.com/watch?v=jKEK4hb9Nn8
SHA	https://www.youtube.com/watch?v=dcCl72uebos



Notes:



Information Security - I

MODULE - III

System and Server Security

System and Server Security

Module Description

Most of the business operations are purely dependent on the internet. The internet is considered as one of the critical resource for the organisation growth. Imagine the world without the internet is extremely difficult. Intruders are targeting all the operations of the internet, so there is a security threat to the organisational resources. Every organisation tries to protect their information and assets from intruders. Awareness on intrusion and its effects would help to design a strong security system.

This module starts with a brief description about system security and possible threats and how it can be protected with the help of firewalls. As we know that many organisation's information systems are protected with a simple username and password authentication, so this module focuses on different password cracking techniques used by hackers to hack the user account. It also focuses on keyloggers, different types of viruses, worms and windows security. This module also focuses on various causes and effects of malware and spyware on the computer system along with their prevention methods. The main objective of this module is to protect the security of the system rather than harming it.

At the end of this module, students will be able to understand the importance of system security, server security and its possible threats such as virus, worms, spyware, keyloggers and also its counter measures. Based on this information, organisation can protect their system from security threats by using proper security methods. The students will also learn about several firewalls and their drawbacks.

Chapter 3.1

System Security and Firewalls

Chapter 3.2

Virus, Worms, Malwares and Spywares

Chapter Table of Contents

Chapter 3.1

System Security and Firewalls

Aim.....	115
Instructional Objectives.....	115
Learning Outcomes.....	115
3.1.1 Introduction.....	116
3.1.2 System Security.....	116
(i) Introduction.....	116
(ii) Concerns of System Security	117
Self-assessment Questions.....	120
3.1.3 Desktop and Server Security.....	121
Self-assessment Question	122
3.1.4 Firewalls.....	123
(i) Packet Filter.....	125
(ii) Dynamic Packet Filter	127
(iii) Application Gateway	127
(iv) Circuit Relays.....	129
(v) Personal and/or Distributed Firewalls.....	129
Self-assessment Questions.....	130
3.1.5 Techniques of Password Cracking.....	131
Self-assessment Questions.....	135
3.1.6 Keyloggers.....	136
(i) Hardware Keyloggers.....	136
(ii) Software Keyloggers.....	137
(iii) Implementation and Security of Keyloggers	138
Self-assessment Questions.....	139
Summary	140
Terminal Questions.....	142
Answer Keys.....	143
Activity.....	144
Case Study	145
Bibliography.....	146

e-References	146
External Resources	147
Video Links	147



Aim

To familiarise the students with the concepts of system security and its possible threats and solutions



Instructional Objectives

After completing this chapter, you should be able to:

- Explain the concept of system security and its need
- Elaborate desktop and server security
- Explain the use of various types of Firewall and its design structure
- Enumerate about various password cracking techniques used by hackers to hack the user account
- Describe the main features of different types of Keyloggers



Learning Outcomes

At the end of this chapter, you are expected to:

- Outline the concept of system security and privacy and security issues related to it
- Distinguish between system, desktop and server security
- Recognise the advantages and disadvantages of each type of firewalls
- Demonstrate the design and working of various types of firewalls
- Identify the types of password cracking methods used by hackers
- List pros and cons of hardware and software Keyloggers along with its implementations and security

3.1.1 Introduction

Since internet connects all the systems across the world and transmits data, one must ensure that the data being sent must be secured over the network from being intruded. So, to ensure this security, a strong security system is to be built.

System security refers to the control of access to a computer system's resources, especially its data and operating system files. The main objective of the system security is to protect the data. This chapter helps us to understand the various concerns related to the security of the system and the solutions related to these issues.

At the end of this chapter, student will be able to understand the loopholes present in the systems that are exposed to the intruders. Students will also learn about the strengths of a security system and firewalls to build a strong security system.

3.1.2 System Security

(i) Introduction

Most of the world population is using the internet today. This number will increase over a period of time, which will increase the probability of threat. Most of the confidential information is stored on servers, which are connected to the internet. The target of the intruders is to get an access to such information. So, the protection at each level of connectivity can prevent computer crimes and computer abuses.

Computer crime and computer abuse are two distinct factors:

- **Computer Crime:** It is the manipulation or theft of computers and its resources by any method to obtain money, property or any advantage.
- **Computer Abuse:** It is an unauthorised use of computer and its resources for unethical activities.

Computer crime breaks the laws, whereas computer abuse misuses the laws.

Most of the organisations believes that “protecting their system from external and internal threats can only protect their business progress”. Achieving and maintaining the system security for any organisation is not so simple. To build the security solution, one must consider the resources and productivity of the organisation.

System security can be planned for an organisation in multiple phases.

In the initial phase, let us focus on protecting the organisational information from the external computer crimes such as hackers and cyber crimes. To achieve this, system security must be combined with firewalls, antivirus software's, Virtual Private Networks and intrusion detection and prevention systems. Once the system is built, check for potential gaps and possible loopholes, which the intruders will use to penetrate into the system.

In the next phase, the focus is on the internal security. This focuses on the security requirements within the organisation. Major security problems within the organisation will be focused on access control management. So, ensure that a proper access allocation method is used. Educate every employee of the organisation with security policies and ensure that they will use best of possible password combinations.

In the next phase, the focus should be on emergency plans. In this phase, a continuous monitoring system is deployed, to monitor the serious possible security violations. Certain action plan needs to be initiated, such as switching off the servers, diverting the network traffic through backup routers, diverting the regular activities through backup servers and so on.

(ii) Concerns of System Security

Security system always concerns about the factors, which disturbs the critical characteristics of information. They are:

- **Confidentiality:** Protecting the disclosure of the information from the unauthorised users.
- **Availability:** Access of information by the authorised users, whenever needed.
- **Integrity:** Protecting the information from being modified by the unauthorised users.

Major concerns of system security are hacking, spoofing, spamming, jamming, malicious softwares, sniffing and identity thefts. Few security issues will have simple and common solutions, but few of them will have exclusive solutions.

- **Hacking:** If any illegal or unauthorised user accesses the system, then it can be considered as hacking. A hacker with a crooked mind sometimes tries to crash the system. These illegal accesses are done through hacking software's, *for example*, angry IP scanners, Kali Linux, Cain & Abel and so on. These softwares can be hidden from the scanners and antiviruses.

As a solution to the problem, update the antivirus software's every day and deploy strong firewalls with strong packet filter rules, which can filter the messages.

- **Spoofing:** Spoofing is a malicious practice of sending a message from invalid source, claiming as a valid source.

For example: sending appointment order by using the names of a well-known organisation. These emails seek the account details for the personal benefit.

Sending prize winning emails under the name of well-known organisations.

Sending software links from the friend's email address.

Now-a-days most of the intruders are creating false websites, which appears exactly like original website and used to collect the sensitive information known as "phishing".

Most of the spoofing can be avoided only by careful observations of mail addresses or URLs. A firewall can help to some extent.

- **Spamming:** A practice of sending unwelcomed mails and unwanted messages can be considered as spamming. Many times spamming is used to make network congested and study the loopholes of the system. This mostly happens to emails.

Spamming can be avoided by using strong antispam software and strong firewalls.

If an individual wants to protect themselves from spams, then they should not believe in unknown user mails and prize money mails. Strong spam rules should be set for an email client to filter the spam mails. Firewalls can be configured to filter the spam mails.

- **Jamming:** With this kind of activity, a huge number of messages are created and sent into the network. This huge number of messages will create congestion in the network and drops all the existing messages in the network. In this process, along with unwanted messages, valid messages will also be dropped. This kind of threat can be considered as jamming or Denial of service (DoS). Jamming provides less access to the valid users and decreases the performance of websites.

As jamming is considered as a crime, most of the administrators will try to collect the information of intrusions as a proof of the crime.

As a solution to jamming, the backup router should be activated to control the network congestion. Network firewalls can also be used to filter unwanted messages.

- **Malicious softwares:** These are the softwares, which enters the system and creates a malfunction in the system. It can be a virus, worm, spyware, so on.

Malicious softwares can intrude into the system from websites, files, emails, messengers and so on. Some of the malware is hooked on to the valid software system too.

Security systems can use antivirus software to protect the system. Scanning of the entire system can be performed periodically to protect them. Necessary care must be taken when external devices are connected to the system.

- **Sniffing:** These are the applications, which are majorly designed to read and collect the network data. This data can be used to analyse the network vulnerabilities. These applications are also called as sniffers. Sniffers will collect the network packets and checks for credential information. This information can be used to perform illegal activities.

Cryptography is an important solution for the sniffer attack. Even though information is collected, it cannot be processed, since it is in the unreadable format.

- **Identity theft:** It is a kind of theft of identity of users.

Some of the identity thefts are as follows:

- Theft of username and password
- Theft of identity and address proofs
- Theft of photos

The information which has been stolen may be used for illegal activities, Such as identity proofs are used to produce SIM cards in our names without our notice. Most of the identity thefts are unknown to the offender until it comes to lime light.

Safeguarding from such activities majorly depends on the individual attention only.

Few of the safeguard techniques are:

- Never write confidential information on any piece of paper which can be accessed from public places.
- Never take the photographs of your passwords to remember.
- Never disclose personal identities to anyone.



Self-assessment Questions

- 1) “A SIM card is procured using my name but I did not know about it until I got a call from IT security team”. The above mentioned statement is valid for which kind of security threat?
 - a) Cryptography
 - b) Spoofing
 - c) Identity Theft
 - d) Malicious Software's
- 2) Which of the following security threat is used to collect and analyse the network information?
 - a) Sniffing
 - b) Identity Theft
 - c) Brute Force attack
 - d) Spoofing
- 3) “All the employees of my organisation have got a mail saying that you have won 10 Cr ₹ as prize money please gives us your bank details”. Such mails come under which of the following security threat?
 - a) Identity Theft
 - b) Hacking
 - c) Malicious Software's
 - d) Sniffing

3.1.3 Desktop and Server Security

Desktop security is not just protecting the desktop physically. Desktop security has its own role in an organisation's overall security. Most of the organisations protect their servers and network but give less importance to desktop security. A small compromise in the desktop security can reveal most critical information about the organisation.

It is advised to follow the security principle to protect desktop from intrusion effect. Some of the security measures are:

- Update antivirus and operating system periodically to get security from new threats to information security.
- Never open emails from unknown sender and never reply to them unless its authentication is confirmed.
- Use most complex password to access the system and change it periodically, so that it becomes difficult to guess the password. Never include personal information in your password.
- Always share the files with password protection and share the password with the receiver to open the file in more secured fashion (by using cryptography).
- Keep back up for all the information on the desktop in most secured location.
- Periodically perform security audit to all desktops of the organisation to check for security violations.
- Insure the device for physical damage.

Server Security: Most crucial applications and databases are stored on the servers. All the users need connectivity with the servers in different possible ways. An intruder can penetrate into a server and grab all the secured information; hence it needs very high level of security.

It is advised to follow the below listed security principles for server security enforcement:

- Update antivirus and operating system for more advanced security mechanisms to protect the server.
- Use different authentication measures to authenticate the server other than a simple username and password. It can be employed with secure shell (SSH) authentication system rather than normal authentication.
- All the communication from the server are encrypted and decrypted at valid source and valid destinations only.

- Configure server with most advanced backup and recovery concepts, so that the backup problem will not occur.
- Use virtual private networks (VPNs) for communication with servers from a remote system.
- All the ports through which server can be reached must be configured with application firewalls
- All the network paths which reach to the server must be secured with network firewalls.
- All the documents that are saved in the server must be password protected. If they are encrypted it could be much safer.
- Strong security policies must be implemented for server communication.
- Privileged user must be double authenticated before allowing them to communicate with the server.
- Conduct internal and external security audits to periodically check the security violations and glitches.
- Verify all the security certificates of organisation periodically.
- Never keep most secure application of the server in a demilitarised zone.
- Reduce network traffic towards server by using multiple proxy servers.
- Create multiple active directories to protect sharable and non-sharable resources of the server.
- Never allow a user to connect external storage devices without an administrator approval.
- Never install software whose authenticity is not confirmed.
- Physical security should also be employed in the place, where servers are installed.
- Insure the server for physical damage.



Self-assessment Question

- 4) “I want to access my secure information stored in my organisation server from my home”. Which of the following methods would allow me to do it by following all security basics?
- a) Keep organisation data in demilitarised zone
 - b) Copy all server data in your desktop and carry it home
 - c) Connect your server by using virtual private networks
 - d) It is impossible for you to access you files from home

3.1.4 Firewalls

Most of the networks are highly secure within the organisation. Whereas, internet security is unpredictable, allowing packets or messages from the internet directly to the organisation network is not safe. A security shield or barrier is required between trusted and untrusted network as shown in the figure 3.1.1. Firewall plays the role of the security barrier between secure and unsecure network.

A firewall is a software or a hardware filter that filters the packets from external network based on the predefined conditions specified by the organisation security team/experts.

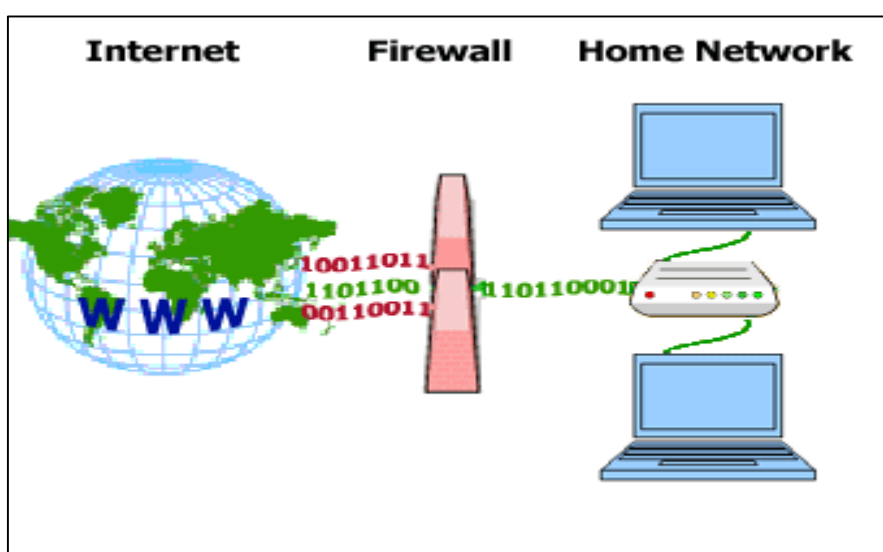


Figure 3.1.1: Working of firewall

A firewall is a security component, which acts as a filter between the organisation and the outside world.

A firewall is a software program or hardware component, which protect the organisation data from intruders or malicious codes or threats based on the rules specified. These rules are specified by the information security officer or data administrator.

Based on the filtration rules, either it will allow the packets to enter inside the organisation's network or deny the packet which has not satisfied filtration rules.

To work with the firewall effectively, an organisation must setup their network in such a way that the entire data flow (incoming or outgoing) should happen only through a firewall only.

Firewalls can perform the different functionalities to secure organisation network and data.

Various functionalities are:

- Act as a potential barrier to accept or reject the packets from a private network.
- It provides powerful authentication to the user.
- Important information about the organisation, such as network components, network structure or topology, computer names are hidden by firewalls.

Features of firewalls:

- All the traffic must pass through the firewall for providing right and tight security.
- The firewall has a capacity to protect itself from the intruder.
- Firewall implementation takes input from risk analysis factors (which will be covered in module 4).
- Firewalls are the crucial components for building VPNs.

Limitations of firewalls

- It avoids only external threats not internal.
- Firewall can't stop the accessing of websites with malicious codes by internal users.
- It will not be used for decision making process.
- It cannot protect the organisation from threats, if the organisation's policy is too complex.
- Firewalls cannot stop physical intrusion.
- The firewall acts as a congestion point if it has a poor implementation.
- Firewalls cannot prevent the intrusions, if rules are not clear.

Based on the working and processing modes, firewalls are categorised into five types. They are:

- Packet filter
- Dynamic packet filter
- Application gateway
- Circuit relays
- Personal and/or distributed firewalls

These firewalls work on various layers of the OSI reference model, as shown in the figure 3.1.2.

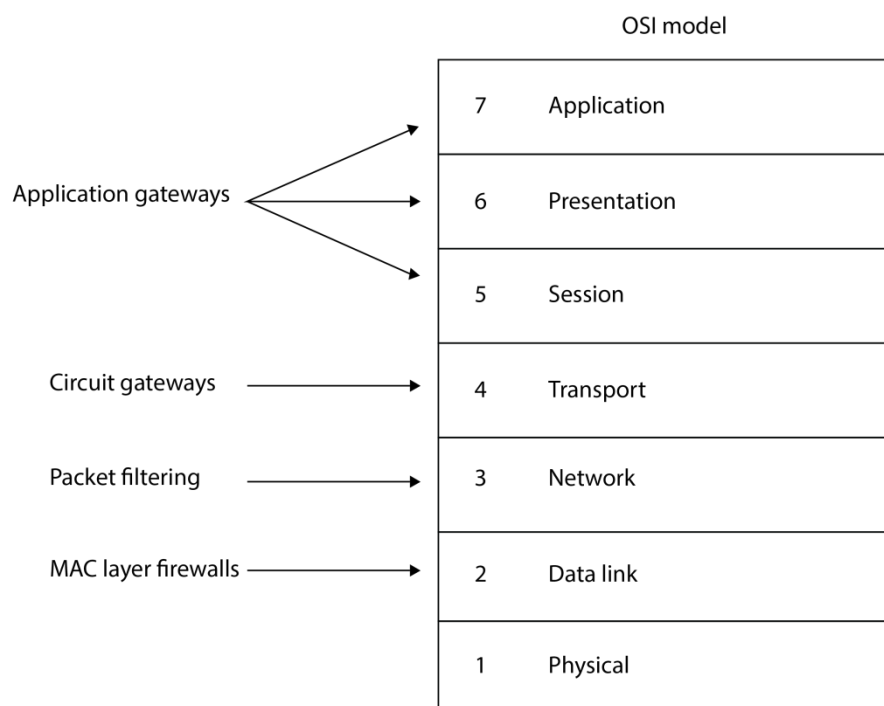


Figure 3.1.2: Types of firewall

(i) Packet Filter

It is also known as a simple filter firewall. A packet filtering firewall operates at the router and examines the packet information received. It checks the header information to allow or drop the packet based on the filtration rules. So, it is also known as a static filter firewall.

To allow or restrict the packet, the firewall uses the following packet information:

- Destination address
- Source address
- Type of packet (TCP OR UDP)
- Listening port numbers
- Direction of message (incoming or outgoing)

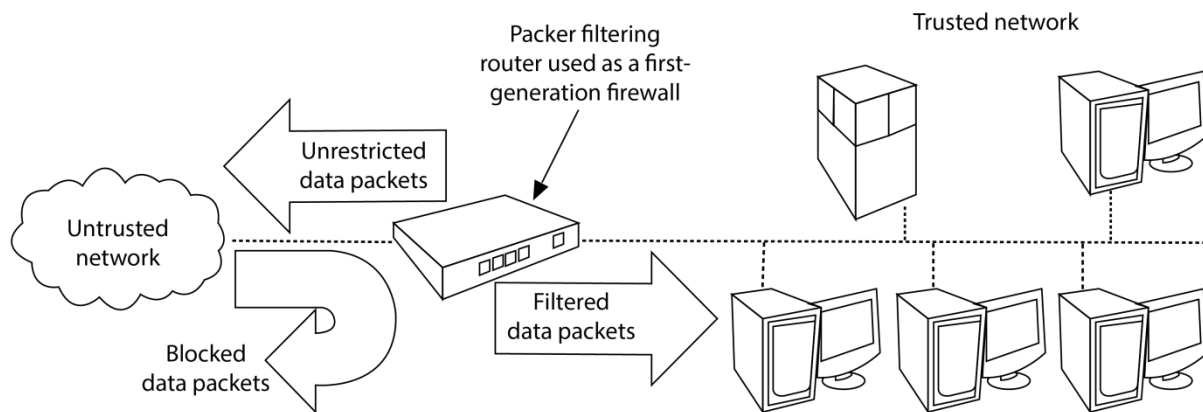


Figure 3.1.3: Packet filter firewall

As shown in the above figure 3.1.3, if any packet is entering an organisation's network, then the firewall checks the header information and compares it with specified rules. If the packet satisfies the rules, then it will allow the packet, else it will drop the packet.

Example: If the organisation network IP address is 200.1.100.x. The filtering conditions for packet filter firewall can be framed as follows:

Any packet from the source 28.28.28.x are allowed

Any UDP packet from source 12.1.x.x. are allowed for 200.1.100.1 to 200.1.100.36

By considering the above filtration rules, the packet filter takes the decision as shown in the table 3.1.1.

Table. 3.1.1: example for working condition of packet filter

Source IP	Destination IP	Type of Packet	Accept/Reject
28.28.28.1	200.1.100.220	TCP	Allow
12.1.1.1	200.1.100.126	UDP	Reject
28.27.28.120	200.1.100.3	TCP	Reject
12.1.23.67	200.1.100.28	UDP	Allow

**Advantages:**

- Implementation cost is very less, since it uses current network routers.
- They are easy to install.
- They are faster than other firewalls because they perform fewer evaluations.

**Disadvantages:**

- Packet filters do not understand application layer protocols.
- Packet filtering routers are not very secure if the rules set in it are not strong.
- Can't differentiate good and bad packets.
- Implementing the filtration rules is difficult.

(ii) Dynamic Packet Filter

It is also one of the packets filtering firewall. The static filtering firewalls only see the header information, whereas dynamic packet filter firewall not only sees the header information, but also sees the previous packet received history from the same source and whether the packets are allowed inside the network or rejected.

Dynamic packet filtering firewall filters the packets based on:

- Administrative rules, which clearly outlines the allowed ports and IP addresses.
- Connection state and previous routing history of packets from the same source that have entered through the firewall.
- Packet content and source information.

Dynamic packet filtering is better than the static filtering because the level of security is more than a static packet filtering firewall. It also provides a closer look to the packet to see the content.

(iii) Application Gateway

As the name suggests, it works on application, presentation and session layers of the OSI reference model. Other names of the application firewalls are application level firewall, application gateway or proxy server. This will be installed on a separate computer, where the organisation-filtering router is not installed, but it works along with the filtering router. Generally, the proxy server provides cache services between the web server and website users as shown in figure 3.1.4. Proxy server stores all recently used objects on a website.

Proxy servers always request the document from webserver on behalf of the client request. All the requests of the user are diverted to the proxy server, which verifies the validity and authenticity of the request by using the filtration rules. If it is satisfied, request headers are flipped and replaced with new headers. This process of flipping the header will not allow intruders to know more about original source details. If an intruder tries to attack the proxy server, they merely fail because it is connected to packet filter.

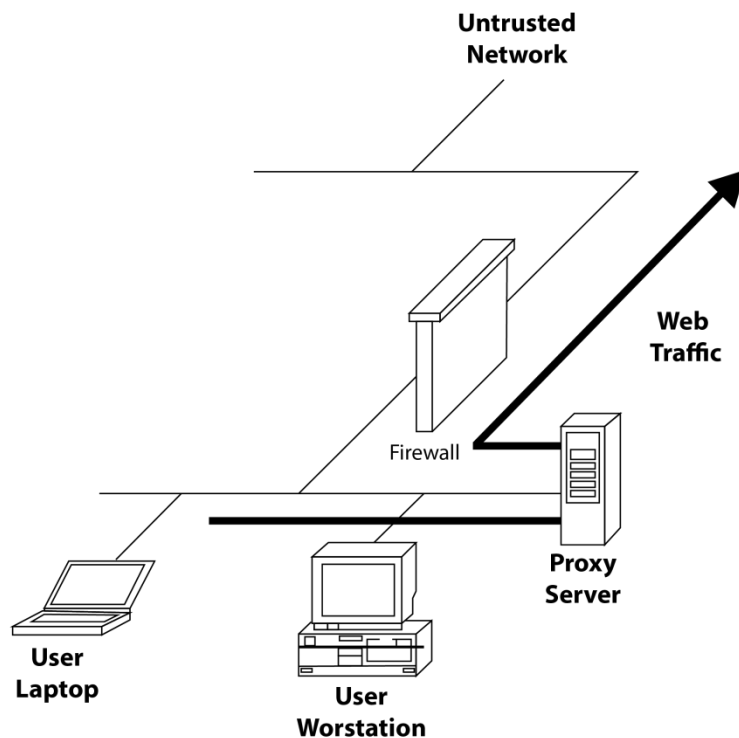


Figure 3.1.4: Proxy server firewall

In most of the organisation's networks, the proxy server is always kept in the Demilitarised Zone (DMZ), which is an exposed zone of an organisation's network to the outside world. It can also be considered as an intermediate zone between the trusted and untrusted network. Proxy server never gives the chance to any service to directly communicate with data server and web server. To secure the organisation's internal network, many organisations are implementing the filtering firewalls behind the proxy server.

An application level firewall provides more security for an organisation's data with the concept of proxy. Most of the eCommerce sites are using the proxy server concept. The problem with this firewall is that it works for limited protocols and reconfiguring based on the new needs and requirements are difficult.

(iv) Circuit Relays

Like a packet filtering firewall, the circuit relays or firewall does not work on filtering of data packets based on specified conditions. The main work of this firewall is to validate the network connections. Circuit relays avoid the direct network connections between the processes of different networks. If the connections are between valid sources, then it creates the tunnels on each side of the firewall to connect the processes.

Through the tunnel, it allows data only from authorised connections as shown in figure 3.1.5.

According to the John Wack, he describes the operation of a circuit gateway as follows: “A circuit level gateway relays TCP connections, but does no extra processing or filtering of the protocol”.

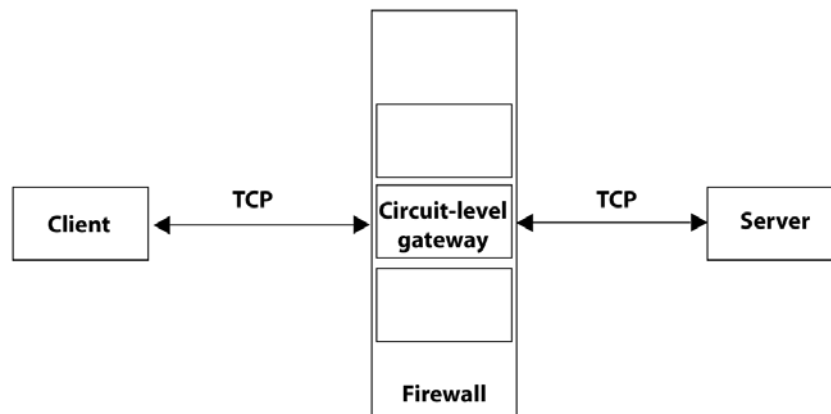


Figure 3.1.5: circuit gateway

For example,

If a Telnet application process can be bound to circuit level gateway, then it allows only data packets which belong to another authorised Telnet application.

(v) Personal and/or Distributed Firewalls

Many experts argue that firewalls are not needed if cryptography is introduced for data transmission. They believe that firewalls create unwanted transmission hurdles. Many computer experts say that firewalls are needed, but their usage should be left in the interest of the users of it. To support the above statements, a personal firewall is introduced. They are also known as desktop firewall. It exists in the form of software or hardware. It executes in the background.

This firewalls act as secondary protections and most of them do come along with the operating system. Personal firewalls execution is completely in the hands of its users.

The main aim of personal firewalls is to protect from internal threats, since most of the intrusive activities are within the organisation. Even though the firewall is personal, its activities are monitored by using a centralised system so it is also called as distributed firewall. Centralised system will change the rules of the personal firewall repeatedly.

However, personal firewalls act as a congestion points for your system, if the network speed is more than the execution speed of the firewall.

Hence every organisation must use the firewalls based on their needs and must provide continuous awareness programs to the employees to work with firewalls.



Self-assessment Questions

- 5) Firewalls protect the organisation's network from?
 - a) Worms and Virus
 - b) Natural Calamities
 - c) Connecting to the outside and inside network
 - d) Unauthorised persons logins from private networks
- 6) An OSI reference model consists of several layers of process to implement the network. If anyone wants to protect their network using firewalls then the proxy firewall implementation can be done on which layer of the OSI reference model?
 - a) Network Layer
 - b) Physical Layer
 - c) Application Layer
 - d) Data Link Layer
- 7) An IP packet consists of several information fields in the header portion. Among those fields____ is the address of the receiving computer or device.
 - a) Source Address
 - b) Destination Address
 - c) Offset
 - d) Time of Leave
- 8) Which of the following firewall works on predefined rule set?
 - a) Circuit Level Firewall
 - b) Packet Filtering Firewall
 - c) Proxy Firewall
 - d) Personal Firewall

- 9) Which of the following is the false statement about the firewalls?
- a) Firewall works based on organisation specified rules
 - b) Only through firewall traffic is allowed from outside to inside or vice versa
 - c) It hides the organisation network details to the outside world
 - d) Different firewalls work on different layers of the OSI reference model

3.1.5 Techniques of Password Cracking

Password plays an important role in many cases. Most of the organisational information will be bound with single authentication mode using username and password. So, if anyone cracks or hacks the password, then the valuable information about the organisation or users will be in their hands. Attacks inside the organisation are in many forms like spoofing, Denial of service (DOS) attack, Distributed DOS attack, etc., which will damage or cause a threat to the organisation information systems or networks.

Password cracking is the attack where intruders use this technique to enter the resource or system of someone. Using this technique, anyone can collect any type of information from password-protected resources like mobiles, laptop, emails, desktops and servers.

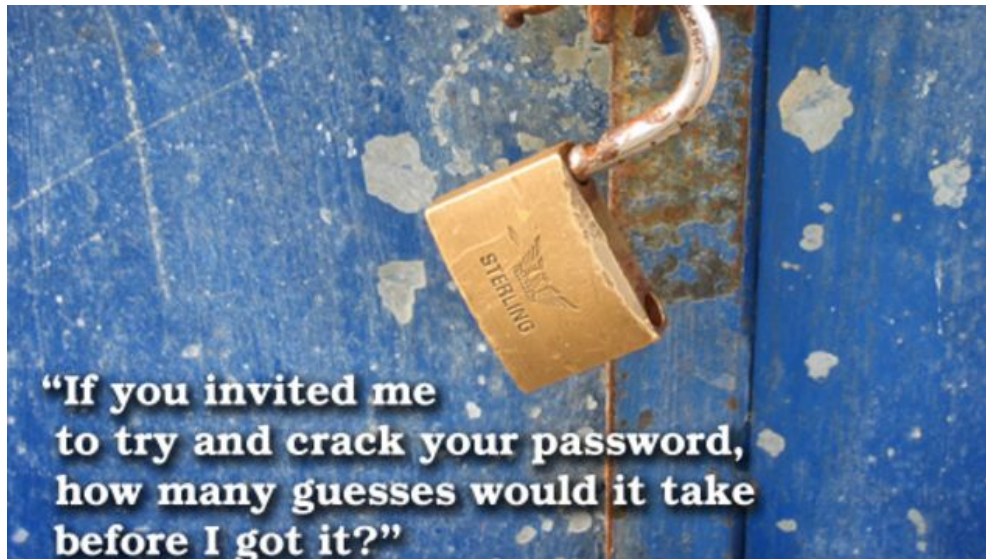


Figure 3.1.6: Password cracking

As mentioned in the above figure 3.1.6, do not give the chance to others to guess or to think your simple passwords. Try to use and create complex passwords, which others cannot crack.

Types of Password Cracking Techniques:

Cracking of the password is not simple, if password strength is high or complicated. To hack or crack the password, hackers use different techniques. Like brute force attack, dictionary attack, social engineering attack, phishing attack, rainbow table attack as shown in the below figure 3.1.7.

Brute Force, Dictionary Attack, Rainbow Table

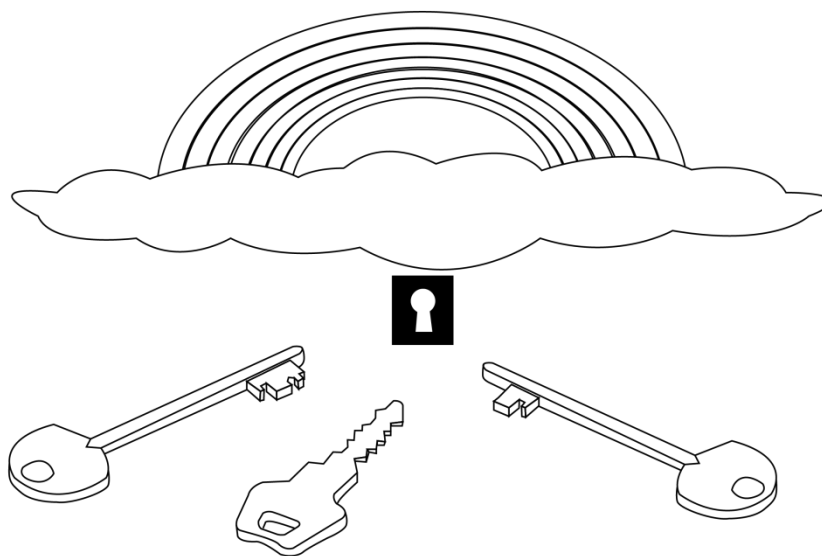


Figure 3.1.7: Password cracking types

1. **Guessing:**

Hackers will guess the password of others to use their resources. This is one of the most commonly used techniques to identify the passwords of any password protected resource. If the hacker is close to the person, then it is very easy to hack the victim resource using the combinations of personal information.

To avoid easy hacking, it is advised to not to keep the person names, surnames, date of birth of their family members, place of birth, marriage dates, important person names, any known information to others, or mobile numbers to list a few.

- a. It is always advisable to not to write or mention the passwords in the public access places like writing in notebooks, keeping the information below the keyboards, pouches, etc.
- b. Do not use the same password for many authentication purposes.

2. Brute force:

Brute force attack is the most commonly used technique to hack the passwords, but it is a time consuming attack. It takes a long time to identify the password of resources. In this attack, the hackers use the combination of capital and small case letters, numbers and special characters. There may be a chance for hackers to retrieve the password.

The solution for this attack is:

- a. Try to use the combination of upper case and lower case characters, numbers and special characters.
- b. See to that the length of the password should exceed more than six characters. If the password is long and complex, then it will take some years to crack it.

3. Phishing attack:

Phishing is another type of attack to get the account details of the individuals or organisations. Attackers create the false sites to get the required credentials. The hackers create fake sites that are similar in kind to that of the original sites to hack the data.

The solution for this one is:

- a. Check the Uniform Resource Locator (URL) information, when providing the personal information. This is because, the false sites may differ with jumbling of the characters from the original site

Example: If the users want to check their mails on the www.gmail.com website, The URL for the phishing sites will be almost similar to original websites differs by very few characters *for example*, www.gmaili.com.

- Proper security perimeters should be used to identify these kind of the problems.
- Do not provide the data for unknown sites.
- The files or software's from unknown senders or from popup menus should be never downloaded.

4. Social Engineering:

This is the latest technique used by the hackers to collect the information. In this technique, they will call or send some fraud mails to individuals to acquire the data or facts. There are many victims of this fraud. Hackers make a call to the persons to collect their debit or credit card and some important information through which they will get

some benefit. Nowadays, most of us are receiving the mails saying that some verification mail or prize winning mails, etc. If we respond to such kind of the mails, then the attackers gain the useful facts.

To save themselves from this attack, the users can do the following things:

- a. Never give your credit/debit/personal information to unknown users.
- b. If anyone asks to collect your information, then try to collect their identity information and verify them whether they are the right or authenticated users before providing the details.
- c. Do not provide personal information to prize claiming mails.

5. Rainbow table attack:

The hacker uses a table in this method, which consists of the hash values for each and every character combination. Basically when a user provides a password, it immediately encrypts into hash values using cryptographic hash functions. In this attack, the attacker will create the rainbow table with all possible combinations to retrieve the person's or organisation details. But the drawback is that the table needs more memory space to store it.

For example:

- If a password consists of 14 capital letters, then for storing the combination of these characters hashes table uses 0.6 GB of memory space.
- If a password consists of 14 characters with the combination of capital and small case letters, numbers, special characters, then in this case memory required is 64GB to store the hash table.
- The countermeasure for this one is the creation of long and complex password, which will take a long time and lots of resources to crack the password.

6. Dictionary Attack:

Most of the users have the habit of using dictionary word combinations as passwords. To crack such passwords, a dictionary attack is used.

A dictionary attack is a method which uses a program with a list of words from dictionary to try/guess the password. Right now, most of the hackers are using the advanced programs which use a combination of alphanumeric words to hack the passwords.

Anyone can be safe from this attack by using complex passwords which are very difficult to guess.

To protect the password from hackers, the organisation or individual must use the above techniques to save their data.



Self-assessment Questions

- 10) Ram wants to hack the user credentials for his benefits so, he created a fake site for the original site. This attack is known as?
- a) Rainbow Table Attack
 - b) Phishing Attack
 - c) Social Engineering Attack
 - d) Salt Attack
- 11) A table consists of hash values for every combination of characters, numbers and symbols. The attacker uses this table for hacking the information. This attack can be called as_____?
- a) Rainbow Table Attack
 - b) Dictionary Attack
 - c) Social Engineering Attack
 - d) Phishing Attack
- 12) Collecting the credential information over the phone call by calling the victim is treated as _____.
- a) Dictionary Attack
 - b) DOS Attack
 - c) Spamming Attack
 - d) Social Engineering Attack
- 13) Sam wants to protect himself from brute force attack. Which of the following solution is better for him?
- a) Never provide the information over the calls
 - b) Never respond to mails
 - c) Create strong and complex passwords
 - d) Install strong security measurements in the system

3.1.6 Keyloggers

Persons are very curious to get the personal information like the nature of their job, income and other information. Whether employees are using the information assets for the right cause or not is unknown. To get these details, most of the individuals are using keyloggers. Keyloggers are available in both hardware and software that can be connected or installed into the system. It is also known as keystroke logger or system monitor.

The main work of keylogger is to monitor and store the information about the keystrokes performed by the user in the system. It stores the information either in a file or sends a mail to the concern user. It is just like a call recorder in the mobile, which records the complete conversation.

With these keyloggers, parents can monitor the activities of their children's. As it comes in a software and hardware form, anyone can use them in any format. By using keyloggers, hackers can know the behaviour of others, i.e. the nature of activities. It also plays a vital role in protecting the organisation data, because it helps the management to keep track of activities done by various users or employees in the organisation. It even helps the top management people to implement the access control registers.

(i) Hardware Keyloggers

Hardware keyloggers are the hardware devices that are used to collect and store the keystroke information of the users. Hardware keyloggers are attached to any slot of motherboard, USB, PS2, etc., now a days they are available in wireless fashion.

Hardware keyloggers are the external hardware devices connected to the system. They can be connected through keyboard port or through external devices as shown in figure 3.1.8. They have some internal memory to preserve the key strokes. They are very difficult to detect by the antivirus software's and scanners. Most of the hardware keyloggers are independent of operating systems, hence they are most preferred.



Figure 3.1.8: Hardware keylogger

(ii) Software Keyloggers

Software Keyloggers are the software's installed in the system to collect and transmit the key stroke information of the users to others. Some organisations consider them as malware because they collect sensitive information. Some organisations consider them as monitoring tools to keep an eye on the activities of employees

The keylogger software run as a background process which stores the keystroke information in the specified file. Few keylogger software allows the user to mail the content automatically to the pre-specified mail address. When a user installs the keylogger software in the system, it deploys two files, one is .DLL and the other one is an .exe.DLL. They will have all the code to store and record the data, .exe is meant for executing the code.

If anyone browses their personal information through an unknown sources can detect keyloggers using following two methods:

- Disable the keylogger by using task manager (if the keylogger is running in visible mode).
- If keyloggers are running in invisible mode, then use antispysware. It can identify and abort the execution of keyloggers.



Advantages:

- Software keyloggers are used by an organisation to check the trust level of the employees within the organisation to fix the organisation policies.

- Hardware keyloggers can be connected to the system in such a way that the others cannot notice it.

**Disadvantages:**

- Keylogger in the wrong hands may reveal the personal information to the intruders.
- Undetectable keyloggers introduced through web browsers will reveal the personal information of all the employees, when they use their personal information to access bank account details, mail details and credit card details.
- As hardware keyloggers are mostly undetectable by spyware and scanners, the intruders are using this widely to grab sensitive information.

(iii) Implementation and Security of Keyloggers

There are many factors which govern the implementation of keylogger such as:

- Operating system in which it has to be implemented
- Different hardware component with which it should interact
- If it is hardware keylogger, where it should be connected

Most of the keyloggers are implemented as a part of internet browser by using JavaScript coding. They use a few techniques for keylogger implementation. One among that is hooking, hooking is a software design technique that takes all the information which has been typed by using keyboard and re-transmits them to the original destination. As the information reaches to the desired location, even the user of the system or the operating system will not be notified with the execution of the keyloggers.

Most of the keyloggers which are implemented in the organisation do exist in the form of client and server processes. The client collects the information from the employees of the organisation and arranges the data in the required format and sends it to the server. The server will collect the data and check for any violation of security policy. If the activity of any employee appears to be suspicious, then necessary action can be initiated on them with sufficient proofs. This helps the organisation to protect their information security policy. Most of the organisations will inform this policy details well in advance to the employees during the induction process. If they feel that the concern site needs to be blocked, then it will be introduced in the Access Control List, so that it will block the user access.

To safeguard the system from the keylogger (if is not used for monitoring) it is advised to:

- Use anti-spyware software's
- Check the unwanted process executions
- Disable all the unwanted ports of the system
- Check for extra hardware's attached to the system before using it
- Keep an eye on the files transferred through internet



Self-assessment Questions

- 14) A hardware keylogger device is used to ____.
- | | |
|---------------------------------------|---------------------------------------|
| a) To crack the password | b) To stores the hitting of keys data |
| c) To delete the data from the system | d) To crash the system |
- 15) Which of the following method will be used to implement the software keylogger?
- | | |
|------------|--------------|
| a) Hooking | b) Thrashing |
| c) Hashing | d) Sniffing |



Summary

- System security is a process of securing the organisational data from the intruders.
- System security is employed to safeguard the confidentiality, integrity and availability of the organisational resources.
- There are many threats to the security of information, they are hacking, spoofing, spamming, sniffing, jamming, identity threat and malicious software's though which intruders will penetrate into the system.
- The server is the critical point where most of the important software and data resides. Hence securing the server from attackers is a very important task for any organisation.
- Even if the server of the organisation has strong security, since the desktop is connected to the server, the security of the server is still at risk.
- To ensure the security of organisational network, only valid and authenticated users can be permitted through firewalls.
- Packet filtering firewalls will filter all the packets which are not following the security rules.
- The circuit relays firewall creates a tunnel mode transmission for all the packets to avoid packets flow in different network paths.
- Application firewalls create a proxy server to avoid interactions with the original server.
- Keylogger is used to track the keystrokes of the users.
- Software and hardware keyloggers are two different varieties of keyloggers available.
- Software keyloggers are installed in the system. They store the keystrokes in a file and transmit them through a mail.
- Hardware keyloggers are hardware devices connected to system to store the keystroke information.

- Many organisation set the security policies for employees based on the data extracted from keyloggers
- Password cracking is a method of identifying the password of the user.
- Phishing, guessing, brute force, dictionary and rainbow table techniques are used for password cracking.



Terminal Questions

1. What is desktop security? Explain the basic principles of desktop security.
2. Compare and contrast various types of firewalls.
3. Explain in detail about software keyloggers.
4. List and discuss the techniques involved in password cracking.
5. Mention the differences between packet filtering and application gateways.
6. Briefly explain the uses and working of proxy server.



Answer Keys

Self-assessment Questions	
Question No.	Answer
1	c
2	a
3	c
4	c
5	d
6	c
7	b
8	b
9	b
10	b
11	a
12	d
13	c
14	b
15	a



Activity

Activity Type: Offline

Duration: 45 minutes

Description:

With increasing complexity in the world of information security, firewalls have become an integral part of the security of an organisation. Discuss the firewall design in this context.

Case Study

Myfootware Corporation wants to enter into an online business. All the products they own are listed on their web site. Every customer can see all the listings of products available, but if they want to purchase the products, then they must register themselves by using their personal information. As an introductory offer, they announce an offer that anyone can get 75% off, if they register themselves along with 10 other people's valid email ids and phone numbers.

Registrations started flooding and they got a huge amount of data with them. They found that many other intruders are stealing this information. Now, the organisation thought of building a strong security system to protect the users' details, which they have collected. An administrator was appointed to protect this information with a simple password protection system.

As Myfootware Corporation has entered the online business very recently they have no firewalls or keyloggers implemented in their system. More than 200 people were working in the online business model and all of them have direct access to server deployed.

After observing massive business for a month, the organisation decided to extend the offer for 2 more months.

Discussion Questions:

1. Why the organisation is collecting 10 email ids and phone numbers of customers' friends?
2. What are the possible security threats the organisation may encounter?
3. If you are the administrator for this organisation, what could be your recommendations for establishing the system security?

Bibliography



e-References

- *Security measures*. Retrieved 18 Jan, 2017 from <https://www.digitalocean.com/community/tutorials/7-security-measures-to-protect-your-servers>
- *Password Cracking*. Retrieved 18 Jan, 2017 from <http://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-1-principles-technologies-0156136/>
- *Keystroke Logging*. Retrieved 18 Jan, 2017 from http://adventuresinsecurity.com/images/Keystroke_Logging.pdf

Image Credits

- Figure 3.1.1: <https://4.bp.blogspot.com/d6oCkuR6hvc/V7cWfmSizwI/AAAAAAADYc/FyGYobzz8oIIFubi3dXrFMTXp15Hv4CwgCLcB/s640/Personal%2Bfirewall.gif>
- Figure 3.1.2: http://images.slideplayer.com/16/5156324/slides/slide_39.jpg
- Figure 3.1.3: http://images.slideplayer.com/15/4789146/slides/slide_42.jpg
- Figure 3.1.4: http://windowsitpro.com/site-files/windowsitpro.com/files/archive/windowsitpro.com/content/content/15602/figure_02.gif
- Figure 3.1.5: <http://flylib.com/books/4/178/1/html/2/images/fig9-1.jpg>
- Figure 3.1.6: https://i.kinja-img.com/gawker-media/image/upload/s--lh-RI5bF--/c_fill,fl_progressive,g_center,h_358,q_80,w_636/18ixp7q66cpy2jpg.jpg
- Figure 3.1.7: <https://image.slidesharecdn.com/passwordhacking-140319221812-phpapp02/95/password-cracking-10-638.jpg?cb=1395267803>
- Figure 3.1.8: <http://www.geekandblogger.com/detect-keylogger-software/>



External Resources

- Whitman, M. E., & Mattord, H. J. (2003). *Principles of information security*. Boston, MA: Thomson Course Technology.
- Stallings, W. (2000). *Network security essentials: applications and standards*. Upper Saddle River, NJ: Prentice Hall.
- Pachghare, V. K. (2009). *Cryptography and information security*. New Delhi: PHI Learning.



Video Links

Topic	Link
Information Systems security	https://www.youtube.com/watch?v=8caqok3ah8o
Firewalls	https://www.youtube.com/watch?v=OQyXMYh6qLo
Password Cracking	https://www.youtube.com/watch?v=97CdJFyAv1s



Notes:



Chapter Table of Contents

Chapter 3.2

Virus, Worms, Malwares and Spywares

Aim.....	149
Instructional Objectives.....	149
Learning Outcomes.....	149
3.2.1 Introduction.....	150
3.2.2 Viruses.....	150
(i) Types of Viruses	152
(ii) Prevention.....	154
(iii) Impact of Virus on IT System	155
Self-assessment Questions.....	156
3.2.3 Worms	157
(i) Types of computer worms.....	157
(ii) Symptoms of a Computer Worm.....	159
(iii) Computer Worm Removal	160
Self-assessment Questions.....	160
3.2.4 Malwares	161
(i) Types of Malware	161
(ii) Impacts	162
(iii) Prevention.....	163
Self-assessment Questions.....	164
3.2.5 Spywares.....	164
(i) Types of Spyware.....	164
(ii) Causes	165
(iii) Effects	166
(iv) Prevention	166
Self-assessment Questions.....	167
3.2.6 Windows Registry	167
(i) Window Security Model.....	168
(ii) Registry Root Keys	169
(iii) Windows Registry Values	171
(iv) Registry Key Security	172
(v) Access Rights.....	173
Self-assessment Questions.....	174

Summary	175
Terminal Questions.....	176
Answer Keys.....	177
Activity.....	178
Case Study	179
Bibliography.....	180
e-References	180
External Resources	180
Video Links	181



Aim

To familiarise the students with the basics of window registry and the preventive measures for virus, worms and malwares, to make the system more stable



Instructional Objectives

After completing this chapter, you should be able to:

- Explain various types of virus and its preventive measures
- Classify the types of computer worms and prevention techniques for worms
- Describe impacts of malware on the computer and their prevention methods
- Explain various types of spyware and their prevention
- Illustrate how window security model enables you to control the access to the registry key



Learning Outcomes

At the end of this chapter, you are expected to:

- List the different types of virus
- Summarise on consequences of virus attacks
- List the consequences of worm attacks
- Recognise malware and how to prevent them
- Recognise causes and effects of spyware
- Outline how window security model enables you to control access to the registry key

3.2.1 Introduction

Information being transmitted over the network can encounter several attacks. Any system that is not protected can be compromised within few seconds of its connection over the network. Such attacks or infection can be from viruses, malwares, spywares, adwares, worms, Trojans, etc. Though all of these are malware, their functionalities are different. These malicious softwares behave differently.

In this chapter, we will learn about various types of attacks such as viruses, worms, malware and spyware and its impact over the system and its information. Finally, we will brief about windows registry which will be helpful to make system more stable.

At the end of this chapter, the students will be able to differentiate between various attacks. Students will also learn that not all these attacks are the same. Each of them has their own impact over the system. Students will also learn about how to prevent their system from these attacks. Students will be able to analyse the reasons for adverse effect on the system and can strengthen it by using windows registry.

3.2.2 Viruses

Computers can do many things, from the creation of a simple application like word document to complex application like robotics. One can design the applications for a good cause and other can create for a bad cause. Now a day's most of the people are designing software to create threats to data or system.

A virus is a program code, which spreads and attaches it to any program. This affected program damages all its associated files. Sources for the virus are emails, USB, CD/DVD, etc. There are various damages caused by virus. It has the potential to damage several systems at a time, which are connected in a network.

A program that contains a virus is known as infected file. The infected file is the major source to spread the virus. When anyone tries to use this infected file, then immediately virus spreads into their system. A computer virus alters the program content and creates the duplicate copies of same program by altering the permissions of the files.

Examples: Blaster Worm, Sasser, code red, Anna Kournikova worm Melissa, I love you, etc..

During the lifetime of virus, it will go through four stages, as shown in figure 3.2.1

They are as under:

Dormant phase:

In this phase, the virus is idle, i.e. it will not perform any kind of the action. The virus will be activated by any of the following events:

- Pressing of any key by the user
- Execution of supporting file or program inside the system
- Specific time and date
- The capacity of the disc exceeding the given limit

Propagation phase:

This is the stage of virus, in which it creates the similar or replicated copies to multiply itself. These copies attach to other programs or some parts of the system. The infected files or programs having the identical copy of the virus again enter into propagation phase to occupy the complete programs or files or system components.

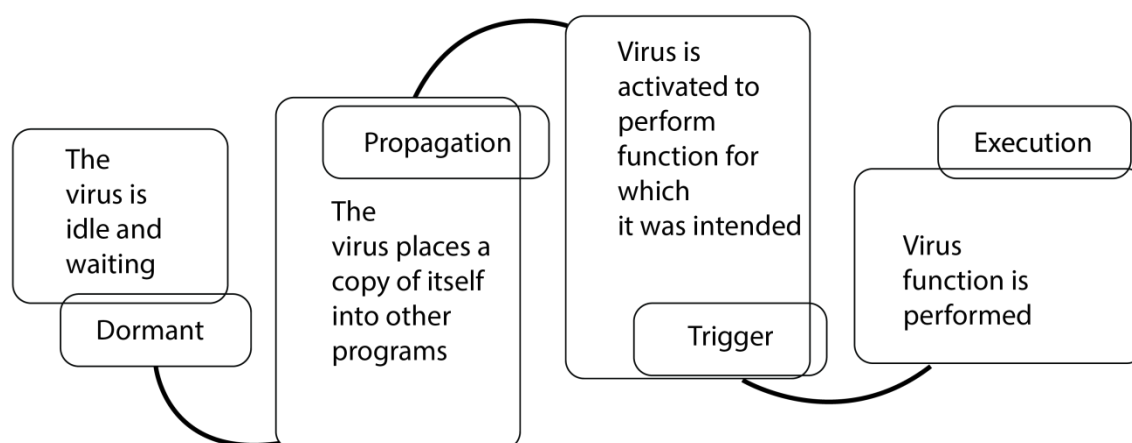


Figure 3.2.1 Phases of virus

Triggering phase: After the dormant phase, the virus gets activated at this level. Few user activities and infected file execution are main causes for virus activation.

Execution phase: In this phase, the virus starts working by deleting files, erasing some content of infected files or making the system obsolete.

These above stages of the virus are also known as the life cycle of the virus. In this pattern, the virus crosses all the stages to complete the predefined tasks.

(i) Types of Viruses

Various types of viruses are:

- **Boot Sector Virus:**

The boot sector virus affects the boot sector portion of the system. It is a very dangerous virus, which we cannot completely remove. When the system is switched on, the very first section accessed by the processor is the boot sector. The virus takes complete control of DOS or Master Boot Record (MBR). Since it works on DOS AND MBR, it is highly impossible to remove it completely. It is very difficult to retrieve the data from the system once this virus attacks the computer.

If the system is infected with this virus, then users will get the error message “cannot boot now”. If the system shows this kind of the error message, then the user has to reformat the system, which will erase the entire data.

The main sources for boot sector virus are floppy disks and hard disks. A proper virus security scan should be done before assessing the external files.

Example: MrKlunky, Meve, Randex, Michelangelo and Stones

- **File Infector Virus:**

This virus is the most popular one. It attaches to the file or program by itself. When the infected file or program is opened, this virus starts its execution along with the program or file or application. Basically, these infected files are spreadsheets, game files, application or word document. When the user runs these infected files, first virus is executed followed by the execution of the file. The virus infects either .COM or .exe files.

Any antivirus software can easily detect this virus. So, it is recommended to install antivirus software to protect the data from virus and other types of threat.

Example: Jerusalem and cascade.

- **Polymorphic Virus:**

A polymorphic virus is different among the other viruses, because it encrypts itself and replicates continuously. Therefore, it is very difficult for any antivirus software to identify existence of this virus and search for its signature.

Example: HSFX virus, W95/HPS virus

- **Multipartite Virus:**

This virus finds different places or targets to occupy and starts attacking the files present over there. This virus spreads faster than other viruses. Basically, it works as a combination of boot sector and infected file virus. So, removing this virus is difficult using antivirus, so the only solution is the cleaning of boot section.

Example: Tequila, Ghostball

- **Non- Resident Virus or Transient Virus:**

The virus that will show the very minimum impact on the files and system performance is the non-resident virus. This is also known as a direct-action virus. It will not install or store in the system. It will attach to the file, if the infected file executes then it will search for similar type of files to infect. This type of virus' lifetime depends on the lifetime of the infected file. If an infected file is deleted, then this virus gets deleted along with the file.

Downloading files from the internet is one of the sources for this virus. By using any antivirus software, we can detect these infected files easily. The user has to delete the infected file to get rid of this virus after identifying the infected file.

Example: All executable viruses

- **Resident virus:**

It is also known as terminate and stay virus. It is one of the file infector viruses and resides in RAM memory. It executes itself in the system. The resident virus is a very dangerous and permanent type of virus, because even though the infected file gets deleted by the user, it will still exist in the system. As the name suggests it will reside in the system and infects all the files.

Example: Jerusalem

- **Macro Virus or Document virus:**

These viruses attach to the file or application which consists of macros. Macros are the small programs that help the user to perform a series of actions automatically when the macro runs.

Examples: Relax, Melissa.A, Bablas, O97M/Y2K.

- **Parasitic virus:**

This virus targets files of the operating system. The virus program has been designed in such a way that it appears as an operating system file. The Operating system cannot differentiate the virus file with the original file, hence allows it to execute.

Example: Jerusalem

- **Stealth virus:**

The files that are infected with this virus hide itself from antivirus software and operating system. This virus edits the file size, modifies date and a few other properties of the infected file in order to hide from virus scans.

Example: DOS virus

(ii) Prevention

A virus is a malicious code, which attaches itself to the files and damages it. Therefore, computer users have to implement the proper security mechanisms to safeguard themselves from computer viruses.

“Prevention is better than cure” so it is much wiser to use prevention techniques from viruses instead of repairing the systems or files.

The various prevention techniques are:

- Downloading the files from unknown individuals or sites should be avoided.
- Installation of proper antivirus software which will automatically identify the threats.
- Not responding to the mails from unknown senders
- Implementation of the security mechanisms tightly such as firewalls, intrusion, detection and prevention mechanisms to take care of systems as well as the organisational network.
- Copying of files from external sources into the systems without scanning should be avoided.

- Backup of files and data should be taken.
- Installation of updates as per requirements
- Enabling of security components, which comes along with the operating system software,
- Downloading of files only from the trusted or authenticated users. Avoiding of pirated software because they are the best sources to spread the virus.
- Using the antivirus softwares which will provide the total security in all aspects like system, Password, Internet, etc.
- Prohibiting unknown users to connect their devices to the system
- Making disks as write protected from others so that they cannot copy the information into the system.
- Using complex passwords to secure the system and permitting only authorised persons to use the system.

(iii) Impact of Virus on IT System

Viruses create small to large-scale problems to the individuals or groups. In the network, if a virus affects one system, it automatically spreads to the entire network, if the network is not properly secured. This can lead to financial and time loss.

Viruses, when it affects the system or file brings the following changes in the system:

- It will hack the important information from the system.
- Due to the virus attacks, some programs get corrupted.
- Few viruses completely delete the files or programs and its data.
- Most of the virus damages the boot sector, which will cause either to reboot the system repeatedly or to reformat the system by losing data.
- Few viruses will damage the important operating system files, making it inoperable.
- The Performance of the system will slow down.
- Some viruses will create the problem in restarting the system.
- Some of the viruses will create trouble while charging the system.
- Few viruses will blast the systems.
- Few viruses will interrupt the work of the user by sending unnecessary prompt or advertisements.
- Some of viruses change the file type from one format to another so that users cannot open the infected file further.



Self-assessment Questions

- 1) Which of the following is a property of virus?
 - a) It is a hidden program
 - b) It enters a computer without the owner's knowledge
 - c) It can modify data or computer programs
 - d) All of the above

- 2) Match the following:

a Document Virus	i) Its life depends on the life of the host	
b Resident virus	ii) It affects highly structured files comprising data and commands	
c Transient virus	iii) It attaches itself to executable files and replicates.	
d Parasitic virus	iv) It locates itself in the memory	
	v) Hidden by itself	

a) a->iv b->v c->ii d->i	b) a->i b->ii c->iii d->iv
c) a->ii b->iv c->i d->iii	d) a->iii b->i c->iv d->v

- 3) Which of the following type of virus attaches itself to executable files and replicates when the infected program is executed?
 - a) Stealth Virus
 - b) Polymorphic Virus
 - c) Parasitic Virus
 - d) Macro Virus

- 4) _____ will create copies during replication that are functionally equivalent but have distinctly different bit patterns.
 - a) Boot Sector Virus
 - b) Polymorphic Virus
 - c) Parasitic Virus
 - d) Macro Virus

3.2.3 Worms

Computer worms are the malicious programs or software, which alter the normal execution of the system. Worms are also a type of viruses that can harm the system. Worms have one major difference with viruses, i.e. the viruses need activation, whereas worms can replicate or multiply themselves. Because of this replication, they overload the system, server, or networks and slow down the PC performance.

Computer worms always choose some places, where the operating system files reside. They identify vulnerabilities within the operating system and make that portion as a target for their execution. Few worms combine with small malicious code to steal and transfer personal information through some way of communication. Some other part of the code will compromise the network firewalls such that viruses can enter the system to do the rest of the work. If worms start spreading through the network, then they cause denial of service attack and create congestion in the network.

(i) Types of computer worms

In accordance to the nature of the target, worms are classified as:

- **Email worms**

As the name indicates, they majorly target the email of clients. Once they infect an email account, they identify all the email addresses available in the address book of email client and send a file as a link, which is a source for worms. One click on the link or if the file is opened, the worm will find its place for its residence. This chaining process continues and affects all the systems of the organisation or network. Sometimes lists of all the email addresses are shared with the hacker who created this worm and this list can be used for performing the illegal activities.

The best *example* of the email worm is “ILOVEYOU” worm in the year 2000. An email with the subject as ILOVEYOU was sent. It was attached with visual basic script, which affected the outlook module of the operating system. This in turn sends a “Melissa virus” to first 50 email addresses of the list.

- **Internet Worms:**

Internet worms will start their process from the system that is infected. When a system with internet-worm is connected to the internet, it scans the entire network to find the

system with security loopholes. During this scan, if it finds the system with loopholes then it penetrates into that system. The main intention of this worm is to scan for newly installed security configurations and operating system updates.

One of the best *examples* for this worm is “code red” worm, which was used to infect IIS web server.

- **File-sharing Networks Worms:**

File-sharing network worms mostly target the location, where more files are residing. It becomes part of the file. This file copies itself into new device or location. Then, along with the original files, even worms will get copied into the location. This process will continue as a chain reaction.

One of the best *examples* for this is “Phatbot.” It has infected millions of computers in the year 2004 and was very much successful in stealing the personal information saved on the computers.

It is always advised not to insert any external storage device into the system until it gets scanned with antivirus.

- **Instant Message and Chat Room Worms:**

This kind of worm execution is very similar to email worms. The only difference is the nature of the target they choose to act. Chat room worms will scan the contact list of the chat room and starts sending the link to each member. However, these worms will show its effect only when the user accepts the message and clicks on the specified link. Since most of the users would not do it, it is less harmful than the email worm.

- **Multi-vector worms:**

If a worm has more than one way of its implementation and execution, then it called as Multi-vector Worm. *For example*, if a worm targets instant messenger and emails, then it can be called as Multi-vector worm. As this kind of worm has its implications in different places, it is considered as most dangerous worms.

Some of the well-known worms are Stuxnet, duqu and flame. Stuxnet and duqu are the computer worms which were targeted towards Iran Nuclear Power plant between 2008 to 2014. Flame worms are created with an intention of spying the internet users.

Even though the worm's implications are very slow their final effects will be always ending with major risk.

(ii) Symptoms of a Computer Worm

Worms will not show their presence very soon. Their impacts are not immediately visible, but are very dangerous. Its effects are very hideous. The symptoms of worm attack are as follows:

- The Performance of the computer will be slowed down
- Few programs will be run automatically
- Most of the system components will be freezing randomly
- Internet browsers functioning will be unpredictable and unnatural
- The Hard disk will be creating more sound than normal
- Firewalls will be generating error messages continuously
- Few files will appear to be missing, *for example*: dll missing
- Few file names will be modified
- Different unwanted icons will be appearing on the desktop
- Operating system error messages will be generated very frequently
- Unwanted emails will be sent to all the users without user's knowledge

Many of the above mentioned malfunctioning acts in the computer can appear around the same time. Immediately antivirus should be installed to protect the system as an initial precautionary step.

Safeguarding computer from Computer Worms by:

- Updating the operating system and antivirus
- Avoid opening mails from the unknown receiver
- Never try to open unwanted links

(iii) Computer Worm Removal

To remove the worms from the system, we should implement the steps described below:

- First, disconnect the system from the internet and LAN. This process stops the worm from spreading to other systems. If this is not done, then there is a chance that it will come back from other sources
- Download all the operating system updates and antivirus software updates from the system which is not affected with worm and store them in external storage
- Install the updates into the system
- Scan the computer with antivirus and clean up all the worms

After confirming the cleanup, all firewalls of the organisation with new rules should be updated and then the device can be connected to the network



Self-assessment Questions

- 5) Which of the following security threat is a replicating program that runs independently and spreads through vulnerabilities?
 - a) Worm
 - b) Viruses
 - c) Spyware
 - d) All of the above
- 6) Which of the following type of worms gets attached itself to a file and moves to a different location when file is being copied?
 - a) Internet worm
 - b) File sharing and network worm
 - c) Email worm
 - d) Chat room worms
- 7) Which of the following is not a preventive measure to avoid worm attack?
 - a) Never install any antivirus in your system
 - b) Take a regular backup of all the files
 - c) Avoid clicking unwanted links
 - d) Do not open any attachment of an email from an unknown sender

3.2.4 Malwares

Power of programming and programmers are not only seen in the development of valid and secure software's but also in developing softwares that can create a great threat to the security system of the organisation. Softwares, which create such kind of threat and compromise the security system can be called as malfunctioning softwares or malicious softwares or malwares.

Viruses, worms and disruptive softwares are different variations of malware. Their aim is to create inconvenience to the security system. Even though antivirus and internet security software's are finding every new possible way of protecting the system, still many of the hackers are able to find new ways to penetrate into the system. Previously, worms were designed to multiply themselves until the system goes to a halt. But nowadays, the same worms are used to get sensitive information.

Some of the malware is installed on different systems and they are connected to each other through the internet and exchange of information between them happens until it reaches a specified point. These kinds of networks formed between malwares are known as BOTNETs. Major source for botnet creation, the chat rooms and email clients.

(i) Types of Malware

Based on their nature of existence and targets, the classifications of malware are as follows:

- **Adware:** The design of this malware is to pop up the advertisement of a product or organisation. It is very difficult to find the source of this malware. They just cause discomfort for the users of the computer, because they continually pop out disturbing regular work while in progress.
- **Spywares:** This malware used as a spy for your systems. This software majorly focuses to collect the sensitive information of the users. Key loggers can also be considered as a type of spyware. Detailed explanation about spyware can be found in section 3.2.5
- **Viruses:** The creation of this malware is to disrupt or crash the security system. The objective is to destroy the security system or to compromise the system. Their effects are visible as soon as they affect the system. It is always better to prevent the entry of the viruses rather than going for recovering from it. Detailed expiation about the virus can be found at section 3.2.2.
- **Worms:** This malware penetrates into the system and starts multiplying by themselves. In many occurrences, their existence is unknown to the user until the system gets

crashed. Many times, worms are used to trigger the viruses because viruses will not be able to spread by themselves. Detailed explanation about worms can be found in 3.2.3.

- **Browser Hijackers:** Hijackers are also a type of malware that target web browsers and take the control of the few components of web browsers. They try to move your control to the pages, which you would have never opened at all. Many times, they make their website page as the default page of your web browsers.
- **Diallers:** This software will make calls by using your internet connection and create huge bills to the users. Sometimes these calls are also made for terrorist attacks.
- **Deepwares:** These are the softwares which will try to execute directly, with hardware without the need of an operating system. They penetrate very deeply into the system and execute where, even antivirus software programs cannot detect them.
- **RootKits:** It is a collection of malware designed to get access to the system. This word is a combination of “root” and “kit”, which means a set of software’s that acts as privileged. This rootkits find the vulnerabilities in the security system and deploys some programs to tackle them.
- **Ransomware:** Ransomware is a malware which locks or encrypts few important files or resources of the system. The designers of this malware demand some money or benefit to release this resource. Some of this malware may block access to information systems.

(ii) Impacts

Most of the times, the malware creates a huge loss or damage to the system where it was installed. The major effects can be as follows:

- Slowdown in the performance of the system
- System crash
- Slowdown in the internet connectivity
- Continuous display of error messages
- Continuous popping out of the ads Theft of useful information
- Deletion of important files
- Redirecting the browser control
- Broadcasting the information to all other users
- Sending unwanted emails
- Installation of unwanted toolbars
- Creation of unwanted icons

- Switching off the firewall to compromise the security system
- Unauthorised resource utilisation
- Loss of the capability of shutting down and restarting the system

There can be more than the above mentioned effects that might have not come into the notice of the world.

(iii) Prevention

As the well-known proverb says, “Prevention is always better than cure”, preventing the entry of malware is very important for an individual or organisation. Following preventive measures can be followed to avoid penetration of malware:

- Keep operating system, anti-malware and antivirus software always updated
- Never allow external storage device without scanning with anti-malware and antivirus tool/software.
- Never open the attachment of a mail from unknown users
- Configuring the firewalls of the system should be in such a way that important messages should not leave from the system and intruders should never enter the system.
- More than one antivirus should be installed because if one misses the threat, others will try to find it out.
- Enable all the security settings of internet browser such that it avoids the installation of toolbars and Trojans.
- Schedule the regular scans of anti-malware and antivirus such that threats can be found before it creates the damage
- Always install new software by keeping anti-malware and antivirus tool enabled
- Create an awareness in the employees about all possible malware and the steps to be taken to protect the system from them
- Before installing the new software, it is better to read the license agreement completely
- Download any software from only known and trusted websites, install new softwares in virtual machines rather than in the production environment.
- Be double sure before clicking any unknown link.
- Schedule regular backups to avoid loss of confidential and important information.

Initially, most of the malware was developed to show the power of the programmer’s programming skills. Now the builders of malware have very clear intention of damaging the system, so to prevent the malware one must use anti-malware and antivirus software/tools.

Hence, it is very much important for anyone to be careful before installing new software into the system.



Self-assessment Questions

- 8) A malicious software is known as ____.
- | | |
|---------------|------------|
| a) Middleware | b) Malware |
| c) DOS | d) Stealth |
- 9) Which of the following type of malware can make calls from your system and increase the mobile bill for you?
- | | |
|------------------|--------------|
| a) Dialer | b) Deep ware |
| c) Trojan horses | d) Hijackers |

3.2.5 Spywares

Spywares are a type of software that are designed to collect the information about the system or user without their notice. It becomes the malware, if it has been built with wrong intentions. Many spywares are created to steal the financial information of the users.

Many spywares are also built with very valid intention of monitoring the system performance of the user without their notice. The spyware with monitoring capacity helps organisations to build organisational policies and blockers.

The difference between malware and spyware is the intention. The malware aims to create harm to the system where as spyware just monitors the system. Spyware can also be called as malware if the intention of this is to create the harm.

For example: Trojan horse

(i) Types of Spyware

Based on the nature of usage, spyware can be classified as follows:

- **Adware:** These kinds of spyware will collect the information like users' interests, most visited websites, online purchases, products that users are willing to purchase. This information helps the spyware builders to decide the kind of advertisements, which will

attract their attention. This spyware will pump huge number of pop-ups based on the user interest and troubles them with ad pop-ups.

- **Commercial spyware:** These are the software spies that are created and sold based on demand. These spyware is used to act as a spy for the employee activities, parental monitoring, private investigators, spouses, etc. These spyware is majorly used to identify the threat with sufficient evidence to take legal action on the intruder.

Many parental control software is part of the antivirus software programs. This parental control software will help the parents to monitor their children's activities such as websites that they are watching along with the duration.

- **Trackware:** A program which clandestinely monitors the performance and behaviour of the user and sends the same information to the others.
- **Cookie profiling:** It is also known as web profiling. This spyware is designed in such a way that, few cookies, which are employed by this spyware collect the user activities. These cookies are gathering the required information when websites are browsed by the user.
- **Keyloggers:** These are the spyware that is used by most of the organisations to monitor the keystrokes of the employees. This helps the organisations to decide their security policies.
- **Trojan horses:** These are the malicious software, which appears as useful software but they show their adverse effect after completing the installation. They are majorly used for designing Remote Access Tools (RAT). These tools help in accessing the system from remote systems and collect all the data in a centralised location.
- **Web bugs:** It is a form of adware that will collect your internet browsing patterns and sends it to a centralised location. Most of these spyware collects the data for statistical purposes. It completely tracks the activities performed by the user. User can disable the cookies to get rid from web bugs.

(ii) Causes

- Most important causes for the spyware entry to the system are installing the software's without reading the complete end user agreement. Most of the software's will have

additional tools along with the original software. These additional tools will be clearly specified in the end user agreement, but we neglect to read them.

- Some of the spyware is intentionally installed into the system to monitor the activities of the user or tools.
- Installing the software, which are not completely bug free may also be a cause for the spyware installation. Some part of the original software may hook with spyware code, which even antivirus cannot detect. Hence, users need to install the softwares that are from genuine websites.
- Phishing websites will also make you to download unwanted spyware and get them installed in your system.

(iii) Effects

In most cases, the effects of the spyware will be very adverse and dangerous. These are the few effects of spyware:

- Identity theft can be noticed. Hacking of mail passwords, an increase in mobile bills and unwanted mails and calls can be an effect of spyware.
- Slowdown of PC because of more RATs are installed in the system
- More traffic flow from/to system can be noticed
- More programs will be running more than you have opened, which makes your system hanging and regular restarting of the system is done.
- Banking websites might be hacked
- Many criminal activities can happen through your system or mail address
- Advertisements can be made by using your system as a source of advertisements
- Spoofing can happen from your mail address

(iv) Prevention

As spyware is much dangerous than virus and worms so its prevention is very important for an organisation or an individual

- Configure all types of firewalls which will not allow any spyware to be installed in the system
- Do not save any personal or banking information in the computer
- Never use any key websites without antivirus, anti-spyware and internet security installed in the system.

- Never install any software from unknown sources of organisation Install the antivirus like windows defender and schedule its scan every day
- Check for the security vulnerabilities of the organisation repeatedly
- Do not respond to any mails which has only links in it
- Do not give installation permissions to the other unknown users
- Keep confidential data in the most secure location of the organisation



Self-assessment Questions

- 10) Which of the following software acts as an informer?
- | | |
|--------------|-------------|
| a) Viruses | b) Worms |
| c) Hijackers | d) Spywares |
- 11) _____ is used to protect the system from spyware and other similar programs.
- | | |
|-------------------------|---------------------|
| a) Windows Defender | b) Windows Firewall |
| c) Windows Active Icons | d) Windows Spyware |
- 12) _____ is a well-known example of spyware's, which captures the keystrokes to the users?
- | | |
|---------------|-------------|
| a) Viruses | b) Worms |
| c) Keyloggers | d) Monitors |

3.2.6 Windows Registry

A computer is a collection of software and hardware. Most of us are unsure of the impact when we connect any device to the system. To understand how the system will get impacted and the information about the system will get stored, we use “windows registry”.

For windows operating system, the central database is the windows registry. It will store the information about configuration details regarding installing and installed softwares, hardware device configurations, settings of the system, preferences of the user, modification or update details of the software's, working with display settings.

The windows registry is an important thing for a windows operating system. Even a small change in this will create huge problems. So if the user is doing modification, it is always advisable that to maintain the image of the current state of the system before editing the data in windows registry.

(i) Window Security Model

Windows security model is a subsystem of overall windows architecture as shown in figure 3.2.2. In a broader sense, Windows architecture divides the overall system in two parts:

- **User mode**

This is the mode where the user will access the system. Two modules will be controlling the user mode, they are the local security authority and win32 subsystem. All the other functionalities will interact with kernel mode through these modules.

Local security is responsible for all the local security validations. This module takes the responsibility of the logon process, user account management, policy management and maintains the audit log of the system.

Any executions of service or application are done through win32 subsystem. Even the win32 subsystem also interacts with local security authority to validate their access right and privileges with central access control repository.

Local security authority interacts with the global security database, which under the control of the security reference monitor, will make the final call.

- **Kernel mode**

Kernel mode is unique for all the users of the windows system. All the service execution, which needs interaction with hardware are done through kernel mode. It provides a huge number of executive services like I/O management, virtual memory management, security reference monitor and so on.

When the security model is used, the security reference monitor will also be used to verify the global resource allocation policies and global audit log.

All the users created will have their own private and local repositories. When it is to be verified with global resource access rights, then it contacts with a module called a security reference monitor. This security monitor will validate all the access controls and validations.

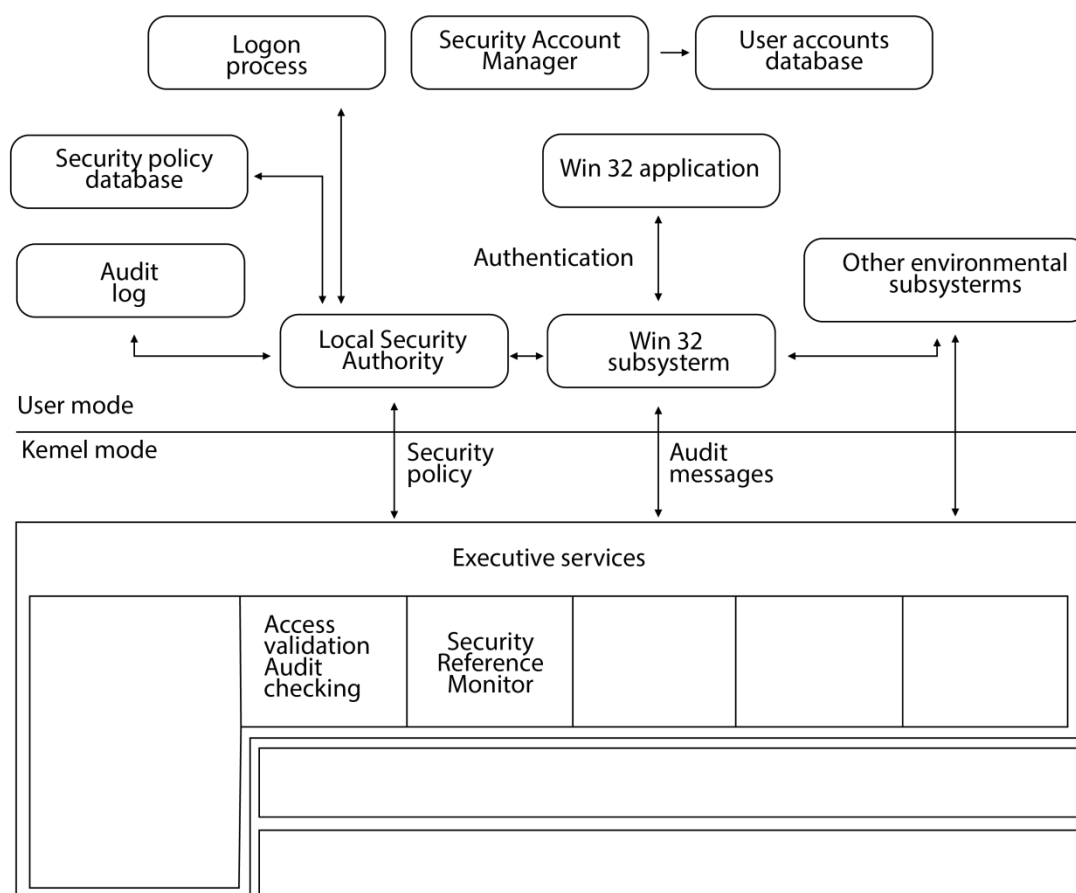


Figure 3.2.2: Windows Security Model

(ii) Registry Root Keys

The Windows registry information is presented like tree structures. The information held by the containers is known as keys. The containers are like folders in the normal computer terminology. Every key has its own sub keys. The windows registry stores the information in the binary data. The information inside the key may contain different types of data formats like numbers, strings. Hive is the major portion inside the registry, which consists of 5 keys known as root keys.

Every key in the hive performs and stores specific information.

Registry basic comprises of two elements that are key and values. If register keys are considered as folders, the files in that folder can be considered as values. A registry may contain sub-keys and values. Sub-keys may have some more sub keys and values. This hierarchy starts with windows registry divided into 5 root keys they are further divided into keys and values.

The root keys are:

1. **HKEY_CLASSES_ROOT:**

Also known as HKCR the HKEY_CLASSES_ROOT stores the information about the program registered in the windows operating system such as Object Linking and Embedding (OLE), data related to the application, file name extensions and short cuts. HKCR is the direct access given to the software programmers for HKEY_LOCAL_MACHINE\Software\Classes.

HKCR contain various sub folders to maintain additional information about the applications as shown in figure 3.2.3.

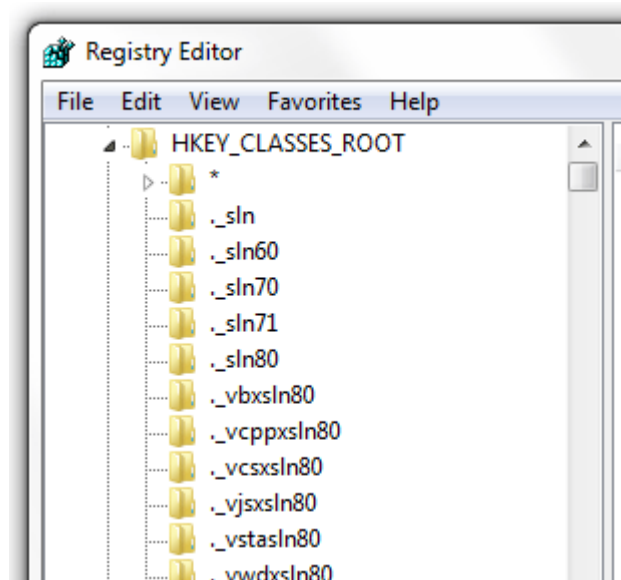


Figure 3.2.3: HKEY_CLASSES_ROOT registry

2. **HKEY_CURRENT_USER (HKCU)**

This is the registry that maintains information about the settings related to the current user who are using the system. If multiple user accounts exist, then this storage only maintains the current user settings.

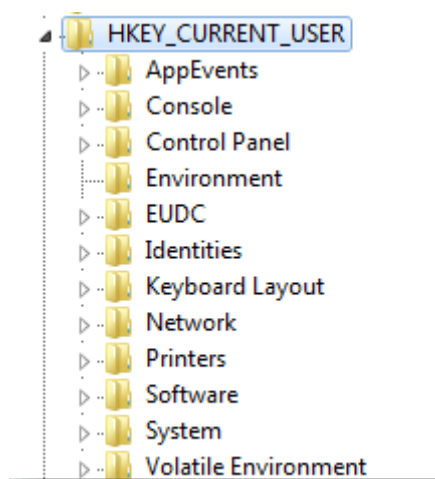


Figure 3.2.4: HKEY_CURRENT_USER root registry

3. HKEY_LOCAL_MACHINE (HKLM)

HKLM has been the most frequently used registry hive. This key contains the configuration information about software and hardware. We can find details of the system bus for the security of the system. It covers every aspect of the system.

Most of the attackers, viruses majorly focus on this registry because scanning this folder is almost equal to scanning the entire system. By considering the values of this registry, system compromises can be identified.

4. HKEY_USERS (HKU)

HKU is the storage for all users setting information. By using this register any one can get the information about number of user accounts and their access details up to current date. Most of cases HKU and HKCU values are similar.

5. HKEY_CURRENT_CONFIGURATION (HKCC)

HKCC majorly focuses on the values of hardware used by the current user. The values of HKCC are almost empty and they get their value during the OS booting.

(iii) Windows Registry Values

The values of the windows registry stored in different data formats. There are mainly five data types. They are:

1. **REG_DWORD** – It is a 32 bit number. It is commonly used as a Boolean value for either enabled (1) or disabled (0). Many system services and device drivers use this data type for representing their values in decimal and hexadecimal format.
2. **REG_BINARY** - This stores data in binary format. In many cases, this will be used for representing the hardware information.
3. **REG_SZ** - REG_SZ is the string representation terminated with a null character. Basically, it will be either ANSI or Unicode string.
4. **REG_MULTI_SZ** - This type is only available in advanced windows registry editor, i.e. REGEDT32 used for representing the multiple strings like lists or a variable consist of multiple values. Multiple values represented by this string are separated by a null character.
5. **REG_EXPAND_SZ** – This type of data type is for expanding the data string. This will be used for expanding the references for environmental variables.

(iv) Registry Key Security

Windows registry holds most crucial and critical settings of windows system. So, if the value of the registry is edited directly without any proper knowledge, then it may damage the system.

According to the windows security model, all the access controls of the user can be retrieved from the registry keys. Few function calls provide an access to edit values of the registry key values. The advantage with this approach is that this method can validate and avoid the danger of giving wrong values to the keys of the registry.

The methods are:

- **RegCreateKeyEx:** It is used to create a new key in the registry.
- **RegSetKeySecurity:** it is used to set values for the key. The key name should be the argument.

If no arguments are provided then null is used, it focuses on the default access rights of user which are available in access control list (ACL).

- **RegGetKeySecurity:** it is used to get the key values, which are used for security enforcement.
- **GetNameSecurityInfor:** it is used to find security information assigned for specific key value.

(v) Access Rights

Windows uses Discretionary Access Control (DAC) to assign the access rights to various users. Access Control Lists are created for every user with all possible permission to the resources.

When an administrator assigns the access rights to the users, the corresponding registry values get edited and some values are set for them based on the access right given to the users.

There are few valid access rights available; the same should be used while assigning the values to register keys. They are:

- **DELETE:** has the right to perform delete operation to the resource
- **READ_CONTROL:** has rights to read the resource
- **WRITE_OWNER:** user is the owner of the resource and has permissions to write about it.
- **WRITE_DAC:** user has right to change the default values assigned to resource. This means that the user can change ACL values of the other user.

If any user tries to change the access rights, then the user access rights are verified with their ACL. If they have no rights to change the values, then the operation of the user fails with appropriate error message.

If the administrator enables any user with WRITE_OWNER permission, then they can edit the access rights of the user.

Regedit.exe: It is used to view and edit the key values of any key.

Crucial security information of the operating system is available with registry keys, hence it is always advisable not to edit the key value without proper knowledge of the keys.



Self-assessment Questions

- 13) _____ is not a registry root key?
- a) HKEY_CURRENT_MACHINE b) HKEY_CLASSES_ROOT
 - c) HKEY_CURRENT_USER d) HKEY_LOCAL_MACHINE
- 14) Which of the following registry key value stores the information about the environment variables?
- a) REG_BINARY b) REG_DWORD
 - c) REG_EXPAND_SZ d) REG_MULTI_SZ
- 15) _____ is used to set the value to registry key?
- a) RegCreateKeyEx b) RegSetKeySecurity
 - c) RegGetKeySecurity d) GetNameSecurityInfor



Summary

- The information system faces huge threats from different viruses, worms, malware and spyware.
- Viruses are the malicious software, which will attack the system and corrupt the file, which it has attacked.
- Worms are small software programs, which penetrate into the system, reside in the system and starts multiplying itself until the system is crashed.
- Most of the worms are used to compromise the security of the system
- Malwares are the malicious software, which are created for malfunctioning the systems. Even viruses and worms are malwares.
- Spywares are the software, which acts as a spy for the system. They collect the information from the system, hand over this information to the source of spyware.
- Most of the required information for the smooth execution of the windows security system is residing in the windows registry.
- The organisation of Windows registry contains keys and values. Keys are like folders and values are like files. Each key can have sub keys and values.
- Windows operating system is employed with a different security model for providing security to the registry values.



Terminal Questions

1. List and explain general characteristics of virus?
2. What are the symptoms for the worm existence in the system and how can they be removed from the system.
3. Why malwares are dangers to security system and how can they be prevented.
4. “Few spywares can be used as monitoring tool”, justify the following statement with your answer.
5. What is the role of windows registry in the security system and how access controls can be assigned to them?



Answer Keys

Self-assessment Questions	
Question No.	Answer
1	d
2	c
3	c
4	b
5	a
6	b
7	a
8	b
9	a
10	d
11	a
12	c
13	a
14	c
15	b



Activity

Activity Type: Online/Offline

Duration: 30 Minutes

Description:

Over time many big companies have faced problems related to system threats and attacks. Search the internet and find out 5 most popular attacks over internet and how companies solved this problem.

Case Study

“Myfootware Corporation” wants to enter into an online business. All the products they own are listed on their web sites. Every customer can see the listings of products available, but if they want to purchase the products then they must register them self by using their personal information. As an introductory offer they announce an offer that anyone can get 75% off, if they register themselves along with 10 other people’s valid email ids and phone numbers.

After announcing this offer, the administrator observed few changes in the systems of the users and servers. They found that at least 3 systems among the 200 systems were crashed and most of the employees were getting repeated spam mails. The windows registry values were also edited.

The administrator was fully confused. He was looking for ways to handle the situation. He contacted the management and explained the consequences of this scenario.

1. What is the reason for the adverse effects happening in the “myfootware Corporation”?
2. Suggest some security measures to be implemented in organisations?
3. If you were the administrator of “Myfootware Corporation”, what would you do to prevent the situation from happening?

Bibliography



e-References

- *Virus*. Retrieved 5 Feb, 2017 from <http://searchsecurity.techtarget.com/definition/virus>
- *Worm*. Retrieved 5 Feb, 2017 from <http://www.pctools.com/security-news/what-is-a-computer-worm/>
- *Spyware*. Retrieved 5 Feb, 2017 from <http://usa.kaspersky.com/internet-security-center/threats/spyware#.WLG102-GN1t>

Image Credits

- Figure 3.2.1: <https://image.slidesharecdn.com/23-networksecuritythreatspkg-140220233706-phpapp01/95/23-network-security-threats-pkg-30-638.jpg?cb=1392939507>
- Figure 3.2.2: https://www.microsoft.com/resources/documentation/windowsnt/4/server/reskit/en-us/net/images/xng_b22.gif
- Figure 3.2.3: <http://mintywhite.com/vista/hkcr-hkcu-hklm-hku-hkcc-registry-root-keys/>
- Figure 3.2.4: <http://mintywhite.com/vista/hkcr-hkcu-hklm-hku-hkcc-registry-root-keys/>



External Resources

- Whitman, M. E., & Mattord, H. J. (2003). *Principles of information security*. Boston, MA: Thomson Course Technology.
- Stallings, W. (2000). *Network security essentials: applications and standards*. Upper Saddle River, NJ: Prentice Hall.
- Pachghare, V. K. (2009). *Cryptography and information security*. New Delhi: PHI Learning.



Video Links

Topic	Link
Spyware	https://www.youtube.com/watch?v=oqPbAEMlgRY
Windows Registry	https://www.youtube.com/watch?v=Zp63Ahunpgc
Hacking Windows Registry	https://www.youtube.com/watch?v=rZ8dvMhdLew



Notes:



Information Security - I

MODULE - IV

Internet Security and Prevention

Internet Security and Prevention

Module Description

The internet is an unavoidable requirement of any organisation. Organisations are using the internet to extend their business opportunities and reach every customer by spending a very limited amount of time. It is an important requirement for business establishment and expansion. If proper plan is not there during the installation and maintenance of internet then it will be a big threat to the organisation's information security. The security system of any organisation or individual can be appreciated only when it provides reliability at each level of the network.

This module focuses on the security of LANs and email. As we know that the threat to security is majorly due to hackers, this module focuses on different hacking techniques and their prevention plans.

At the end of this module, students will be able to understand the importance of securing networks from the hackers. This could strengthen any organisation network from the hackers effectively and focus on identifying the new hacking methods to safeguard the networks from the hackers.

Chapter 4.1

Internet Security

Chapter 4.2

Preventive measures for hacking attacks

Chapter Table of Contents

Chapter 4.1

Internet Security

Aim.....	183
Instructional Objectives.....	183
Learning Outcomes.....	183
4.1.1 Introduction.....	184
4.1.2 Internet Security.....	184
(i) LAN Security.....	185
(ii) Email Security.....	191
Self-assessment Questions.....	192
4.1.3 Hacking attacks	193
(i) Types of attacks	193
(ii) Hacking attacks countermeasures.....	194
(iii) Hacking Tricks	195
Self-assessment Questions.....	197
4.1.4 Approaches to Hacking.....	198
(i) Physical Intrusion.....	198
(ii) Password attacks.....	199
(iii) Network Access and Web Server Attacks	200
Self-assessment Questions.....	204
Summary	205
Terminal Questions.....	206
Answer Keys.....	207
Activity.....	207
Case Study	208
Bibliography.....	209
e-References	209
External Resources	209
Video Links	209



Aim

To familiarise the students with the concepts of internet security and its preventive measures so that network can be protected from hackers and protect the information on the internet.



Instructional Objectives

After completing this chapter, you should be able to:

- Elaborate various types of internet security
- Explain the types of hacking attacks and tricks with their countermeasures
- Classify various approaches of hacking with respect to the mode of attack



Learning Outcomes

At the end of this chapter, you are expected to:

- Outline the types of Internet security and its reach
- Recognise network security risks and related measures to prevent security threats
- Outline the different categories of hacking attacks and tricks so that countermeasures can be taken to prevent them

4.1.1 Introduction

The internet has reached every corner of this world. Most of the communication problems faced earlier is solved with the invention of the internet. Most of the business operations and individuals are bounded together with the internet. A message sent using the internet has to cross a lot of transit points before reaching the end system. All the communication channels and transit points are good sources to the hacker for hacking.

We have learnt the concepts of security and intrusions in the previous chapters. This chapter focuses on securing the LANs and emails because they are the best source for the hackers to penetrate into the system. This chapter also focuses on hacking and their possible attacking techniques.

4.1.2 Internet Security

Most of the complicated problems of communication have found their solution with the invention of internet. The internet has reached its peaks. The only thing that is changing is the number of people using it, which is increasing massively. Most of the bank operations have become online; most of commercial businesses are operating over the internet. Because of all these flexibilities, every single industry has made internet as a part of their process.

A massive growth in internet users and their operations has eventually increased the possibility of threats.

The internet is defined as a network of networks. So security of the internet relies on the individual networks that are part of the internet. The internet is not just a flow of information, it also involves a lot of network devices, servers and communication channels. The building of a strong security system can be possible, but only if we know every part of the system clearly.

Hence, the security of the network depends on:

- Connectivity of network
- Communication medium
- Nature of communicating people
- Limited access of network

Based on the accessibility of network, they can be classified as:

- Closed network model

- Open network model

Closed network models focus on connecting all the systems and forms a network, but they will never allow outside data to enter or leave the system. They are more realistic in building and communicating with others. Since there is no intrusion into the network, most of the security problems can be avoided, but they cannot be called as secured because the threat can emerge within the network system. Intrusion is defined as an unauthorised or forceable entry into someone's network/internet.

The open network model focuses on connecting all the devices of the network with each other along with the external networks. As they allow the external devices to communicate with the internal networks, they are more scalable than the closed network. As external intruders are penetrating into the system, the system will be at high risk. More focus should be given to protect the system.

Special security hardware and software's are required to secure the system. They are firewalls, intrusion detection systems, VPNs, tunnelling, network access control and security scanners

Security of the internet major depends on the security of the LANs, so let us focus on it.

(i) LAN Security

LANs are the computer networks that scale up to very limited geographic vicinity. All the systems within the LANs can communicate with each other without any internet.

LANs deals with most of the hardware components that do not have any security by themselves, hence they are more prone to security attacks.

Most of the protocols used by LANs are stateless and much prone to security attacks. Some of them are as follows:

ARP Spoofing:

Address resolution protocol (ARP) is a protocol used to find the hardware address for the IP address of the system. To find the hardware address of the system, every system will raise an ARP request. The request includes the source IP address, the source hardware address and request an IP address. The request is then broadcasted. On receiving the request, every system checks for the requested IP address. The system with requested IP address will respond back with its hardware address. The ARP Response is passed to all the systems on the network. All

the system records each and every packet IP address and MAC address in a table called ARP Cache.

The ARP Response with requested details is broadcasted to all the systems of the LANs. Every system will maintain the ARP details that it has received in a table called as ARP cache. ARP spoofing is the process, where an intruder creates a false ARP Request with IP address of some system in the network and their MAC address and sends it to other systems of the network. All the other systems create a record of the attackers IP address and hardware address.

The attacker always chooses the IP address in such a way that all the packets pass through the attacker's system. As all the packets are passed through the attacker's system, the attackers can use the data of every packet.

To explain in detail let us take a look at Figure 4.1.1

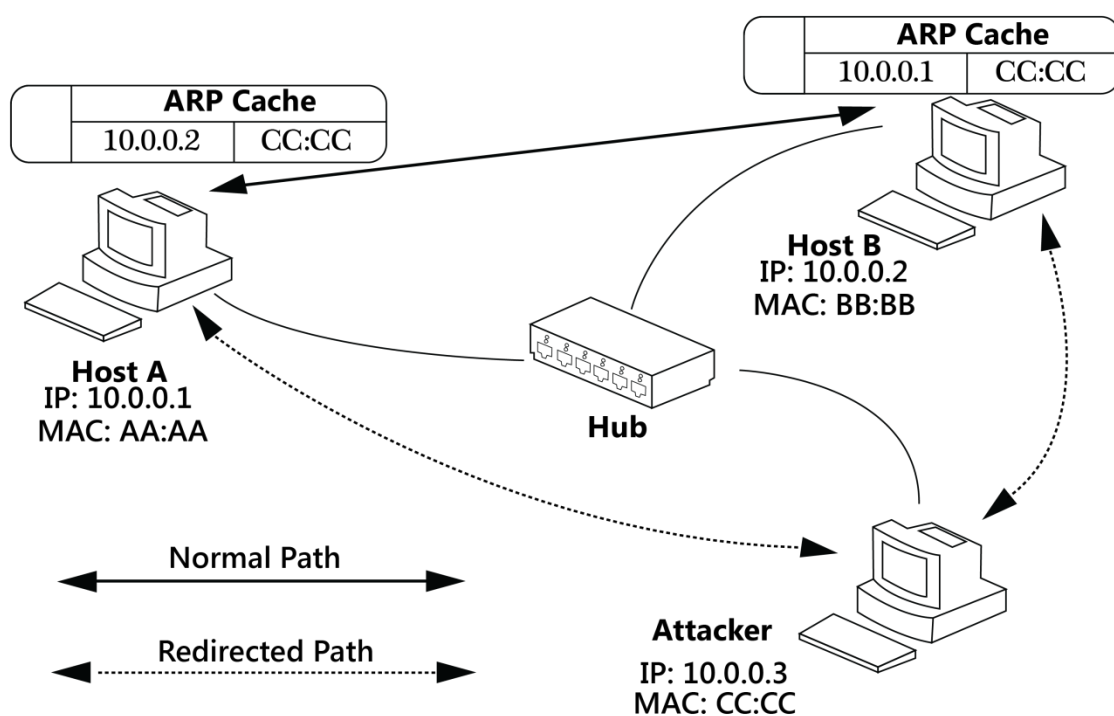


Figure 4.1.1: ARP Spoofing

- Step 1: Attacker has chosen his IP address as 10.0.0.3 and his hardware address as CC:CC, which is a valid IP address for LAN shown in Figure 4.1.1
- Step 2: Attacker creates an ARP packet with his IP address and MAC address and passes to Host A and Host B.

- Step 3: Host A and Host B receives the message from the attacker and creates a record in their ARP Cache
- Step 4: As attacker always chooses the IP address in such a way that, their system becomes a middle point of communication. So Host A and B communicates with each other through the attackers system.
- Step 5: When A sends a message to B, it will go through the attackers system.

MAC flooding:

The switch maintains a table called Content-Addressable Memory (CAM). This table contains the details of the MAC address of all the systems connected to the switch and port to which they are connected. On receiving, any packet switch will verify the destination MAC address of the packet and forwards the packet through the corresponding port. If the switch receives any new packet whose address is not available in the table, then it creates the new row in CAM. To optimise the usage of CAM, records that are not used for a long time will be removed.

The hacker will flood huge number of messages with different MAC addresses, thereby filling up the CAM. When no memory is available in CAM, then the switch enters into a mode called “fail open mode”. In this mode, messages are broadcasted through all the ports of the switch without checking the MAC address of the message. All broadcasted messages will reach hacker.

So, the hacker's message will reach every system. This message may have malware to do the rest of the harm.

Port stealing:

CAM of switch is empty when it is powered ON. On receiving a packet from any system of LAN, it creates a record with the MAC address of the system and port number through which it has received the message. This process is known as learning switches.

After the switch has filled CAM with considerable records, if any packet enters the switch, the switch will verify the destination MAC address of the packet and sends the packet through the corresponding port.

If an attacker creates the false packets with MAC address of others system and projects it as their MAC address and sends the packet to switch, then the switch updates the port number of MAC address with a new port number. Due to this update, the attacker will receive all the messages of a valid source.

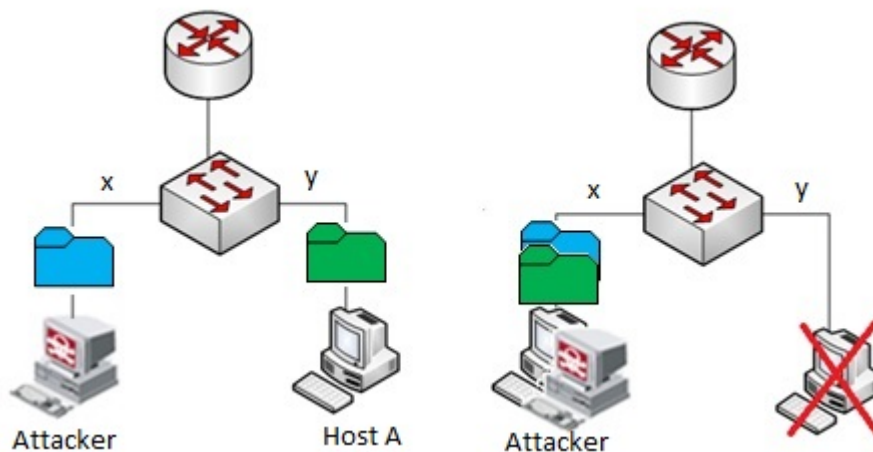


Figure 4.1.2: Port Stealing

For example: As shown in Figure 4.1.2, consider Host A is a valid MAC address and its port number is Y. The attacker has created a message with the same MAC address of Host A, but port number as X. As soon as the attacker sends a message, then the switch after seeing the MAC address, will change the port number from Y to X. Now, all the messages for Host A will get diverted to the attacker.

DHCP Attack

DHCP servers will provide IP address to the clients based on the request. The response generated by DHCP server will have all the required settings to start the communication. Many organisations are using the Dynamic Host Configuration Protocol (DHCP) for providing an IP address dynamically to clients based on the request. The attacker will employ a Fake DHCP server and provide the IP address to all the client requests, before the original DHCP server responds, as shown in figure 4.1.3. In the DHCP response, the attacker will provide their server address as a default DNS address. Therefore, any data getting in/out of the networks will flow from this server. With this, they can grab all the data of the messages transmitted. This attack is named as DHCP attack.

To avoid the DHCP attack, an extra switch is added between trusted DHCP server and client. Any DHCP request coming to the switch will only forward to the trusted DHCP server because the switch knows only one valid DHCP server address. All the responses from DHCP server will only forward to clients, as shown in figure 4.1.3.

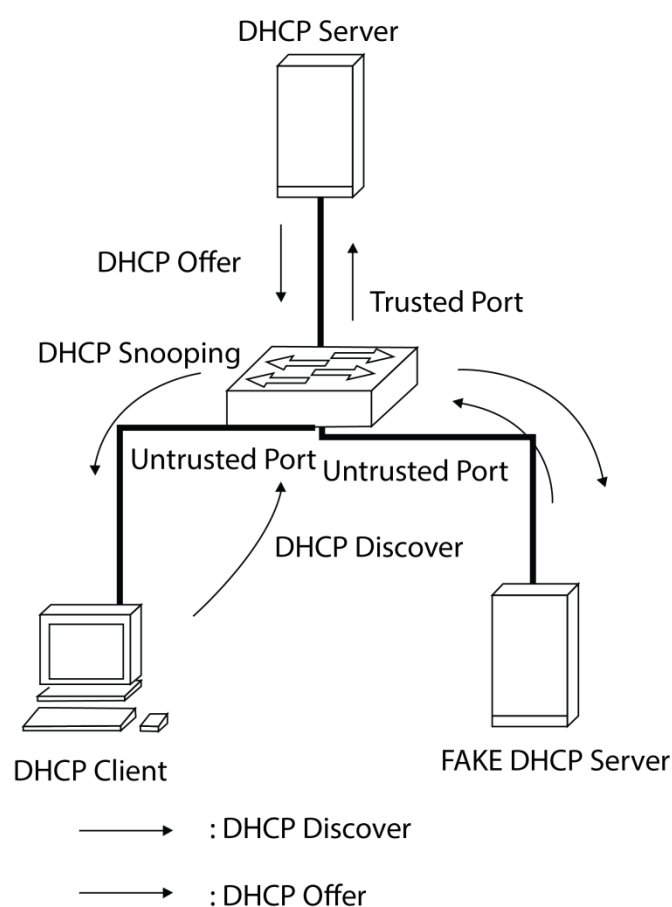


Figure 4.1.3: DHCP snooping

Attacks on the Spanning Tree Protocol:

When different LANs are interconnected using bridges, loops (cycles within the network) get created between the bridges. These loops can be formed or created intentionally. The existence of loops makes the broadcasted packets to stay within the network without being destroyed. This will increase the congestion. To avoid this congestion, we can use the spanning tree algorithm.

This algorithm will deactivate few ports of the switches to avoid the loops. This is a dynamic algorithm. Any switch failure or port failure will activate the deactivated ports of the switch. The entire process will continue by taking a single bridge as a base, which is known as root bridge (a bridge with the smallest ID among other bridges).

If attacker focuses on grabbing the authentication of root Bridge, then the attacker can control the required port activation to divert all the data packets through the bridge, which they have created. Hence, Root Bridge should have a high degree of authentication.

Securing wireless LANs:

A LAN without any wire is known as wireless LAN. There are two important components of wireless LANs they are:

- **Access point:** This is the base station connected between wired router and wireless nodes. Each access point will have some range. Any wireless device within the range can be connected to it, as shown in figure 4.1.4.
- **Wireless Clients** are the wireless devices, which get data from any one of the access points.

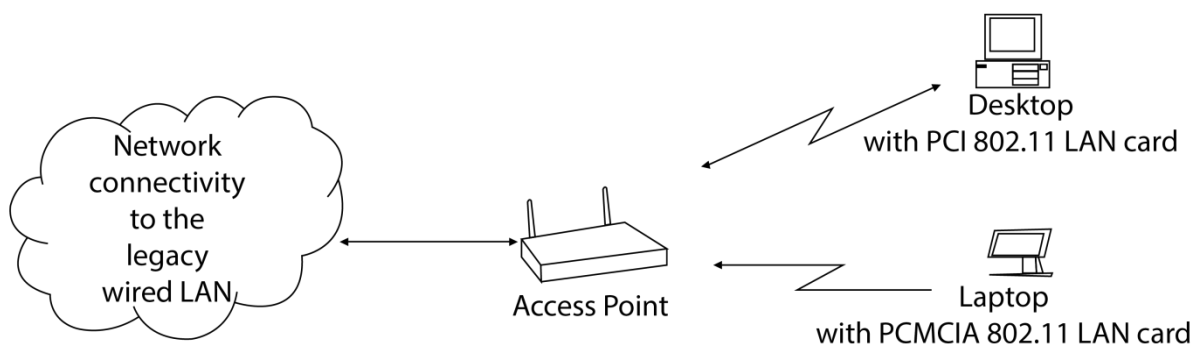


Figure 4.1.4: Wireless LANs

Attacks on Wireless LANs

- **Eavesdropping** – Attack is just to get the data from the network including authentication credentials.
- **Masquerading** – Attacker pretends as authorised user and gets access to the network
- **Traffic Analysis** – Attacker analyses the network data to find the compromises in the network to gain the access.
- **Denial of Service** – Attacker tries to restrict the access to authorised users
- **Message Modification/Replay** – Attacker will modify the message, which it receives and passes to other users.

To prevent these attacks, the following precautions must be taken:

- As all wireless LANs access points are connected to a wired router, installing packet-filtering firewall in a router will secure the wireless LANs also.
- Use more secure password for wireless access points.

(ii) Email Security

Email is the most common mode of communication for most of the organisations. Now a days, it is considered as a valid document because it has all your authentication details and valid source of generations. Most of the attackers choose email as most useful communication point for their attack.

Most of the protocols designed for email transmissions are not much stronger in their security. The classification of email security is as follows:

- **Securing the mail server**

Most of the emails from attackers can stop their penetration into the system, if the mail servers have strong security. Few of the server security configurations are as follows:

- **Configure your mail server without open relay:** Open relay is the mail server setting which allows anyone to send his or her mails through the server. Server with open relay settings acts as a transit point for the mail communication. If mail server has this capability, then it allows the spams to pass through it.
- **Include more authentications to the mail server:** Ask every employee to provide a username and password before sending the email in spite of using auto complete options available within the browser. This helps to avoid spam open relay mails.
- **Limit the number of active connections at a given point of time:** This setting helps you to handle denial of service attack. That is, sending or receiving excessive mails will create a congestion in the network and drops important mail messages.
- **Implement DNS BL:** DNS block list is a list of blocked email ids because they are the spam mail senders. If any new spam mail is found, then record the spam mail id into a block list and finally it attached to DNS for blocking. Hence, mail from that mail id will be blocked automatically.
- **Activate sender policy framework (SPF):** Most of the decoys use a valid sender mail address to send the mails. In this case, even the spam-wares will not be able to detect it. SPF will create the rules in such a way that, even if someone uses the sender's mail id, then it will detect it.
- **Enable SURBL:** Spam URL real time block list (SURBL) detects emails with unwanted links. Having SURBL will block all the emails with unwanted links.
- **Encrypt every mail which is sent or received by the mail server.** It will prevent the information theft from the intruders.
- **Enable all the network firewalls to filter the unwanted mails.**

- **Securing email client**
 - Secure user system with suitable antivirus
 - Secure the system with a strong password
 - Change the password regularly
 - Never open any mail without scanning it by using antivirus
 - Simple PGP encryption can be used for encryption and decryption

Implementation of proper email security will protect the system largely.



Self-assessment Questions

- 1) All the LANs operate in which of the following layer of OSI architecture?
 - a) Application Layer
 - b) Transport Layer
 - c) Datalink Layer
 - d) Physical Layer
- 2) Memory location used by switch to store the forwarding table is known as _____.
 - a) content-addressable memory
 - b) content-accessible memory
 - c) content-acceptable memory
 - d) content-applied memory
- 3) A has requested for the IP address and he has 2 IP address from two servers. What is the reason behind this?
 - a) ARP Spoofing
 - b) Port steeling
 - c) MAC flooding
 - d) DHCP attack
- 4) If attacker attacks the system only for analysing the network data movements, then this attack is known as _____.
 - a) Masquerading
 - b) Eavesdropping
 - c) Traffic analysis
 - d) Denial of service
- 5) 'A' has created a mail server which takes mails from other server and forwards it to another server, then which kind of SMTP settings 'A' has done with his server?
 - a) Enabled with open relay settings
 - b) Enabled SMTP server authentication
 - c) Limited number of active connections at time
 - d) Enable DNSBL settings

4.1.3 Hacking Attacks

Hacking is a process of identifying the weakness in the system or network and get access to the system based on it. During 90's hackers were considered as extreme intelligent programmers. They use to study the system completely and then go for hacking the system. Now a days, availability of more tools for hacking is attracting many of the young minds towards the hacking.

Many organisations are appointing hackers to study the system, before someone hacks it and creates more damage to the system. Many of the young minds are diverting towards the hacking because they feel it is more interesting.

Hacking is not a bad practice until and unless the intentions are wrong. It is always better to safeguard the systems from hackers. To safeguard the system from hackers, it is better to study a brief about hacking attacks and its preventive measures.

Based on the activities performed by hackers, they are classified as:

- **Ethical hacker:** A hacker who finds the weakness of the system and fixes the problem.
- **Cracker:** A hacker who gains unauthorised access to the system for personal use.
- **Grey hackers:** A Hacker, whose role is in between the crackers and ethical hackers. They get unauthorised access to the system, find a weakness and inform the same to the owner of the system.
- **Script kiddies:** these are the hackers who are not professional, but use available tools to penetrate into the system.
- **Hactivist:** These are the hackers, who send social, religious and political messages to others by using hacking software's or websites.
- **Phreakers** are the hackers who focus to hack telephones rather than the computers.

(i) Types of Attacks

Now let us study different types of attacks possible in hacking. Hacking attacks can be classified as physical, syntactic and semantic.

Physical

The attacks that focus to damage the hardware physically are known as physical attacks. These kinds of attacks are very difficult to control because these methods will damage any kind of security enforcements. These attacks are like:

- Using bombs or fire
- Hurting the security guards
- Breaking the doors where secure information is stored
- Stealing of the servers and hard disks, where information is available
- Stealing of password by creating harm to the employees
- Damaging the security cameras

Syntactic

Syntactic attacks are the ways to damage a system by using some malicious software. This software includes virus, worms, malwares and spywares. These softwares are introduced into the system by any means and the software itself can do the rest of the damages. Most of the time, to get the sensitive data from the system, this kind of the software is used. Emails are the best sources to introduce such malicious softwares into the system.

Semantic

Semantic attack focuses on modifying the original information or distribution of wrong information into the system. This process was available even before the computers were introduced, like forgery, duplicate documents, incorrect announcements, etc. In computers, it is very difficult to find the modification done, than the physical modification. Through the computer networks, it is very easy to spread them to all the targets than in physical systems. Most of the semantic attacks will have their effect on decision-making systems.

(ii) Hacking Attacks Countermeasures

- Physical attacks can be controlled by:
 - Using extremely strong security measures like strong locker systems.
 - Security checks for explosive elements
 - Secret cams, danger alarms, hiding servers in stronger security rooms

- Syntactic attacks can be controlled by:
 - Enforce strong antivirus softwares to scan the system regularly and update them regularly
 - Enforce strong email security which avoids threats to enter the system because it is the entry point for many threats
 - Build strong security policy to avoid bringing external storage devices
 - Use only proprietary softwares
 - Configure all the firewalls to avoid the entry of unwanted softwares
- Semantic attacks can be avoided by using:
 - Encrypt each and every message saved in the file system
 - Maintain the modification log for each and every file on the file system
 - Use digital signature for attachment transferred to authenticate the message
 - Enforce strong security rules for all the firewalls to avoid intruders use your system
 - Encrypt every message transmitted over the network
 - Never make any financial transaction until it is confirmed that the website is a valid source

(iii) Hacking Tricks

There are many tricks available for hacking some of them are

- **Spoofing:**

Spoofing is a trick in which unknown and unauthorised users pretend as a known and authorised users. The attacker uses the unsecure portions of the network or system and follows very simple procedures to make them as a part of the network or gets access to sensitive information and uses it to achieve his intentions.

Examples of them are ARP spoofing, DHCP spoofing so on.
- **Malwares:**

Hackers will use chat rooms or emails to insert the malware into the system and based on the intention of attacking, different kinds of malware are created such as viruses to corrupt the system, worms to crash the system and spyware to collect the information. Chat rooms are an easiest way to penetrate into the system. The attacker will send a file into the system and then installs it without the notice of the user.

- **Phishing**

Phishing is a trick of collecting the personal information of the users. The attacker uses websites, phone calls, email and many other ways to collect the personal information about the user. Based on the collected information, the attacker may crack your password, go for identity theft, etc.

- **Electronic bulletin board**

Electronic bulletin boards are forums designed to discuss IT related problems and its solutions. These kinds of forums can also be used for hacking. Are you shocked? Let us see how it happens. The hacker will provide the solution for most of the IT problems. Their suggested solutions will be in such a way that, you will be changing the firewall settings, executing the programs suggested by them, make changes to the program according to their instruction and so on. This solution will create vulnerabilities in system and opens an opportunity for attacks.

- **Information brokers**

Information brokers are the individuals or organisation, which sells the information for some charge, but they sell the information only for known and genuine cause. But some attackers procure this data from different sources and accumulate them to get more information. With the base information available, they will make fake calls and get the remaining information. They also send attractive prizes and collect your proofs and bank details. With all this information, they penetrate into bank accounts and steal your money. Some of them can use your information for criminal activities.

- **Wormhole attack**

This trick is commonly used by the professional attacker to grab the message flowing from the node. In this trick, attackers will create a fake router and present it in such a way that the path from source to destination through that router will be very minimum distance. This confuses the routing protocol and allows the messages to flow through it. Professional hackers will use this information to grab the personal information available in the message, if it is not encrypted and use this information to attack the systems.

- **Internet Public Records**

Governments of many countries will sell the public details of the jurisdiction for good causes. This information is used for research activities and by NGOs for the welfare of the people. If this information goes into the wrong hands, it can be misused.



Self-assessment Questions

- 6) Among the following hackers, who is not a professional hacker, but they hack the system by using tools?
 - a) Ethical hackers
 - b) Crackers
 - c) Script kiddies
 - d) Hacktivist
- 7) Which of the following is not a type of attack?
 - a) Physical attack
 - b) Syntactic attack
 - c) Semantic attack
 - d) Syntax attack
- 8) In which kind of attack hacker will manipulate the original document?
 - a) Physical attack
 - b) Syntactic attack
 - c) Semantic attack
 - d) Syntax attack
- 9) In which of the following hacking trick, hacker pretended as an authorised user to access the resources of the organisation?
 - a) Spoofing
 - b) Information broker
 - c) Malwares
 - d) Wormhole attack
- 10) In which of the following technique, the hacker creates a duplicate document which appears as an original document to collect your information?
 - a) Spoofing
 - b) Phishing
 - c) Electronic bulletin board
 - d) Wormhole attack

4.1.4 Approaches to Hacking

The present era is using the internet for their business activities. At the same time, intruders are designing and implementing various techniques to hack the secure information available. The various approaches for hacking are:

(i) Physical Intrusion

Physical attack refers to damage of physical property such as system, resources of the organisation. Sometimes, the loss or damage ranges from minimum to maximum. The loss or damage can happen with either the human interventions or natural calamities such as flooding, earthquakes or building demolition.

Internal and external person may perform physical hacking. If the person is an insider, then they will not implement many procedures like external hackers. Since the users are internal to the organisation, there will be at least a minimum level of organisational assessments, whereas for external users they have to design various methods to perform the physical intrusions.

Physical intrusion approaches are:

- **Through access cards:**
Gaining the access in the wrong way to enter into the organisation, if the organisation is using the access card system. In this method, either they will create the duplicate access cards or they may steal the original access card of the employees and finally damage the resources of the organisation.
- **Compromise with the insiders:**
If an organisation using the traditional security system such as a security guard, then it is easy for the hacker to perform physical intrusion. In this case, the hacker show benefits to the security person to gain access or enter inside the organisation.
- **Stealing the password:**
If the organisation is password centric, then the hacker steals the password of any employee to gain the access of the organisation.
- **Breaking of security system:**
In this case, the attacker damages the security system to gain access into the organisation and damage the organisational equipments.

So, these are the various methods used by the intruders. If an organisation is planning to implement the security system, they also need to consider the approaches for physical intrusion. Based on the intrusive methods, they should implement a powerful security system to avoid such problems in the future.

(ii) Password attacks

Password hacking is a tremendous weapon used by the hackers to hack the system. If an organisation is using the vulnerable networks, then it is very easy for the attackers to gain the information of an individual or organisation.

In this hacking technique, hackers use the three powerful weapons to hack the password they are:

- **Password sharing:**

The method works based on the sharing of passwords with others. For example, despite of security policy, most of the employees share their password details with their colleagues to keep and maintain the working status ON. Such situations may result in trust issues and sometimes creates a danger of using your password to access all the resources, which others cannot access through their credentials.

Employee for their benefits, with ignorance and trust, reveal their password. Sometimes it will create great problems and punishments to the original employee.

- **Password capture:**

This is the method used by the hackers to retrieve the passwords. In this case, they will use some other equipments to capture the passwords such as key loggers, camera fixing at hidden places, additional popups and some network monitor software's.

- **Password guessing:**

Guessing is the popularly used technique by hackers to identify the passwords of any ones. Basically, they guess the personal information of users such as names, surnames, children's names, company names, important dates or with vehicle numbers to identify the password.

Along with all the techniques given above, the hackers use other approaches for password hacking. Few approaches are given below:

- Hackers create the fake sites to get the password details. The users cannot differentiate such sites because they look almost same as the original site with one or two character differences. Ignoring such details, the users may provide all the details. This is known as phishing attacks.
- Few members having the habit of writing their passwords in some book or paper. So stealing those documents can reveal the passwords.
- Hackers use the traditional dictionaries and try every word that appears in the dictionary to check whether if it is the password. If all the words are completed and does not match, then they try other methods. This technique is considered as a dictionary attack.
- Based on trial and error methods, the passwords are identified and access is gained, which is termed as brute force attacks.

(iii) Network Access and Web Server Attacks

It is not that simple to hack the network or web server. Hackers use various techniques to gain the access to the organisation servers. Many organisations are using the internet concepts to make their work simpler. So hackers are trying to access them through the internet. Since companies are sharing the data through the network, if hackers successfully trap the network, then they will gain the access to the organisation.

Most of the hackers are computer professionals, who implements several techniques on a day-to-day basis.

The approaches used by the hackers to perform the network hacking are:

- **Virtual Private Network (VPN) attack:**
Now a day's most of the companies are using the concept of work from home to facilitate the remote access methodology. To implement this, the organisation IT departments are setting up the virtual private networks. When the organisation is using VPN concept, the IT department people provide the username and passwords for their employees to connect to the organisation network. In this method, hacker collects the basic information of the authenticated user. By using this, the hacker calls the IT people for password, projecting he/she is the authorised user to gain the access by providing

some details. If provided details are correct, they will gain the access and collect information from anywhere and anytime.

- **Chat Technique:**

In this method, the hacker connects to the people through social engineering sites, as he/she is well-known person or authenticated person. With this, they will collect the details from them. In most of the cases, the victims are newbies, who are the members using the network for the first time. In the initial stage of network usage, they will continuously contact or send the messages to service providers. Therefore, the hackers create the fake accounts with the name of service providers and start chatting with such people.

The customers will think that other side person is the correct user and provides the required details to them. With this technique, finally the hackers gain access.

- **Denial of service (Dos attack):**

In this method, the hacker creates the unwanted stuff in the network path, which will create the congestion in the network. With this, sometimes the switching devices completely drop the packets from all the sources. The hacker will make arrangement to access the dropped packets. Those dropped packets may include a lot of valid information. Using this, the hacker can gain the source details and later send the packets by projecting their packets are from authenticated sources.

- **Sniffing:**

In this technique, the hacker uses monitoring tools to get the required information. These tools provide the packet information, network topology, IP address of source and destination ports. It also provides the details about the security measures implemented in the organisation, type of packet information and these are few to list.

- **Web server attacks:**

A web server is software, which stores information (usually web pages) and allow the users to access it through the internet or network. Organisation information stores in the webserver. Now a day's most of the commercial sites allow their customers to purchase the products online. These sites store the important information about their customers along with the credit card details in their servers and becoming richest targets for attackers.

Intruders find the faults in the system such as default settings in the system, bugs in the operating system and servers, misconfiguration of a network and lack of security policies and procedures. Hackers are using various approaches to hack the web servers.

Types of Attacks against Web Servers:

- **Pharming**– in this attack, the hacker compromises with the Domain Name System (DNS) or with the user of the computer to divert the organisation network traffic to the fraud server to gain the access.
- **Directory traversal attacks**– in this attack the hackers enter in to the webserver regions by finding loopholes in the system. Once the decoy enters, then they will install the malicious softwares to collect and spoil the web server files.
- **Sniffing**– in this approach the hackers implement the procedures to convert the encrypted data to plain text to gain the access rights to access the server.
- **Phishing**– In this attackers creates the impersonate sites and divert the network traffic to this false sites. With this, hackers gain the sensitive information of users such as their names, phone numbers and credit/debit card details.
- **Domain Name System Hijacking** – With this technique, the attacker changes the settings of DNS to locate the web server of hackers. All the network traffic is directed to the attacker's web server and gives the chance to collect the various information regarding the assets of many peoples.
- **Defacement**– in this type of attack, the attacker substitutes the organisation's website with other websites that contains the hacker's details.

Email attack approaches:

Email is the richest source for the attackers to gain the information of the users or an organisation. Email attacks top the list in cyber crimes. Basically, people maintain their valuable and important information in their mails. So, hacking email will benefit the hackers. For example, many banks are providing online services to their customers, through which he/she can operate their accounts using internet. During this transaction, customers will get the one-time passwords and confirmations to their emails only. Therefore, the hackers are now targeting the emails to collect such vital customer information.

Decoys use various techniques to attack emails. Many persons will think that spam filter will filter the unwanted mails and it protects their email system. However, the intruders are using the various approaches to hack the emails. Few approaches are:

- **Phishing:**

Phishing is the powerful weapon used by the attackers to hack the person's emails. In this technique, the hacker sends a mail pretending as a known sender to create a threat to the user.

- **Distributed Spam Distraction (DSD):**

This is one of the prominence attack used by the attackers, which is also known as "spam blizzards". This DSD technique will flood the users email inbox with thousands of unwanted mails. The approximate figure is 60000 mails within 12 to 24 hours. To jump out of this issue, the user selects the unread messages and deletes them at once. There is a chance that along with this unwanted mails the victim will delete the important messages. The hackers write a code for retrieving deleted messages, so with this there is a chance for decoy somehow to get the person's details.

- **Bypass email filtration:**

Many of the internet users using the antivirus softwares for securing their data over the internet. They also have a wrong thought process that the spam folder filters all the spam messages. Taking this as an advantage, the attackers are using this technique to spam the mails, which will not enter in the spam folder and reside inside the inbox. Through this technique, there is a chance that the user may respond to these nonsense mails by providing their details.



Self-assessment Questions

- 11) _____ is the technique used by attacker to flood the user's inbox.
- a) Phishing
 - b) Parsing
 - c) Cracking
 - d) Distributed Spam Distraction
- 12) Retrieving the password by using trial and error method this technique known as ____.
- a) Dictionary attack
 - b) Brute force attack
 - c) Parsing attack
 - d) Flood attack
- 13) _____ is the method used by the hacker to be pretended as original user to the victims through the continuous interaction to gain the user details.
- a) Parsing
 - b) Morphing
 - c) Chat technique
 - d) DSD
- 14) In the pharming attack the hacker compromises with ____.
- a) Domain name server
 - b) User
 - c) LAN
 - d) Email
- 15) A hacker replaces the original site with duplicate site, which can be called as ____.
- a) Phishing
 - b) DNS Hijack
 - c) Defacement
 - d) Entrapment



Summary

- Internet security will be strong enough only when its core components are strong.
- LANs are the components of data link layer where most of the protocols have no security by default.
- ARP spoofing, DHCP attacks are few attacks which will be a threat for LAN security.
- Email security can be achieved if and only if email server and client are secure.
- Several server settings are available to secure the email servers.
- Attacks can be classified as physical, semantic and syntactic attacks.
- Physical attack is meant for physical damage, syntactic attacks will focus on malware attacks and semantic attacks focus on message modification.
- Spoofing, phishing, malware, electronic bulletin boards, information brokers, wormhole attacks are few hacking techniques.
- Attackers use various approaches to hack the details of individuals or organisations such as phishing, chat technique, dictionary attack, VPN attack, DOS attack, DNS hijacking, defacement, distributed spam distraction, bypass email filtration, etc.



Terminal Questions

1. Why LAN security is important? Explain few attacks on wired LANS.
2. Email security critical for any organisation. Justify.
3. What are the different types of attacks and how can the system be safeguard from those attacks?
4. Compare and contrast the techniques used by the hackers for password cracking.
5. What is bypass email filtration? How intruders gain access using this method?



Answer Keys

Self-assessment Questions	
Question No.	Answer
1	c
2	a
3	d
4	c
5	a
6	c
7	d
8	c
9	a
10	b
11	d
12	b
13	c
14	a
15	c



Activity

Activity Type: Offline

Duration: 30 minutes

Description:

Identify and list hacking attacks other than the discussed hacking attacks and create a document on them

Case Study

Myfootware Corporation wants to enter into an online business. All the products they have are listed on their websites. Every customer can see all the listings of products available, but if they want to purchase the products, then they must register themselves by using their personal information.

To provide this online service, myfootware organisation has been divided their network into 5 LANs. Out of them, 3 networks use Ethernet and 2 of them use Wi-Fi 802.11g. All the systems in the network get their IP addresses from the DHCP server. Out of 5 departments, the department which takes care of designing the footwear are not allowed to use the internet because their creativity will be duplicated, if the design information is leaked to the outside world.

Design section will interact with other departments only through email. Sales team uses Wi-Fi because they need to move to each and every department to know the status of their orders and inform the same to the client.

Business started expanding and they were getting huge orders. Then they incurred few issues in their networks, such as too many spam emails, most of the emails are reaching very late, most of the chatting messages were having unknown links, corrupted documents, etc.

Management has decided to analyse the system and secure the system

- a) Could you suggest some security measures that need to be followed by the organisation to avoid the email problems?
- b) What are the possible security threats for the sales team and how can you avoid them?
- c) The design section of the organisation has no connectivity with the external world, but still many spam mails are generated. Could you analyse what could be the reason behind it?

Bibliography



e-References

- *Hacker Attacks*. Retrieved 18 Jan, 2017 from <http://www.infoworld.com/article/2610239/malware/7-sneak-attacks-used-by-today-s-most-devious-hackers.html>
- *Password Cracking*. Retrieved 18 Jan, 2017 from https://en.wikipedia.org/wiki/Password_cracking
- *Hacking Techniques*. Retrieved 18 Jan, 2017 from <http://www.computerworld.com/article/2563639/mobile-wireless/wireless-hacking-techniques.html>

Image Credits

- Figure 4.1.1: <https://tournasdimitrios1.files.wordpress.com/2011/02/arp-spoofing.png>
- Figure 4.1.2: https://secit.sk/sites/default/files/lan2_2.jpg
- Figure 4.1.3: <https://danuwi.files.wordpress.com/2014/12/dhcp-snooping-flow1.png>
- Figure 4.1.4: <http://www.slideshare.net/victerpaul/8-80211-wireless-lan>



External Resources

- Whitman, M. E., & Mattord, H. J. (2016). *Principles of information security*. Australia: Delmar.
- Stallings, W. (2011). *Network security essentials: applications and standards*. Boston, MA: Pearson.
- Spivey, M. D. (2012). *Practical hacking techniques and countermeasures*. Boca Raton, FL: Auerbach.



Video Links

Topic	Link
LAN Switch Security	https://www.youtube.com/watch?v=JNTsd7w-Ibk
Email Security Failure	https://www.youtube.com/watch?v=D8o9CT6JRq8
Types of attacks	https://www.youtube.com/watch?v=4BNgels4_8k



Notes:



Chapter Table of Contents

Chapter 4.2

Preventive Measures for Hacking Attacks

Aim.....	211
Instructional Objectives.....	211
Learning Outcomes.....	211
4.2.1 Introduction.....	212
4.2.2 Planning for hacking incidents.....	212
Self-assessment Questions.....	217
4.2.3 Hacking Prevention Methods.....	218
(i) General Prevention	219
(ii) Website and software.....	220
(iii) Email Accounts	222
Self-assessment Questions.....	224
4.2.4 Damage Limitations.....	224
Self-assessment Questions.....	226
Summary	227
Terminal Questions.....	228
Answer Keys.....	229
Activity.....	230
Case Study	231
Bibliography.....	232
e-References	232
External Resources	232
Video Links	233



Aim

To familiarise the students with the concepts of hacking prevention methods from threats and damages caused by hacking the resources of an organisation



Instructional Objectives

After completing this chapter, you should be able to:

- Explain various preventive measures to avoid attacks by applying plan on the hacking incidents
- Enumerate various preventive measures from threats
- Elaborate on the damage limitation caused by various types of attacks on the information



Learning Outcomes

At the end of this chapter, you are expected to:

- List various preventive measures for avoiding attacks by applying plan on the hacking incidents
- Identify methods and tips to prevent system from attacks
- List how to limit the damages caused by hacking

4.2.1 Introduction

In the era of internet, network scaling is highly required. As the scaling of the networks happens, the possible threats will also increase. As the threats are increasing, organisations have to spend sufficient amount of time and money in securing the system. By creating a preventive platform for the threats, organisation can have a safe breath for a while.

Organisation have to give importance to plan against hacking otherwise their existing security software's may not be helpful for them always.

This chapter starts its discussion with organisations planning to handle the hacking attacks. It also provides various preventive measures to handle the different hacking incidents. Finally, we will learn about various simple procedures used for minimisation of damages caused by hacking the organisation resources. This chapter concludes with damage limitations.

At the end of this chapter, students will be able to estimate the need of planning against hacking, understand the preventive methods for avoiding the attacks and damages caused by hacking the information system.

4.2.2 Planning for Hacking Incidents

Any organisation or individual is not an exception from the hacker's attack. Hackers will not leave any possible chances for intruding the system. Their mind will be always searching for new intrusion systems and new vulnerabilities. It is highly difficult to track or trace their ideas, but it is definitely possible to plan your system to prevent them from their intervention.

Planning for hacking incidents is a continuous process because, hackers always change their plans and actions -Plan for all possible type of attacks that the hackers may use; it may be physical, syntactic or semantic. Hacker majorly tries to enter the system through any of the communication channels. It can be emails, chat rooms, file downloads, file transfers, etc.

Always use the technique "stop the hackers for stealing before they stops you"

Most of the organisations plan their security system for any hacking incidents, which can be named as incident response plan (IRP). Incident is nothing but hackers' attacks like malware, phishing, spoofing, etc. This plan operates with a dedicated team whose aim is to continue business without any hiccups, even if any incident occurs. This planning team organises trainings and workshops for every member of organisation.

Common responsibilities of IRP team are:

- Identify the hacking incidents, which can be any type of attack
- Resolve the incidents as quickly as possible
- Safeguard all the assets and minimise damage
- Recover the system from the hacking attack to the safe state
- Minimise future risks for the organisation
- Prepare documents for each and every incident for future reference

IRP follows methodology for resolving the incident. Let us try to understand one of such methodologies designed by National Institute of Standards and Technology publication (NIST). This methodology divides the overall process into six phases as shown in figure 4.2.1

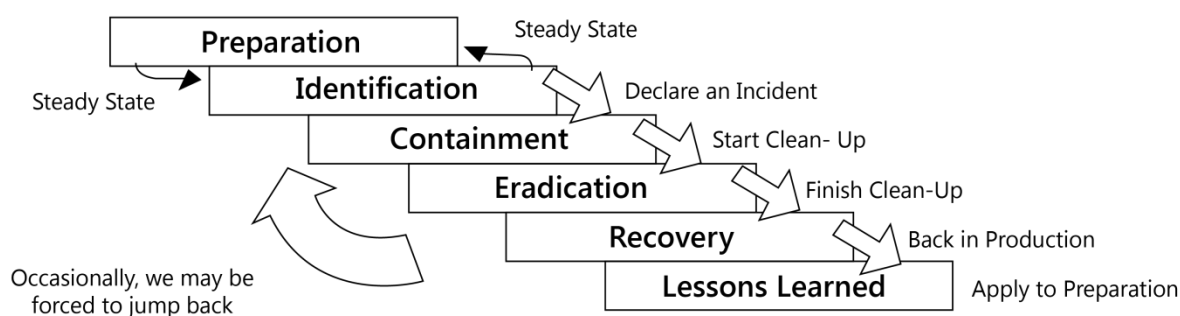


Figure 4.2.1: Methodology for IRP

Preparation phase:

In preparation phase, they will form a team, which is responsible for handling the incidents. Assign roles and responsibilities to each team member. Define a tracking procedure for the incident reported, so that every team member knows what others are doing. The tracking procedure may use many common documents or tracking software based on the availability of resources. Plan for all the required softwares and trainings to handle the incident.

Identification phase:

This is the trickiest phase because different incidents are identified by using different approaches. Some of the incidents are extremely difficult to identify. After identifying the incident, check whether the incident occurred is a positive incident or negative incident. Positive incidents are normal transactions, which will not create any problems to the system or

normal transactions of the organisation. Negative incidents are the incident, which have some negative implication to the organisation or the incidents of hacking.

If any negative implication is there, then calculate the risk involved with the incident by using the formula:

$$\text{Risk} = \text{Threats} * \text{Vulnerabilities} * \text{Impact}$$

Rank the incident based on the risk value if the risk value is very high, check for few factors like:

- Do we have sensitive information available as an evidence to handle the incident legally?
- Does the incident have any impact on other portions of organisation network? It could be interoperability between the different department activities.
- Is the impact of incident visible? Most of the incident impacts are not visible for extremely long durations.
- Does the incident resolution need any economic requirements?

If sufficient team members are required and software tools are not available, then go back to preparation phase and check for the resource availabilities. After accommodating all the resources, then come back to the identification phase as shown in the figure 4.2.1

Containment phase

This phase focuses on suppressing the incident before it creates more impact than expected. After identifying and analysing with the data available in identification phase, the Subject matter experts of the organisation will take a call on containment of incident.

Few containment procedures are as follows:

- Shutdown and disconnect system where incident has been identified. This is not a wise procedure, if the incident happened at the operational servers.
- Change the firewall settings based on the new incidents to stop the impact of it.
- Disable few functionalities of the system, where the incident is identified.
- Notify all the departments of the organisations about incident and provide the details of incident and ask them not use that functionality until IRP team intimates them.
- Ask all the departments to save their working status.

See to that the containment procedure followed will have very limited effect on the business continuation. The impact of incidents can be high in few business scenarios.

Eradication phase:

After containment of the incident, to spread further, it is necessary to eradicate or remove the incident effects.

Following actions used to eradicate the incident:

- Restore the system to a safe point
- Rebuilding the system from start
- Replace the infected files with clean back up files
- Install operating system and antivirus patches
- Change all the passwords
- Change the firewall rules
- Include incident source to the block list
- Add more security at the core network layers
- Restore the registry file settings to default Educate every member of the organisation about the incident
- Conduct internal security audit to check for any security requirements

Recovery phase

The goal of this phase is get back the operation process to initial phase. After eradication of incidents, all the effects of the intrusion need to get back to the safe state. SME of the IRP team has to confirm the system can continue its operations. SME need to conduct a lot of internal security audits before confirming the future operations. In very few cases, the impact of hacking incidents cannot be recovered. This is considered as damage. To avoid this in future, team again goes to preparation phase as shown in figure 4.2.1 and analyses the new requirements to avoid the damage again.

- Follow safe recovery procedures
- Document all the activities of IRP team
- Review all the backups for assurance
- Check for all the communication channels

Lessons Learned Phase

This aims to document all the incident impacts. IRP team will pull all the evidences and incident impacts. This review document comprises:

- What happened?
- How it has happened?
- Damage done by impact if any?
- Possibilities of reoccurrences
- What actions of the team were correct?
- What actions of team went wrong and what were the reasons for it?

This document helps the team to handle future incidents. If this document has sufficient evidences, then a file a legal case against the intruders. This document also helps in making the security policy, because many times incidents happen with the actions of internal users. Therefore, this document helps in future trainings regarding the incidents.

IRP is applicable for the organisation, whereas the individuals should also plan their system for hacking attacks.

- Every individual who are making their transactions using internet have to secure the system by using anti viruses and proprietary operating system.
- Must scan each and every storage devices connected to the system before copying the files.
- Systems that are used by kids must be monitored and scanned again and again.
- Open all the banking and online websites by remembering the website address rather than searching them through search engines.

IRPs are the best planning done and practiced but hackers are still successful if they can cross the identification phase. IRP is not a simple process to follow because having a dedicated team to handle the incidents may not be affordable for all the organisations. Hence, most of the organisations prefer to use general preventive techniques as the base plan to handle the incident.



Self-assessment Questions

- 1) IRP designed by NIST has how many phases?
 - a) Four phases
 - b) Five phases
 - c) Six phases
 - d) Seven phases
- 2) Which phase of IRP focuses on requirement analysis?
 - a) Preparation phase
 - b) Identification phase
 - c) Recovery phase
 - d) Containment phase
- 3) What is the formula for calculating the risk value?
 - a) Risk= Threats * Vulnerabilities * Impact
 - b) Risk= Threats * Number of impacts * Impact
 - c) Risk= Number of Threats * Number of files corrupted * Impact
 - d) Risk= Number of vulnerabilities * Vulnerabilities * Impact
- 4) In identification phase, if any requirements are needed then IRPs again goes to _____.
 - a) Preparation phase
 - b) Identification phase
 - c) Recovery phase
 - d) Containment phase
- 5) Which phase of IRP focuses on bringing the system back to safe state?
 - a) Preparation phase
 - b) Identification phase
 - c) Recovery phase
 - d) Containment phase
- 6) Which of the following is not an activity of hacker?
 - a) Malwares
 - b) Identity theft
 - c) IDPS
 - d) Phishing

4.2.3 Hacking Prevention Methods

Hacking is the process of attaining the access to the unauthorised resources. The word hacking creates tension to every member, to secure their resources from unauthorised members. It is not so simple to recover their resources from hacking. Therefore, it is advisable to implement preventive measures than recovering.

“If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked?” — White House Cyber security Advisor, Richard Clarke.

Computer hacking can be done in a number of ways such as Email hacking, personal system hacking and blog or website hacking. According to university of Phoenix a survey on hacking is done, where 67% of United State people are aware of the fact that their accounts are hacked by the hackers. In most of the cases, victims of hacking are social engineering site customers.

Users can implement the preventive measures for securing their assets. The preventive measures should deploy at various levels and it should be in continuous fashion.

The organisation must implement certain policies to safeguard their system. The following are the few security measurements that should be implemented by the top-level management:

- Minimise the communication channels or scan all communication channels with antivirus and accept the files on success from the scan.
- Don't run any installation files until you confirm with system administrators.
- All the software's must be downloaded or used from the valid sources.
- Clear the temp files of the system repeatedly, because it is the home for most of the malware.
- Any installation planning must need administrator's approval.
- All pen drive or external drive access must be notified to the system administrator.
- All attachments of emails must be scanned with antivirus before opening.
- Block list must be maintained to block all the sources, which tries to intrude the system with malware.
- Along with the above, one can design the layer of security.

By following a few general preventive techniques, impact of hacking can be minimised. Some of them are as follows:

(i) General Prevention

Preventions to safeguard their resources from hacking are:

- **Implementation of strong security policies:**

Every employee of the organisation must protect the information asset. It is the duty of organisation to design the policies and the same to be disseminated among employees. Periodically, they should conduct the sessions to educate and to provide the awareness about these policies. Restrict user access to the information resources, based on some rules.

- **Installation of updates at proper time:**

In most of the cases, due to the busy schedule or negligence, users skip the updates, either regarding to the operating systems or web browsers. However, installing the updates at appropriate time will safeguard their system from attackers.

- **Password protections:**

Always protect the resources by using strong passwords. Many people use very simple passwords, but this is not recommended. Since hackers are the professionals, do not keep the password quite simple, else in a very little span of time hackers can crack the passwords. Try to use lengthy and complex passwords so that others cannot hack and use your password-protected assets. Change the passwords very often.

- **Install proper security system using firewalls:**

As everyone knows, the firewalls are available in all varieties based on their needs. The need may be protecting small house with single system, home with multiple systems, organisation with large set of systems, network monitoring, packets filtering and implementing proxy system to name few. So for each and every need, there is a solution from firewalls. So identify the need and install the proper firewalls for protecting them from attackers.

- **Install anti- adware /spyware programs:**

The adware program is not complicated as virus and worms, but it will continuously display the advertisements/ads on browsers. Sometimes, these ads irritate the users, disturb their work and reduce the quality of effort. Few adware programs change their names as soon as it gets installed in the system, which is difficult even to uninstall. On the other hand, spyware program monitors the user activity and copy the passwords for

illegal purpose. Many people think that anti spyware and adware software's are not required. However, it is always good to install anti spyware and adware programs to safeguard themselves.

- **Installation of proper antivirus software:**

Install the antivirus software in the system to safeguard from hackers. This software scans downloads to find the inappropriate content, any external devices like pen drives, CD's, DVD's and hard disk connected to the system for malicious code. It will monitor and take required measures to overcome from it.

- **Two-way authentication:**

Always do not depend on the single authentication system. It is better to rely on two-way authentication system. In a two-way authentication user has to cross the two levels of authentication to access the asset.

Example: Now-a-days banking system is working on this two-way authentication system, one is regular password and another is one time password (OTP) which will be sent to mobile and registered emails. By using a combination of password and OTP, they can perform their transactions in their accounts.

- **Backup of data:**

After taking all the precautions, it is always better to maintain the backup copy of data. Based on the size of data, different persons use different time intervals for taking backup of data. So backup may be taken on daily basis, weekly basis, fortnight basis or monthly basis as required.

(ii) Website and software

- **Limit the access to web server:**

Information of the website is stored in the web server. So, never give a chance to the people to directly access the web server. Provide very limited access only for few authenticators. Provide the proxy server concept for normal users, to protect main web server from the threats. See to that number of transactions should be limited while working with web servers.

- **Do not use admin as a password for websites:**
Many website owners do the blunder, keeping same admin as username and password. Website creators use admin as temporary username as well as password. Once the website is hosted, then it is mandatory that to change this username and password by the website owners.
- **Use encrypted services:**
Any data transfer between web server to the system and vice versa should be encrypted using encryption technologies. Due to this, even if the information is in the hands of hackers, then also it is difficult for them to get the original information. Even extensions of these encrypted services up to user's authentication level will provide more security.
- **Avoid auto-form filling and auto connects options:**
Never give the auto form filling servicers to your legitimate users. Most of the attackers collect sensitive information from these forms only. Many web browsers are allowing the users to save their data and password. If your website is having this option, disable it.
- **Do not store sensitive data without any protection:**
Web pages are stored in the web servers. Provide very tough security for the web servers by installing various protection or antivirus software. Web pages many times connect to the important details.
- **Provide alerts for suspicious activities:**
Websites must provide the alerts to the users about suspicious activity. Most of the websites are providing this nowadays, when users are trying either upload or downloading the content through their websites from various sources.
- **Layer security methodology:**
Do not rely on single security component. Provide security measures in level-by-level fashions. With these levels of security, even if one level security fails to monitor the threat, then other levels will take care to identify the threats. If possible, place the web server in the defence of depth zones.
- **Verification of advertisements:**
To generate more income most of website owners are allowing others to post their advertisements (ads). In this case, it is the primary duty of website owners to thoroughly check the ads for malicious code before hosting into their website. Later, if any problem comes with the ads, they should not blame the ads owners. Therefore, it is always a good practice to do content checking before hosting into the websites, because even a small negligence will create a lot of damage to them.

- **Perform PCI scan at regular intervals:**

Periodically, perform peripheral component interconnect scans for checking the loopholes in the system. PCI is used to connect hardware device to the systems. Therefore, it is better to install the powerful device control mechanisms to monitor and maintain the connected device details.

- **Patch the systems with latest updates.**

To provide more security based on the trends or needs, every software vendors releases the service packs or patches to the software's. This patch information will be intimated to their valid customers through popups or mails. To keep the system in safer state installs the updates immediately. Users can also enable the "auto update installation option" under the PC settings, which will automatically install the recommended updates in the system.

- **Keep the sensitive data out of the cloud services:**

Cloud is the modern trend to store the data. So, before storing the data in the cloud ensure that, the vendor of the cloud provides the required security. Very few cloud owners are providing encryption for data. So, if encryption facility is not there, do not keep the sensitive information in the cloud, instead maintain it in the secure place.

- **Delete the cookies data:**

One of the biggest sources for attackers to gain some information is cookies. Cookies are small working areas or files in the browsers containing modest information about the activities by the client or server. Sometimes there is a chance to the intruder to get some details from the cookies. If the users Use the internet cafes for their activities, then there is a chance to the hackers to gain some details from these cookies s. So, delete the cookies once the work is finished and delete the history in the browsers.

(iii) Email Accounts

Email accounts are the gateways to personal life and richest targets for cyber criminals, intruders and hackers. Emails are also used to steal your sensitive information, right from social engineering to e-commerce. Though most of us are using the powerful antivirus software, still email hacking is common.

One of the computer professional John McAfee mentions in the IBTimes.co.uk that

"Email accounts are the fundamental identifying elements of the internet. The assumption is that if a person has access to an email account, then that is the real person. Yet these accounts are the easiest elements of the digital world to hack into,". Therefore, it is very important for

every individual to secure their emails from the hackers by implementing the preventive measures.

Few measures are listed below:

- **Consolidation or deleting the old accounts:**

Many people maintain the multiple email accounts to connect to the outside world. However, out of these accounts very few accounts they will operate; remaining they will not. If such kind of unused accounts are there, then one should delete those if it is not required further.

- **Do not use open Wi-Fi:**

Most of us are using Wi-Fi technology to connect to the internet. Many people do their money transactions or checking mails in their gadgets like mobile, tabs, etc. by connecting to the Wi-Fi. Do not connect your gadgets if open Wi-Fi networks are available. Always try to connect for authenticated networks. To hack the details, this is the simple trick used by hackers by providing open networks.

- **Delete emails from unwanted users:**

Do not respond for the mails from unknown senders. Now-a-days most of our inbox is appearing with a mail comprising the prize amounts. Do not give reply for these attractive mails. It is better to delete those mails immediately.

- **Make sure your passwords, security questions and answers are strong:**

Very often change the passwords and also make sure that your answers for security questions are unpredictable by any one.

Protecting the data from hackers is important duty of individual. So, follow the security methods to secure your data from the spys. Do not keep your data in their hands.



Self-assessment Questions

- 7) Which of the following program continuously provides ads through pop-ups to the users?
- a) Spyware
 - b) Adware
 - c) Middleware
 - d) Ads container
- 8) Which of the following is not the security measure for web server?
- a) Installing the proxy server
 - b) Installing antivirus software
 - c) No limit for access the web server
 - d) Use of two-way authentication system
- 9) Cookie is a ____.
- a) Small program to store the session data
 - b) Operating system
 - c) Antivirus software
 - d) Malicious data
- 10) PCI stands for ____.
- a) Peripheral computer interconnect
 - b) Peripheral component interconnect
 - c) Peripheral component internet
 - d) Peripheral component identifier
- 11) Encrypted data means ____.
- a) Redirection of data from the hands of hackers
 - b) Deletion of data by maintaining back up
 - c) Change of language settings in the system
 - d) Converting data from readable to unreadable

4.2.4 Damage Limitations

After a long list of preventive measures, we will be in an opinion that, if the user follows all the preventive measures then hackers will never enter into the system. It is better not to underestimate the power of hackers. Even after following so many preventive measures, still hackers will find a new way to enter the system and corrupt the system.

Many time hackers attack will focus on creating the damage to the system. Proper planning would have stopped them to enter into the system. Most of the times these incidents cannot be observed or identified by the user until it show its effects. There are many legal cases recorded and several victims who had shut down their organisation due to small intrusions.

It is not possible to stop the hackers in all the cases, so it is better to plan a system in such a way that the damage created by the hacker can be minimised. Anyone can use the following simple procedures for minimisation of damage.

Following are few damage limitation techniques identified:

- Infected system is like a slow poison. If you could not recover the system from the damage, it is always recommended detaching the system from the network, until it is recovered from the attack. This is not a correct recommendation if the infected system is a server. Hence, it is always better to maintain replicated servers, which can be switched into the system at safe state and business can be continued.
- Log files are very important ways to limit the damage. Create log for every operation of the computer. This log will help to bring the system to safe state. Just creating the log file is not enough to limit the damage but also to recover the data from the created log files is important. Separate log files must be created for operating system, database system and web servers.
- Create intrusion detection and prevention system (IDPS) that will give the signals of intrusion, so that users can be alert to take the required preventive action against the hacking and this will limit the damage.
- Honey pots, honey net and padded cell system are the software's, which create the illusions to the hacker that they are gaining some details from the organisation. Originally, this software was used for counter-attacks to limit the damages by trapping hacker that collects the hacker details. These details will give the chance to the organisation to proceed legally. Some organisation uses these trapping details for implementing the filtration rules by adding them to block list.
- Security audits are helpful in checking the damage limitation policies implemented by the organisation. If any identified vulnerabilities are there, then they will highlight these issue and see to that the gaps are covered.
- Revealing the information is also damage to the organisation. Hence, this can be limited, if all the data transmissions are encrypted. This helps the organisations to protect the information leakage.

- It is also good idea to appoint an Ethical hacker to identify all the possible intrusions before some hacker tries to collect the information. If ethical hackers are successful in penetrating into the system then make alternative security measures based on their inputs.
- Planning for a damage limitation is a very good approach to keep the system in safe condition. So always, take the expert advices to implement the strong security measurements to safeguard their systems from hackers.



Self-assessment Questions

- 12) What would be the consequences, if damage limitations were not planned?
- a) All the resources of organisation will be safe
 - b) Organisation will never encounter any damage
 - c) There is chance for damaging the resources of the organisation
 - d) Damage limitation has no effect for the safety of resources
- 13) Which of the following tools are used to limit the damages?
- a) Viruses
 - b) Spywares
 - c) Logs
 - d) Keyloggers
- 14) Damage limitations cannot avoid ____.
- a) Information leakage
 - b) Resource damage
 - c) Missing of files
 - d) Hackers attack
- 15) Which of the following avoid data leakage, even if hacker gets the file required?
- a) IDPS
 - b) Encryption
 - c) Logs
 - d) Back up



Summary

- Hacking is unstoppable aspect, because it is not in the scope of organisation.
- Planning against hacking need to be a continuous process.
- Incident recovery plan helps against the incidents of hacking
- IRP has 6 phases: preparation phase, identification phase, containment phase, elimination phase, recovery phase and lessons learned phase.
- IRP not only prevents the hacking, but also provides the damage recovery system.
- Web servers can be secured by installing anti viruses, limiting access to the persons, deploying proxy servers, providing two-way authentication, implementing defence of depth.
- Email can be secured by not responding to unknown sender emails, reducing the email accounts, proper usage of anti viruses, securing passwords and providing unpredictable answers for security questions.
- System can be secured from malware by installing anti viruses, not installing any unknown softwares, installing patches regularly, using only proprietary softwares.
- As hacking attacks is unpredictable, so planning the damage limitations could be the best approach to safeguard the system.
- For limiting the damages, system must maintain log files, all the transmissions must be encrypted, use IDPS for preventions, use honeypots for preparing block lists and create regular restore points.



Terminal Questions

1. What is IRP? Explain its role for providing security for organisational assets.
2. “Security loopholes create the great damage to the individuals or organisation” - justify.
3. Suggest some measures to secure the emails from the hackers.
4. Explain the various methods used by the hacker to hack the web server.
5. Mention a few basic measures to be taken by the data and network administrators.
6. Discuss the few tricks to limit the damage performed by hackers.



Answer Keys

Self-assessment Questions	
Question No.	Answer
1	c
2	a
3	a
4	a
5	c
6	c
7	b
8	c
9	a
10	b
11	d
12	c
13	c
14	d
15	b



Activity

Activity Type: Offline

Duration: 30 Minutes

Description:

Your computer automatically installs a virus from internet in a form of an application. The application can be seen on your desktop as well as your program list. This application downloads a new application every time you are connected to internet. You are unable to uninstall it because the language of application is different from the language you are aware. What type of virus is it and suggest solution.

Case Study

Myfootware Corporation wants to enter into an online business. All their products are listed in their web sites. Every customer can see all the listings of products available, but if they want to purchase the products, then they must register themselves by using their personal information.

To provide this online service, Myfootware organisation has divided their network into 5 LANs. Out of them, 3 networks use Ethernet and 2 of them use Wi-Fi 802.11g. All the systems in the network get their IP addresses from the DHCP server. Out of 5 departments, the department which takes care of designing the footwear are not allowed to use internet, because their creativity will be duplicated if the design information leaks to the outside world.

Business started its expansion to the maximum and they were getting huge orders. Then they observed few hiccups in their networks such as too many spam emails, most of the emails are reaching very late, Most of the chatting messages were having unknown links, most of their business documents started corrupting.

Management has decided to analyse the system and secure the system, so far that they formed one IRP team for planning the prevention mechanisms for securing their data from the attackers in the future:

1. As a chairperson of the Myfootware Corporation do you think that IRP will really help your organisation for securing your data? Explain.
2. Suggest preventive measures for every department to be safe from the hackers.

Bibliography



e-References

- *Planning for Hacking*. Retrieved 5 Feb, 2017 from <http://privacypolicies.com/blog/stop-hackers/>
- *Prevention from Hacking*. Retrieved 5 Feb, 2017 from <http://searchsecurity.techtarget.com/tip/Securing-your-Web-server-to-ensure-protection-from-a-hack-attack>
- *Protect Email Account*. Retrieved 5 Feb, 2017 from <http://m.wikihow.com/Protect-Your-Email-Account-from-Hackers>

Image Credits

- Figure 4.2.1: <https://www.linkedin.com/pulse/incident-response-paul-janes-cissp-gisp>



External Resources

- Whitman, M. E., & Mattord, H. J. (2003). *Principles of information security*. Boston, MA: Thomson Course Technology.
- Stallings, W. (2000). *Network security essentials: applications and standards*. Upper Saddle River, NJ: Prentice Hall.
- Pachghare, V. K. (2009). *Cryptography and information security*. New Delhi: PHI Learning.



Video Links

Topic	Link
Preventing unauthorised email spoofing	https://www.youtube.com/watch?v=hSr7pvGLCxg
Hack techniques	https://www.youtube.com/watch?v=-ocBJKFTwSQ
Incident response	https://www.youtube.com/watch?v=FiVf-L1ywyM



Notes:



Information Security - I

MODULE - V

Risk Assessment and Cyber Laws

Risk Assessment and Cyber Laws

Module Description

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.” - Sun Tzu Wu, Chinese General

This statement is exactly valid for information security. If you know about your source of threats and your organisational security, then you need not worry about intrusions. If you know about your organisational security, but not about the intruders, then one day or the other, you may have to feel the heat of hacking. If you know neither organisational security nor about the intruders, then every day you have to face the problem with the hackers. A framework is needed to study the system continuously and recommend the changes in the security system.

Most of the users on the internet are making their transactions by trusting the internet. A strong cyber laws will only be able to withstand their confidence and continue the business operations by using the internet. Most of the laws framed are very old and need massive modifications in them.

This module focuses on calculating the risk value for any vulnerabilities of the security system, describes different frameworks for the risk assessments, provides details about the penetration testing and its importance and gives a complete knowledge about the cyber laws.

At the end of this module, students will be able calculate the risk value for the security system and imagine the amendments required for the existing cyber laws.

Chapter 5.1

Risk Assessment

Chapter 5.2

Cyber Laws

Chapter Table of Contents

Chapter 5.1

Risk Assessment

Aim.....	235
Instructional Objectives.....	235
Learning Outcomes.....	235
5.1.1 Introduction.....	236
5.1.2 Internet Security.....	236
(i) Risk Assessment Process	237
(ii) Framework.....	239
Self-assessment Questions.....	249
5.1.3 Vulnerability Assessment.....	250
(i) Protective Measures	251
(ii) Procedure	252
(iii) Benefits	253
(iv) Tools.....	253
Self-assessment Questions.....	254
5.1.4 Penetration Testing.....	255
(i) Framework	256
(ii) Services and Types	259
(iii) Importance.....	261
Self-assessment Questions.....	262
Summary	264
Terminal Questions.....	265
Answer Keys.....	266
Activity.....	266
Case Study	267
Bibliography.....	268
e-References	268
Video Links	269



Aim

To familiarise the students with the concepts of risk assessment frameworks and equip them to assess threats & vulnerability and use various types of testing



Instructional Objectives

After completing this chapter, you should be able to:

- Describe the methods of risk assessment with its architecture.
- Explain protective measures of Vulnerability assessment of the system and its benefits
- Classify the types of Penetration Testing and its importance



Learning Outcomes

At the end of this chapter, you are expected to:

- Outline risk assessment methods and its need.
- Outline the vulnerability of the system and tools used for assessment.
- Compare between Penetration Testing and Vulnerability Assessment
- Identify the services provided by penetration testing w.r.t. classification

5.1.1 Introduction

Many users of the internet think that their system is secure, if the antivirus is installed in the system. However, attackers are always hungry to corrupt the system. A small attack on a strong security system may create great damage to the system. Sometimes this damage may be in terms of financial implication. The question is how to design a security system, which is always ready to handle new intrusions and attacks? How can one keep the system always ready to handle the various attacks?

Now, for any kind of measures to be taken we need to measure the kind of risk that occurs and analyse to what level it may be a threat to the network. There are various methods to measure risk and evaluate it. Only once the risk is evaluated, it can be managed. There may be various methods of assessing the risk. Risk always depends on the various factors such as vulnerabilities and threats.

This chapter deals with what is a risk and how to assess it, how risk of the system depends on the vulnerabilities, how vulnerabilities of the system can be identified and how can deep scan of the security system be done with penetration testing.

At the end of the chapter, students will be able identify the vulnerabilities of the security system and able to calculate the risk value by using few risk assessment frameworks. They also will be able to differentiate vulnerability assessment and perform penetration testing.

5.1.2 Internet Security

Every day several organisations or individuals face some intrusions in one way or the other. This intrusion may cause a huge damage to the system. Before getting into handling the intrusion, few questions need to be answered:

- What is intrusion all about?
- Does this threat create damage?
- Does our existing security system can handle it?
- If damage is about to happen, then what could be its magnitude?

Answers to these questions will guide you on how to proceed further. In simple terms, we can identify if the intrusion is risky or not.

The above-mentioned process can be given a simple name called as Risk Assessment.

Risk assessment gives a score to the risk involved for every information asset. This number is an absolute value. Based on the value of the risk assessment, it is possible to estimate the damage possible for each individual asset.

Risk is always measured based on the money and human effort involved in defending the threat, which is responsible for the risk.

Risk of any organisation depends on the number of vulnerabilities. Vulnerability is nothing but a fault in a system or process or security mechanism.

(i) Risk Assessment Process

All the threats that an organisation encounters are not dangerous for organisational security. Now the question is how we differentiate the threats and risks. To solve this problem, a systematic quantifying process is required to analyse the risk. This systematic process can be named as risk analysis.

The overall process of risk assessment divided into five stages as shown in figure 5.1.1

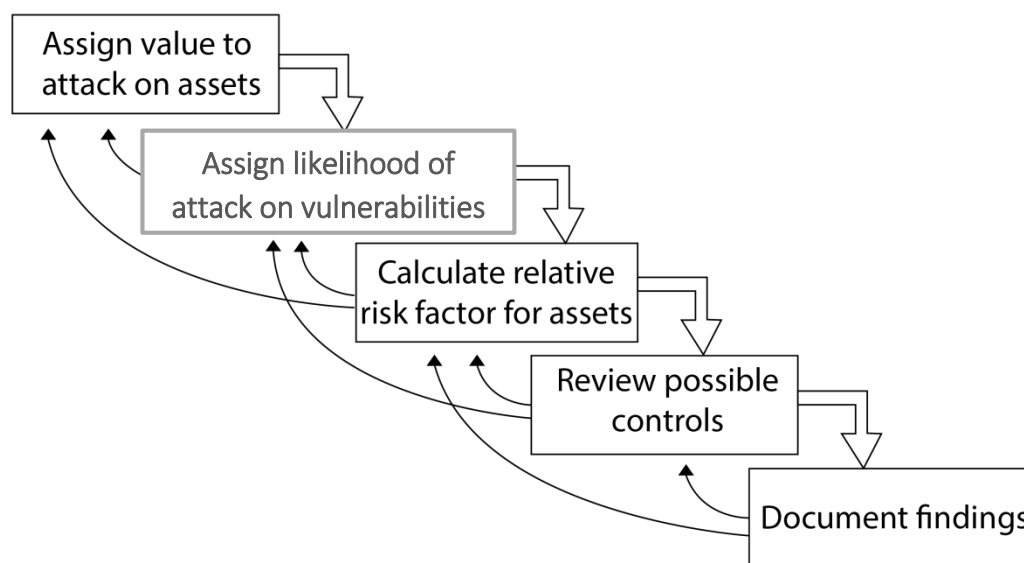


Figure 5.1.1 Different stages of Risk Assessment

- **Stage 1: Assign value to attack on assets**

Every asset must be assigned with some constant value by considering the impact of an attack. Most sensitive and crucial assets which have more risk with attacks, can be provided with a greater value. The asset which has less risk with attacks, can be provided with the least value. A list of all the assets can be prepared, along with the possible

attacks and asset values. If new assets or new attacks are identified over the process, then the list can be updated with new values. This list acts as a base for calculating the risk value.

- **Stage 2: Assess Likelihood of attack on vulnerabilities**

In this stage, a vulnerability assessment is conducted to identify the potential holes in the overall security system. This assessment can be performed by using penetration testing (we will discuss this in detail under section 5.1.4). Vulnerability within the system somehow leads to a chance of attack. Not all the vulnerabilities are critical, only few of them may lead to major attacks.

The probability of a vulnerability that leads to attack is known as likelihood of attack on vulnerabilities. Its value will be in between 0.0 to 1.0. A likelihood value 1.0 is considered as major vulnerability and 0.1 is considered as a vulnerability, which does not impact the system more.

If a new attack found the assessment process, it will move back to stage 1 and update the list of asset and attack values. It then updates the likelihood of the vulnerability.

- **Stage 3: Calculate relative risk factor for assets**

An absolute value for the risk can be calculated by using the likelihood and asset attack values. The absolute value calculated will act as guidelines for the control measure needed to handle the risk. Risk value will always be directly proportional to the financial or human effort implications. If risk values are high, a new tool or a new team is required to control the attack. This new requirement is a financial burden.

Now the question is how to calculate the risk value?

Many frameworks are available for risk assessments and each framework has different risk value calculation procedures, through which the risk value can be calculated. Risk assessment frameworks are covered in 5.1.2 b.

During the process of risk value calculation, if a value change is identified because of the new attack, then the process moves to stage 2 and stage 1 updates the list with the new values.

- **Stage 4: Review possible controls**

Based on the risk value calculated in stage 3, a control of the risk can be planned. Some of the risks can be avoided by using new software tools and some of them may need to stop the running process. Some of them may need a new team's involvement and some of the risk needs more time to handle the attack, even though the required software tools are available. An efficient Subject Matter Expert (SME) will take a decision to minimise the financial implication and promote the smooth execution of business process.

During the process of review of controls, there would be considerable changes in policies, programs and technologies, if the existing control possibilities cannot handle the situation.

Introducing new tools or software adds new asset to the list of assets, hence the process should switch back to the stage 1 to update the list. Inclusion of new tool may lead to new vulnerabilities then the process should switch to stage 2 to update the likelihood values of it. Risk is recalculated with the new updated values. If a risk value has minimised, then the same control process can be used for the attack, otherwise identify new control processes to handle the risk.

- **Stage 5: Document findings**

A proper documentation is needed for the overall process. This documentation can add new updates to handle the risk, but it is advisable to retain old process. The old process documentation will be helpful to train the stakeholders of the system. During the documentation, if you find a new process which is better than the existing process in handling the risk, calculate the risk values for the new process, else, retain the old process.

(ii) Framework

For any system, a design is required to implement the product. A framework gives you a way to assess and calculate the risk value. Many frameworks are developed to do this. Few of them are given below:

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

This is a methodology developed for threat, asset and vulnerabilities evaluation. Software Engineering Institute (SEI) at Carnegie Mellon University designed it in 1999. This method conducts different workshops with different teams of the business units of the organisation. This method is suitable for small and medium scale industries.

An organisation that has implemented the OCTAVE process can implement a strong security system. The security system that they built into a system, responds for risk possibilities.

OCTAVE divides the overall assessment process into eight steps. They are:

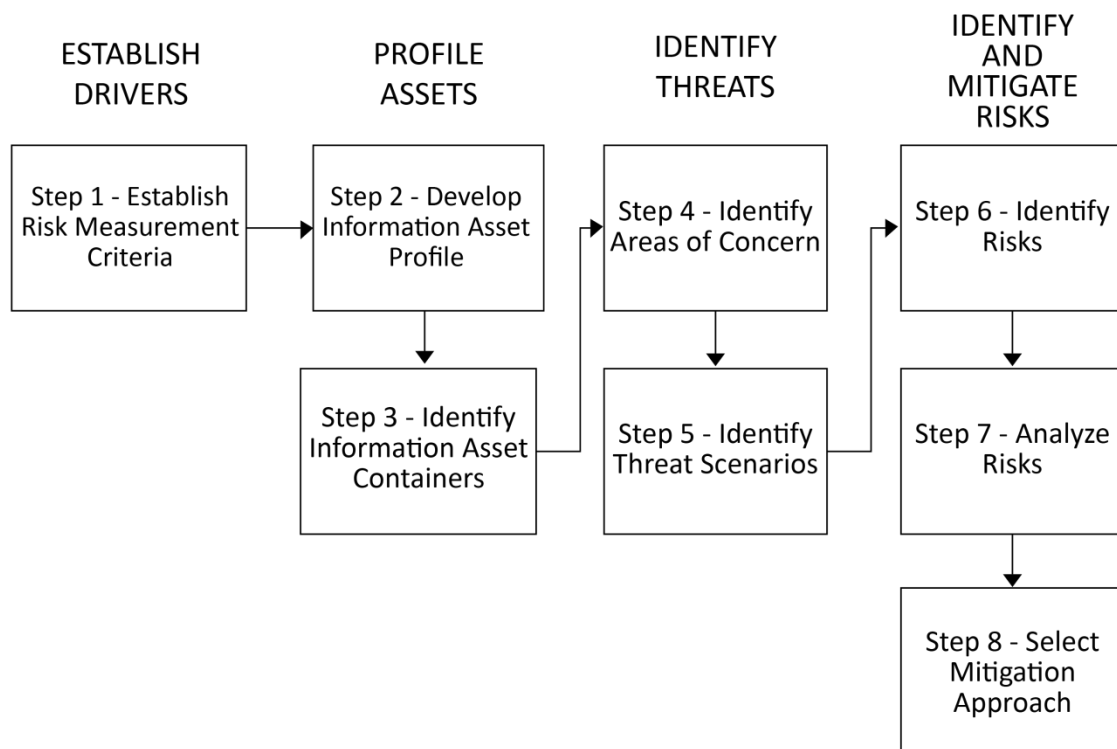


Figure 5.1.2. Different stages of OCTAVE

- **Step1: Establish the Risk Measurement Criteria**

Organisation security teams will decide the risk evaluation criteria and same is to be followed by all the teams. This stage decides and provides some values to each and every possible threat and its risk value calculation procedures. These values may be different for different organisations, because the type of risks occurs for each organisation will be different.

Prioritising the threats on the assets is done in this stage, so that it acts as a base for the risk value calculation.

- **Step 2: Develop an information asset profile**

In stage 2, an asset profile is created. An asset profile is a sheet of assets and its details. The details of the assets are unique features of the asset, its qualities, its basic characteristics and its value. The profile of the assets not only holds the information about assets, but also maintains the boundaries of the assets. Boundaries are a list of stakeholders, who can assess it or the roles of the organisation that can access it.

- **Stage 3: Identify information asset containers**

All the assets are placed inside the containers. Containers are the places, where assets placed, transported and processed. Among all the assets, some of the assets may be outsourced and they are away from the organisational limits. Stage 3 will identify the appropriate containers where assets can be placed. Few assets may require more secure and few can be in an unsecure zone. Based on the security requirements of the organisation, containers are decided.

- **Step 4: Identify the areas of concern**

Step 4 creates a list of possible threats for the organisation's assets. This list is prepared based on the brainstorming conducted with all the security experts and team heads of different teams of the organisation

- **Step 5: Identify the threat scenarios**

The previous step performs the half of the work of step 5. In this step, the scenarios are identified which opens the possibilities for threats. This series of operations is constructed in the form of a tree, known as threat tree.

Some of them are as follows:

- The Root of the tree is the threat, all the branches of it are the causes for the threat and sub branches are sub causes of the problems.
- Figure 5.1.3 is a threat tree for “virus affecting the file”, so it is the root node of the threat tree.

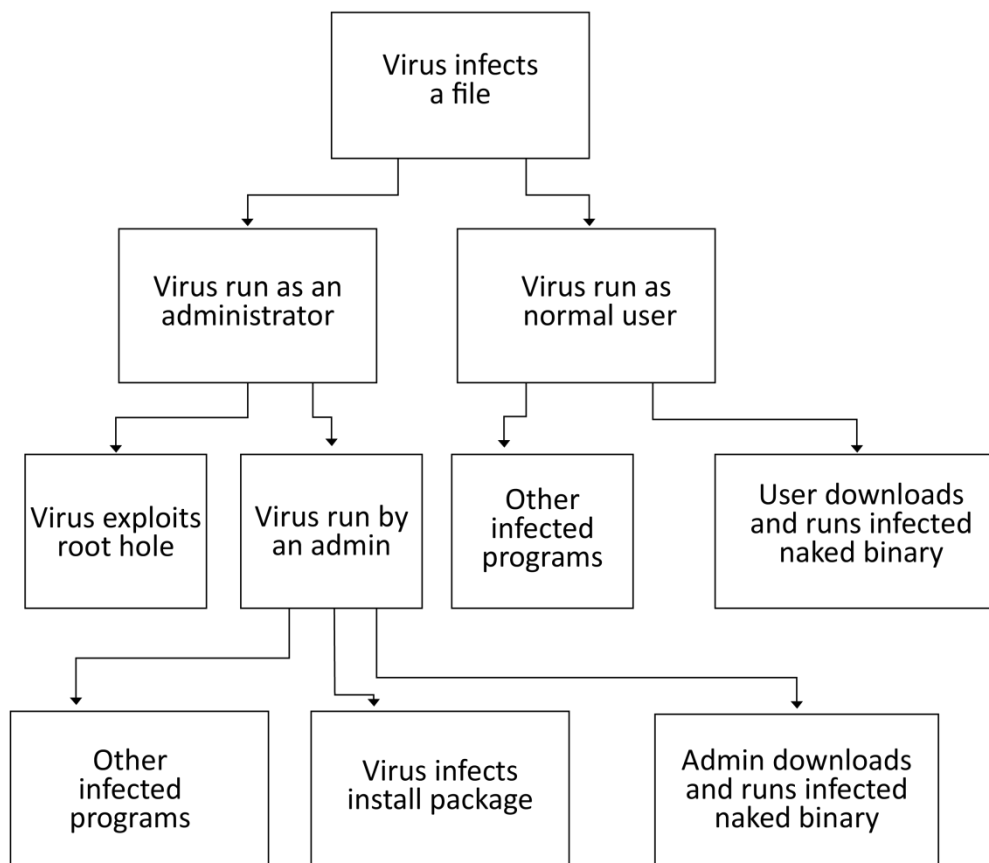


Figure 5.1.3 Example for threat tree

The possibilities for this threat may be:

- it has executed as “administrator” or
- as “a normal user”.

Hence, both the possibilities are branches of root node. Now, two reasons are identified for the virus infection.

- One among them is “virus exploited the vulnerabilities” and
- “virus executed as admin”.

Both these reasons will act as two sub branches to the node “virus run as administrator”. This process continues until it finds the root cause, as shown in the figure 5.1.3. All the leaf nodes of the threat tree are the root causes for the threat. Security teams must analyse all the leaf nodes of threat tree and find a relevant cause for the risk.

- **Step 6: Identify the Risk**

Step 5 identifies the threats and step 6 prioritises the threats based on the expenditure involved in resolving the threats. Threats that can be resolved by using existing infrastructure, which are not considered as risky. Risks are the threats which creates a financial burden for the organisation.

- **Step 7: Analyse risk**

As explained in step 1, depending on the organisational risk assessment equations, risk value is calculated. Different organisations follow different ways of calculating the risk value. Hence OCTAVE suggests, building the risk equation based on the type and scalability of organisational network.

For any organisation, few things are considered in common while calculating the risk value.

- Threats and its corresponding values assigned must be part of risk calculation
- Risk value should be proportional to budget involve to overcome the threat
- If a risk value of any threat is very high, then immediate attention is needed to resolve it.

- **Step 8: Select mitigation approach**

In this step, based on the threat, identify the mitigation process. This mitigation process will try to minimise the implications of a threat to the security system. Most of the times, the mitigation process will choose the existing infrastructure to handle the threat. If the existing infrastructure does not provide any support to handle the threat, then a new process of threat eradication need to be identified.

Expert advice at this stage is most recommended to minimise the budget requirements to mitigate the risk.

OCTAVE is very simple and straightforward approach that can be followed by any organisation with very minimum prerequisites. OCTAVE is applicable to organisations that are able to design and decide the risk assessment based on their needs. If an expert makes any mistake in designing the equations, then even a small threat will appear as a massive risk factor.

NIST SP 800-30:

National Institute of Technology and Standards special publication 800-30 provides a basic platform for the Risk Assessment and Mitigation process. This standard is considered as a Risk Assessment Framework. The overall process of risk assessment and mitigation is divided into nine steps as shown in figure 5.1.4

NIST is the risk analysis framework designed for medium to large scale industries, whereas OCTAVE framework is meant for small to medium scale industries. NIST provides a complete framework stack for analysing the risk without any pre-decided equations depending on the organisation.

- **Step 1: Study System Characteristics**

Step 1 is to study the complete process of security system. The process of system study includes mission, vision, hardware, software, system interfaces, networking components, Storage components, people, etc. It also lists the boundaries of the system and users, the boundaries of the containers, sensitivity of the data and assets, the functionality of each process, interaction each process with another process and policies of the security system.

Completion of this process gives a complete picture of the security system.

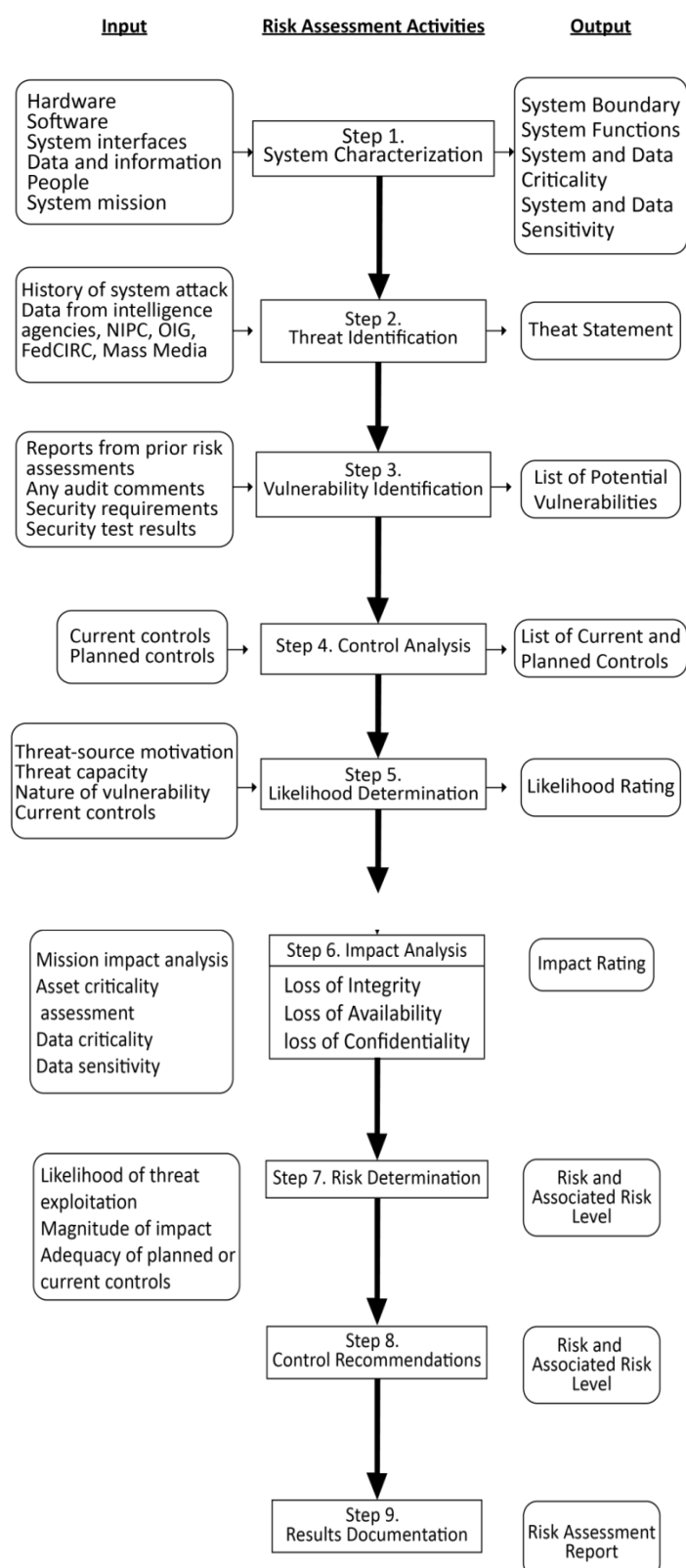


Figure 5.1.4: NIST SP 800-30

- **Step 2: Identify possible Threats**

On the basis of information provided by step 1, possible threats are listed in step 2, by conducting a simple brainstorming session with all the security professional of the organisation. Few organisations will also prefer to draw threat trees to identify threats that are more possible. The organisation will also consider the previous history of threats happened and its results and reports.

- **Step 3: Identify Vulnerabilities in the system**

By conducting vulnerability assessment, all possible vulnerabilities in the system that are identified and listed. Some organisations will go a step ahead and conduct the penetration testing also to find more vulnerability in the security system. Previous attacks history, risk reports, security audit results, new security requirement requests can also be considered for finding the vulnerabilities in the system. After a detailed study, the vulnerabilities are prioritised based on the number of possible security threats with the existence of the vulnerabilities.

- **Step 4: Study the existing Control**

A detailed study on the existing threat control policies and software's available in the organisation are identified and listed. The requirement for new software's to handle the security threats are studied in this step. The controls include policies, process and technology.

- **Step 5: Likelihood determination**

Step 5 acts as an important base for calculating the likelihood. It is the probability of a vulnerability acting as a source of intrusion. Its values are always ranging from 0.0 to 1.0. If the likelihood value is very small, then the vulnerability is not going to affect the risk, whereas if its value is very high, then it indicates that the vulnerability would have a good impact on the security risk. A list of all the vulnerabilities and its likelihood values need to maintain for risk calculation.

- **Step 6: Impact Analysis**

An impact rate of vulnerability is studied. The impact can be of financial or human effort to recover the system to its safe state. If any threat raised because of any vulnerability and disturbs the CIA triangle, then it is considered as most impactful. Any threat, which is trying to access sensitive data or asset, then it is also considered as most

impactful. With the existence of current controls, if any vulnerability is not disturbing the security of the system, then it is considered as less impactful.

For vulnerability, an impact rating is generated and is maintained as records. On every vulnerability assessment, the impact list also alters. The impact is rated between 0 and 9, where 0 is low impact and 9 is high impact.

- **Step 7: Risk determination**

Step 7 calculates risk value for each and every vulnerability based on the formula:

$$\text{Risk} = \text{Threats} * \text{Likelihood} * \text{Impact}$$

Risk value will be directly proportional to the financial implication for the organisation because of the vulnerability. Vulnerabilities with more risk value has more risk and less risk value has less risk.

For example, if the number of possible threats are 1000, likelihood is 0.9, but impact is 2, then the risk values is

$$\text{Risk} = 1000 * 0.9 * 2 = 1800$$

For example, if the number of possible threats are 1000, likelihood is 0.1, but impact is 2, then the risk values is

$$\text{Risk} = 1000 * 0.1 * 2 = 200$$

For example, if the number of possible threats are 1000, likelihood is 0.1, but impact is 9, then the risk values is

$$\text{Risk} = 1000 * 0.1 * 9 = 900$$

This proves that if any vulnerability has less likelihood, it is less risky for the security system. Hence, vulnerabilities with more likelihood value need to be focused more.

Risk value acts as guidelines for the security experts to prioritise their focus on the vulnerabilities to be handled. It helps in deciding the control measure for the vulnerabilities.

- **Step 8: Control Recommendation**

Select the control measures based on the risk value and its financial impact. Risk value, impact and likelihood values act as a base for deciding the recommended controls. If the recommended controls are available, in the existing controls then there is no need of a new policy or process or technology, if it is not available, then there will be a need for a new system. If a risk value of any vulnerability is minimised, then its implementation will be postponed to the next cycle.

- **Step 9: Result Documentation**

Any risk that is handled, should be documented. Even the results of the vulnerabilities should to be documented for reuse. Documentation should also include the details of new assets, new technologies and new processes. This document acts as a reference for the future use.

Both the risk assessment frameworks discussed above are useful for risk assessment. They differ in few factors such as:

Methodology used:

- OCTAVE Method is self-directed. The resources available within the organisation are used to handle the risk. The evaluation process of risk is done through consolidation and analysis workshops.
- NIST is a management system, which allows the experts and third party execution in risk mitigation.

Information Gathering:

- OCTAVE collects the information and comes to a decision using workshop-based approach.
- NIST uses interviews, questionnaires and document review techniques for information gathering.

Assessment Team:

- The OCTAVE assessment team comprises representatives from both the IT department of the organisation and business team.
- NIST does not create any assessment team, but mentions roles for all the stakeholders involved in the methodology.

Risk assessment is a continuous process. It needs to be conducted or repeated for every intrusion, after adding or replacing with new asset to the system.

**Self-assessment Questions**

- 1) A probability of vulnerability leading to security attack is known as _____.
 - a) Impact
 - b) Likelihood
 - c) Threat
 - d) Control system
- 2) What is vulnerability?
 - a) Damaged security system
 - b) New Control system introduce within the system
 - c) A potential hole in the security system
 - d) External stakeholder of the system
- 3) Which of the following factors does not have a negative impact on the Risk?
 - a) Vulnerabilities
 - b) Threats
 - c) Intrusions
 - d) Control Systems
- 4) OCTAVE uses which of the following tool to identify threat scenarios?
 - a) Anti-viruses
 - b) Vulnerability assessment tools
 - c) Penetration testing tools
 - d) Threat trees
- 5) NIST SP 800-30 considers the impact factor range as _____.
 - a) 0-9
 - b) 10-100
 - c) 0-1
 - d) 1-100

- 6) According to NIST SP 800-30, if number of threats possible for a vulnerability is 500 and its likelihood values is 0.4 and impact is 6, then the risk values is ____.
- | | |
|---------|---------|
| a) 1200 | b) 1245 |
| c) 1210 | d) 1225 |
- 7) OCTAVE divides the overall risk assessment into how many stages?
- | | |
|------|------|
| a) 8 | b) 9 |
| c) 4 | d) 5 |

5.1.3 Vulnerability Assessment

Vulnerability assessment or analysis is used to identify and classify the loopholes in the security system. It scans the computers, communication channels and network devices functioning to find vulnerabilities. Vulnerability assessment also estimates the effectiveness of recommended countermeasures and policy changes, once the organisation started using it. It provides the detailed report to the management on identified vulnerabilities and their suggested countermeasures.

Vulnerability assessment many times uses penetration testing to identify the vulnerabilities in the system. On the identified vulnerabilities, a risk assessment is conducted to calculate the risk factor involved with the vulnerabilities.

Vulnerability analysis consists of several steps. They are as follows:

- Identifying and classifying all the resources of the organisation. Classification is done based on system resources and network resources.
- Prioritise the resources of the organisation based on the resource involvement in the productivity of the organisation.
- For each resource, identify the potential threats and list them.
- Identify the countermeasures by developing a strategy to deal with serious potential problems first.
- Identify and implement the procedures to prevent the attacks.

To minimise the effect of the vulnerabilities, the following preventive or protective measures can be followed.

(i) Protective Measures

There are various reasons for the system to get affected by the vulnerabilities. Everyone has to use proper protective measures to safeguard themselves by the hackers.

Measures are:

- **Software update:**
Software updates are the most important security measures for protecting the organisation's security. Hence update the software's time to time to avoid the hacking. Most of the cases, unpatched software's are the sources of vulnerability.
- **System isolation:**
If any system is in vulnerability condition, then try to detach it from the network of the systems, since the victim system becomes the source to hack and gain the other system controls.
- **Replacement of the system:**
Try to repair the system, which is already in a vulnerable condition. If a repair is not possible, then replace the system with a new system to get rid of the problems.
- **Monitoring:**
Continuously monitoring a security system is one of the best strategies to be secure from the vulnerabilities. Build a strong security system to monitor the entire system using firewalls, intrusion detection and prevention system. This security system alerts the users before the attacks. Even after implementing this monitoring system, there is always a chance that the attackers identify vulnerability, so perform the security audits to check the functioning of this system.

Along with the above, there are additional measures to keep the system in safer state they are:

- Training and awareness programs for employees
- Creation of access control limits for users
- Do's and don't's and with security policy need to be educated to all the users of the organisation
- Revising the existing policies and procedures based on the needs

(ii) Procedure

Vulnerability analysis provides the information about the organisation security status. This vulnerability assessment consists of following three phases as shown in figure 5.1.5:

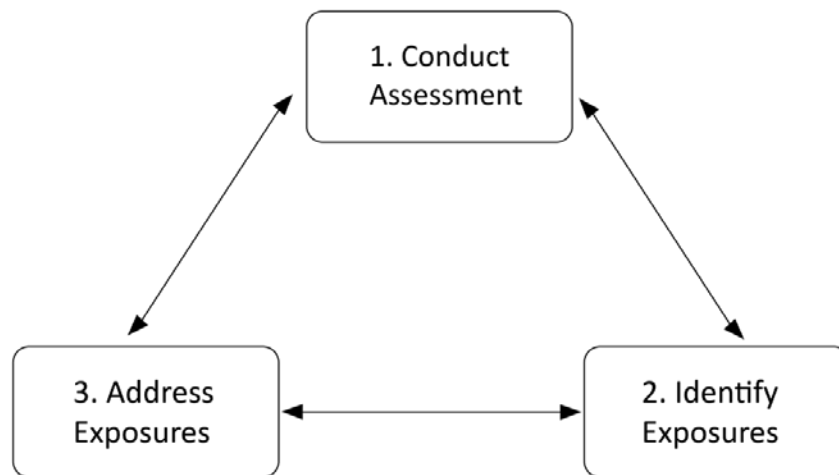


Figure 5.1.5: Phases in vulnerability assessment

1. **Conduct Assessment:** In the initial step of Vulnerability Assessment (VA), complete system details are collected from the important security stakeholders of the system such as a system administrator, network administrator, team leads of different processes. The information collection focuses on the network architecture, software and hardware details, servers deployments, the interface between servers and end users, authentication and authorisation details of users, policies and procedures, etc. These details are studied to identify the vulnerabilities in the overall system.
2. **Identify Exposures:** After collecting the required details from all the possible sources, a detailed study is conducted to identify the potential holes in the system. For simplification of the complex system, all the available resources can be classified into different categories. Assign each system to a different team for assessment. This process identifies the potential vulnerabilities and prioritises them based on the impact of the vulnerabilities in the security system. Some of the vulnerabilities identified may need less focus, as their impact on sensitive resources may be very less. Few scanning tools can also be employed for finding the vulnerabilities.
3. **Address Exposures:** After identifying and prioritising the vulnerabilities, the vulnerabilities which have a great impact need to be handled first. If any of the

unwanted services are creating the holes could be stopped by a careful inspection of its implications. If any of the vulnerabilities are not creating a major risk to the system and its solution is expensive, it can be postponed to the next cycle of inspection by documenting it properly. If any of the vulnerabilities cannot be solved easily, then the same needs to be documented and reported to the higher management for their approvals.

Out of all the vulnerabilities identified, if any of them can be solved by upgrading the system, then it would be a wise decision to go with the up gradation.

(iii) Benefits

Vulnerability assessment will have following benefits:

- Keeps the system up-to-date with all security patches
- Most of the complicated business impact can be minimised
- Alerts the threats possible with the resources
- Safeguards sensitive resources from the attackers
- Suggests proactive precautions to the future threats
- Design control measures for the existing problems

(iv) Tools

There are many tools available to check the vulnerabilities in the system known as “vulnerable scanners”. This scanner is software, assess the vulnerabilities in the system by scanning various components like computers, network configurations existing procedures through scanning. The intruders find out the breaches in the system by scanning the system using the same scanning tools, so it is always better to perform the scanning before intruders. There are various tools or scanners are available. These are:

Network based scanners

This scanner is used to find out the vulnerabilities related to the networks. Basically, this software is installed in the main system within the network. It scans the entire network. This scanner helps to find out the security breaches in the software's, networks or webserver. The network scanner is again classified into various types of scanners. They are:

- **Webserver scanners:** Identifies the vulnerabilities related to the web servers.

- **Port scanners:** It is used to identify the open ports available on the remote system and also the vulnerabilities associated with these ports.
- **Web application scanners:** This scanner helps to find the faults in the web applications that are running on servers. This alone cannot provide the complete security. Human intervention is also needed to identify certain vulnerabilities.

Examples of network scanners: Nmap, Nessus, Nexpose, Saint, SoftPerfect, MyLanViewer, etc.

Host based scanners:

Host based scanner software installed in the host computer. It is used to find the vulnerabilities in the various files on the computer because it is having the permission to check all verities of files like user login files, password file, configuration files and operating system services files to list a few. If the hacker uses this host based scanner, then they can collect the sensitive information easily. This scanner also provides the security gaps in the system.

Example: Lynis, ISS system scanner, Bind View, Microsoft Baseline Security Analyser, Shadow Database Scanner etc.

In the above mentioned software's few software's are open source and few are paid software's. When installing and purchasing these software's, see the requirement and install proper software's to find out the vulnerabilities in the system.



Self-assessment Questions

- 8) Which of the following tool is used to identify the security breach within a network?
 - a) Sniffing
 - b) Exploit of Security
 - c) Vulnerability Scanner
 - d) Hacktivist
- 9) Which of the following is division of host based scanner?
 - a) Port scanner
 - b) Web server scanner
 - c) Web application scanner
 - d) Database scanner
- 10) Which of the following is an example for network scanner?
 - a) Nmap
 - b) Lynis
 - c) Bindview
 - d) Shadow database scanner

5.1.4 Penetration Testing

Penetration testing or pen testing is the security testing to test security risk of the system or organisation. The tester checks every corner of the system to identify the security problem. The penetration tester collects the usernames and passwords to perform the test. With these credentials, they will check for the vulnerabilities starting from the individual systems of the employees to complete organisation.

The process penetration testing calculates the ability of the system to protect the various resources of the organisation like network connections, various important documents, database and other hardware devices either from external or internal users. The penetration testing should be done periodically to check the security level of the system and its flaws. The intruders always use the various means to collect or to perform the damage for assets, if this test is not performed at regular intervals, then definitely there will a great damage to the information.

Is the pen test and system vulnerability assessment are same? Many people get confused with this Question and answer it as “yes”, but it is “no”. They will think that both are using to identify the security gaps. The difference is in the vulnerability assessment. The testers identify the problematic areas for vulnerabilities, whereas in the penetration testing they will collect the credentials of the user to test for vulnerabilities. Major differences between the vulnerable assessments to penetration testing are:

Vulnerability assessments:

- Creates the directory for resources in the system
- List the vulnerabilities for each resource
- Prioritise the resources based on the potential security gaps
- Attempts to mitigate the problems
- It will not be used for real time applications
- Deals with lab components

Penetration testing:

- It is goal oriented
- Identifies the level of vulnerability
- Tester penetrates into the system to find the vulnerabilities with the permission of the management

- Easy to identify the internal intruders
- Gathers the sensitive information from the targeted system to find all the problems
- Produce the detailed report to management about the vulnerabilities and its countermeasures
- Uses for real time applications

Examples of penetration testing tools are: Nmap, Httprint, Super Scan, Nessus, Brutus, Shadow Security Scanner, etc.

In the penetration testing, the tester will submit the detailed report about the testing process to the management.

(i) Framework

Penetration testing integrates various procedures and software's to identify the vulnerabilities in the system. The penetration testing is the step by step process from planning for the test to removing the vulnerabilities.

The steps involved in penetration testing are shown in figure 5.1.6.

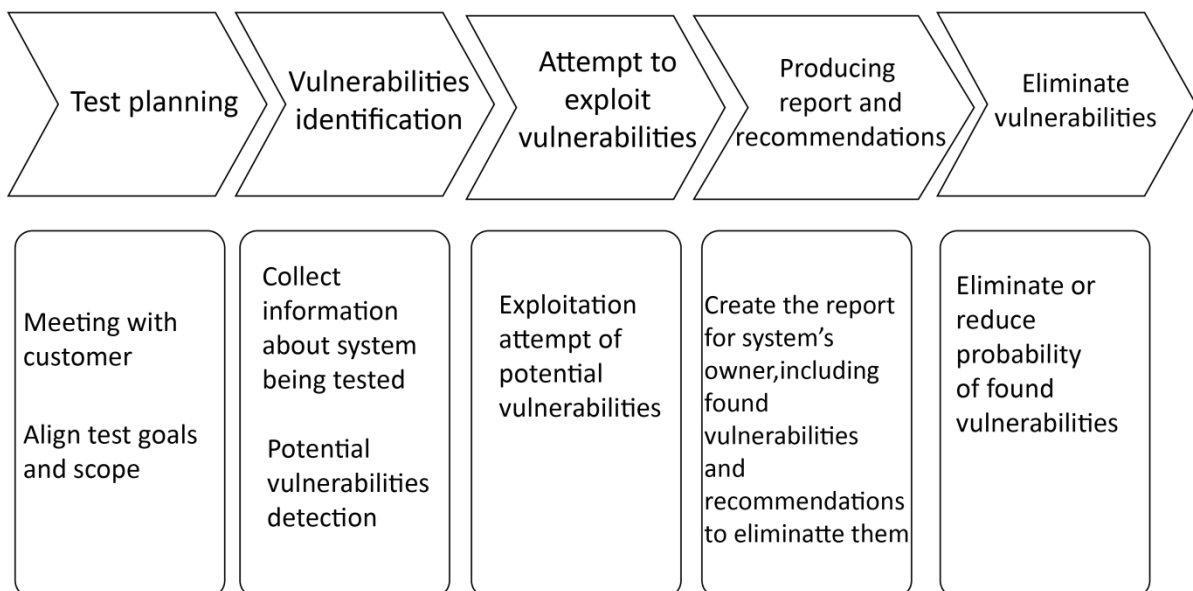


Figure 5.1.6: penetration-testing process

Test planning:

This is the first stage in the process. The tester meets the client and prepares the objectives and aim of the testing.

The main objectives of penetration testing are:

- To identify the various security vulnerabilities
- To calculate the security risk based on the vulnerabilities
- Methods to remove vulnerabilities
- Suggestions to improve the quality of security system to find problems in the system

Vulnerabilities identification:

In this step, the tester collects the complete details about the organisation from the client like network architecture, roles of employees, security system, security policies and any information which is needed to perform the testing. Based on this, they will search the entire system for vulnerabilities.

Many organisations fail to provide the complete details due to lack of knowledge of the system concepts, improper maintenance of information assets, no proper communication between the people to share the details from one department to another. The tester starts their work with the information available to find the flaws. They will scan the complete resources using the automated tools available. During this process, they will verify that how many servers, what kind of the data it consisting of, open ports for devices, etc..

At the end of this step, they will find the vulnerabilities in the entire system by using all types of credentials. They will find all the loopholes in the system, that major problematic location for decoys to enter the system. Once this step is completed, then they will move to the next step for further actions.

Attempt to exploit vulnerabilities:

This is a very crucial step because changes in the security system should retain the organisation policy structure like integrity, consistence of data etc. In this step, they will analyse the identified vulnerabilities, because not all the identified vulnerabilities are potential. After analysis, they will calculate the security risk factor. If the risk factor is very high, then such vulnerabilities need to be addressed immediately so that the threats from such vulnerabilities can be minimised.

Producing report and recommendations:

Once identification of vulnerabilities is found, then submit the final report to the high-level people about the penetration testing. A few points in the report are:

- What all places have been tested?
- What kind of the security breach has been found?
- Whether the security threat is from internal or external user?
- Is any kind of modification required for organisational security set up?
- Are any security components outdated?
- The party, which provided security system, is authenticated or not?
- What kind of training needed for employees to safeguard the system?
- What is the security risk factor in the system?
- What is the overall time they took for identified the faults?

Apart from all the above, they even provide the suggestions to improve the security system and to meet the goals of the organisation.

Eliminate vulnerabilities:

This is the final step in the penetration process. The tester eliminates the identified vulnerabilities.

To better understand the process, let us take a simple *example*.

Aim of the penetration test: to identify chances for hacking the website.

Test planning:

The tester will meet the customer and discuss the goal and scope the test and prepares a testing goal statement and gets approval from the client to go ahead.

Vulnerability identification:

The tester will try to penetrate into the system as a

- Unauthorised user
- User with limited permissions
- Authorised user by violating the access rules

Identifies all the vulnerabilities in the website.

- **Attempt to exploit vulnerabilities:**

Through the identified vulnerabilities, the tester will try to create the damage or introduce a threat into the website. The tester records the level of risk involved with the vulnerability through which the tester penetrates into the system.

- **Producing report and recommendations:**

Based on the identified vulnerabilities and chance of intrusion into the website are clearly reported as a document. The report also comprises of recommended counter measures for the identified vulnerabilities.

- **Eliminate the vulnerabilities:**

Tester and a team of security experts will decide the changes to be carried out to make the website free from vulnerability attack and same is implemented into the website. The complete process of penetration testing is conducted again after incorporating the recommendations of the testing team.

(ii) Services and Types

There are many automated tools available for penetration testing. Penetration testing is not only useful for finding the information security vulnerabilities, but also provides various services like:

Social Engineering Penetration Testing:

Social engineering is one of the persuasion techniques to do frauds by acquiring the assess detail of someone. This social engineering penetration testing is used to identify and remove the vulnerabilities of user accounts.

Example: To calculate the strength of passwords of all the users of the system.

Web Application Penetration Testing:

Web the word making every human to think more. To make their place simple, many organisations are using websites. If an attacker hack the data by penetrating into the organisation website, then this testing will identify and remove the vulnerabilities.

Example: To change the object available in a website without authentication.

Wireless Technology Assessment:

This testing is used to secure wireless connections like Wi-Fi, Bluetooth during transit and communications process between the components.

Example: Taking the control of wireless DHCP server to get the IP address.

Embedded Device and IOT Testing:

This test assesses the problems in the product, chip and code. It tests the functionality and working of the device. If any flaws are found in the functionality, then it verifies the penetrating area in the system, then it finds the vulnerabilities and finally it deletes it.

Example: Open digital secure locker with minimum attempts.

Mobile Application Assessment:

Now a days most of us are using either android based or ios based operating system mobiles. This testing finds the vulnerabilities in the installed applications and also application developer authentication details, data validation, session management etc.

There are still various penetration testing services are available. For every variety of service, automated tools are available from different vendors. So based on the need, the user has to select the correct service. Penetration testing should be done periodically to be in the safe side from vulnerabilities.

Example: Get the contact list of any mobile without user intervention when it is connected to the internet.

Types of Penetration Testing:

The organisation may perform the penetration testing when they have implemented security system newly; security set up is moving from one place to another, variation in the system functionally, any adding or deleting the component from security perimeter. Based on the functionality and details provided by the client, there are three types of penetration testing's. They are:

- **Black Box Testing:** Black box testing will perform by the tester if the client provides no information before testing.

For example, a security system which is built on cloud based environment is best suitable for this type of testing.

- **White Box Testing:** If the tester collects the complete information about the target before penetration testing, then it is known as white box testing.

A security system which is built with very clear requirements is the best environment for black box penetration testing.

- **Grey Box Testing:** The client provides the minimum details about the organisation and its functionalities before the testing.

A security system which is built with very minimum requirement and strengthens over the time is best suitable for this kind of testing.

(iii) Importance

Pen test is used to identify the vulnerabilities in the system. Therefore, management has to plan to conduct this test in the continuous process.

Importance of penetration testing:

- It helps the management to enhance their security system by providing the information about strong and weak security areas. By using this information, management even provides the security in weak places with that they can provide stronger security system to stop the vulnerabilities.
- It helps the management to identify the internal intruders and what kind of the activities that they had performed. For this they will collect employee's credentials from management to perform the security test to identify the internal decoys. To identify the internal intruders they will perform the penetration testing secretly without providing any information to employees about the test. In this case, no prior/ no information to the employees, so there is no chance for the intruders to escape.
- It helps the management to get security system details on how effectively it is working and safeguarding the organisational resources. With this, the management can get assurance about their system and perform different activities without thinking of the vulnerable.

- It helps to identify the applications, which leads to penetrate the system. Even a small loophole during the application development will give a great chance to the vulnerable. Along with this, it will find out the any bugs in the applications and existing software's.
- Penetration testing helps anyone to safeguard their customer's personal information. A small breach in customer data protection will damage the reputation of the organisation also there will be a great damage to financial status.
- It thinks out of the box to give the complete protection to your system from penetrators. The final report of the test will provide the complete status of the security system with this anyone can enhance his or her security concepts.
- It helps in judging, what kind of the training and awareness programs are needed for everyone to safeguard the system from internals as well as from externals.

Penetration testing is important to find the security breaches in the system. Many organisations and persons once they were implemented security mechanisms they will think that it will take from vulnerable. Many persons got shocked after seeing the results of the penetration system for their security systems. The results were unexpected.



Self-assessment Questions

- 11) With the minimum details of the system the penetration testing is done. This test is known as ____.
- | | |
|--------------|-------------|
| a) Black Box | b) Grey Box |
| c) White Box | d) Blue Box |
- 12) When the person analyse the system for vulnerabilities with the credentials, then this type of the assessment is known as ____.
- | | |
|-----------------------------|------------------------|
| a) Vulnerability assessment | b) Penetration Testing |
| c) Cross Script | d) Security check |
- 13) If the organisation provides the complete details about the system, then the type of the testing can be considered as ____.
- | | |
|--------------|--------------|
| a) White Box | b) Grey Box |
| c) Blue Box | d) Black Box |

- 14) When can a tester perform penetration testing?
- a) When weak password on the system
 - b) To guess passwords to perform the vulnerability
 - c) Permission from the owner to identify the vulnerability
 - d) To gain access of the network
- 15) If the organisation does not provide details about the system, then the type of the testing can be considered as ____.
- a) White Box
 - b) Grey Box
 - c) Blue Box
 - d) Black Box



Summary

- Risk assessment helps organisation to estimate the financial implication of the vulnerabilities of the security system
- The risk assessment process is divided into 5 stages: assigning values to attack on assets, Assess likelihood of attack on vulnerabilities, Calculate the relative risk factor, Review possible controls, Document findings.
- Risk value can be calculated by using Risk assessment frameworks such as OCTAVE and NIST SP 800-30.
- OCTAVE divides the overall Risk assessment process into eight steps: Establish Risk Measurement Criteria, Develop Information Asset Profile, Identify Information Asset Containers, Identify Areas of Concern, Identify Threat Scenarios, Identify Risks, Analyse Risks, Select Mitigation Approach
- Calculated risk values based on the existing infrastructure and their vulnerabilities suggest the risk mitigation procedures.
- Vulnerability assessment is the process to identify the vulnerabilities related to various resources of the organisation.
- There are 3 stages to identify the vulnerabilities in the system: Conduct Assessment, Identify the exposures, Address the exposures.
- To identify the vulnerabilities various tools are used such as port scanners, web application scanners, database scanners and web server.
- Penetration testing is used to identify the vulnerabilities in each and every system by knowing the credentials of users.



Terminal Questions

1. Risk value is directly proportional to financial implication of the organisation". Comment on the statement.
2. What are the different risk assessment frameworks available? Which among that you will prefer and why?
3. Explain NIST 800-30 risk assessment framework with neat diagram.
4. Explain how vulnerability assessment helps the organisation to improve the security system
5. What is the difference between penetration testing and vulnerability assessment? Explain how penetration testing is used to identify the vulnerabilities of the system?
6. What are the different types of penetration testing's? Explain them in detail.



Answer Keys

Self-assessment Questions	
Question No.	Answer
1	b
2	c
3	d
4	d
5	a
6	a
7	a
8	c
9	d
10	a
11	b
12	b
13	a
14	c
15	d



Activity

Activity Type: Offline

Duration: 30 minutes

Description:

Create a mind map for the RISK ASSESSMENT chapter.

Case Study

Myfootware Corporation wants to enter into an online business. All the products they have listed in their web sites. Every customer can see all the listings of products available, but if they want to purchase the products, then they must register themselves by using their personal information.

To provide this online service Myfootware organisation has been divided their network into 5 LANs. Out of them, the 3 networks use Ethernet and 2 of them use Wi-Fi 802.11g. All the systems in the network get their IP addresses from the DHCP server. Out of the five departments, the department which takes care of designing the footwear are not allowed to use the internet because their creativity will be duplicated if the design information leaks to the outside world.

All the transactions are happening through single server and data backup and recovery point creation are done on every Friday. Only system administrator has to do this backup activity. No other employee of the organisation knows how to do it. Backup disks are stored in a room with very limited security. The Administrator was very lazy to have a complex password to the server.

Management has decided to increase their business by 10 times. Management is not confident about the existing system. They called for a meeting with all the team heads, IT departments and security audit experts, expressed their concern and asked them to submit the report within 15 days.

Discussion Questions:

1. Do you think MyFootware Corporation should go for risk assessment? If so, then which framework is suitable for their risk assessment? [Hint: MyFootware is a large scale industry]
2. Do you find any vulnerability from the above information? If so, what could be its impacts? Can you prioritise the vulnerabilities? [Hint: backup is taken only on Friday]
3. Why management has no confidence on the existing system? Can penetration testing help them to realise their mistakes? [Hint: no backup server]

Bibliography



e-References

- *Risk Assessment*. Retrieved 02Feb, 2017 from <http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/risk-assessment/risk-assessment-guideline.html>
- *Vulnerability Assessment*. Retrieved 02 Feb, 2017 from <http://searchmidmarketsecurity.techtarget.com/definition/vulnerability-analysis>
- *Penetration Testing*. Retrieved 02 Feb, 2017 from <http://searchsoftwarequality.techtarget.com/definition/penetration-testing>

Image Credits

- Figure 5.1.1: Whitman, M. E., & Mattord, H. J. (2003). *Principles of information security*. Boston, MA: Thomson Course Technology
- Figure 5.1.2: http://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf
- Figure 5.1.3: https://en.wikipedia.org/wiki/Attack_tree
- Figure 5.1.4: https://en.wikipedia.org/wiki/IT_risk_management
- Figure 5.1.5: <http://www.b-infosec.com/wp-content/uploads/2016/01/vuln.jpg>
- Figure 5.1.5: http://auditagency.com.ua/images/pentest1_en.jpg



External Resources

- Whitman, M. E., & Mattord, H. J. (2016). *Principles of information security*. Australia: Delmar.
- Stallings, W. (2011). *Network security essentials: applications and standards*. Boston, MA: Pearson.
- Forouzan, B. A. (2008). *Cryptography and network security*. Boston, Mass.: McGraw-Hill.



Video Links

Topic	Link
Risk Assessment	https://www.youtube.com/watch?v=EWdfovZlg2g
Assessing Vulnerability	https://www.youtube.com/watch?v=UbH-o4pAaW0
Penetration Testing	https://www.youtube.com/watch?v=2gwVFdqwJfI



Notes:



Chapter Table of Contents

Chapter 5.2

Cyber Laws

Aim.....	271
Instructional Objectives.....	271
Learning Outcomes.....	271
5.2.1 Introduction.....	272
5.2.2 Cyber Laws in India	272
(i) Information Technology Act (ITA)	272
(ii) IT Amendment Act (ITAA).....	276
(iii) Scope and Applicability of ITA and ITAA	279
Self-assessment Questions.....	280
5.2.3 Cyber Laws - a Global Perspective.....	281
(i) Contractual Issues in Cyberspace.....	281
(ii) Non-Contractual Issues in Cyberspace	282
(iii) Challenges in the Enforcement of Cyber Laws and Recommended Strategy for Effective Environment.....	284
Self-assessment Questions.....	286
5.2.4 Fair Model.....	287
(i) Purpose of Risk Modelling.....	289
(ii) Benefits of Fair.....	289
(iii) Fair Model Components	290
Summary	296
Terminal Questions.....	297
Answer Keys.....	298
Activity.....	298
Bibliography.....	299
e-References	299
External Resources	299
Video Links	299



Aim

To familiarise the students with various acts available and use them to secure individuals/organisation's information within the boundary of Cyber Law



Instructional Objectives

After completing this chapter, you should be able to:

- Describe various Cyber Laws prevailing in India
- Explain some common global Cyber Laws and issues related to it
- Classify the components of FAIR model with its purpose and benefits



Learning Outcomes

At the end of this chapter, you are expected to:

- Identify the common cybercrimes and law applicable relating to situation.
- List the global Cyber laws and enforcement of its strategies
- Outline the purpose and benefits of using the FAIR model in Cyber Law

5.2.1 Introduction

In the modern era, the rate of cyber crimes is increasing day by day, which makes cyber laws a necessity. The crimes which involve the usage of computers and the internet are generally classified as cyber crimes. Cyber crimes can be done in two ways. One way is by considering computer as the target of the crime and the second way is by considering the computer as weapon used for attack. Attacks like hacking and Denial of Service attack where the information or resources are targeted falls under the category of computer as the target of the crime. Unlike this, the computer also uses a weapon for the attack such as IPR violations and Credit card details hacking. These kinds of attacks create a lot of serious problems with the loss leading to intellectual and monetary loss. Therefore, some measures are to be taken to prevent this which should be globally accepted by everyone. Finally, people came to know that the most acceptable measure can put in place in a compulsory way is through court. Cyber laws are the best methods to avoid any unethical scene happening on the internet. This unethical intrusion of non-permissible user accessing information which may cause a huge loss to the owner of the information is referred to as Cyber crimes.

The cyber laws were introduced to reduce the cyber crimes occurring on the network hub. Cyber laws are laws which integrate the issues related to the internet and its usage as a single unit. It is important to know various cyber laws available to handle a particular violation on the internet.

5.2.2 Cyber Laws in India

Cyber law in India was introduced to set legal standards and infrastructure for e-commerce. The cyber law promotes the usage of digital signature and support e-governance and e-commerce. For each domain, there is a specific act that has been created just like in case of normal judiciary for each crime. Some of them we will discuss here as a part of the chapter.

There are two major acts that go into the domain of Information technology. They are information Technology Act (ITA) and IT Amendment Act (ITAA). These laws are discussed in the following section.

(i) Information Technology Act (ITA)

The Information Technology Act contains 13 chapters, 94 sections and 4 schedules which apply to the Indian subcontinent and persons committing crime involving a network or computer in the Indian subcontinent. The ITA act provides a framework for cyber law by recognising digital

signatures and electronic records. Under this Act, the penalties for each cyber crime are also stated in detail. The ITA was passed by the Indian Parliament on 17th October, 2000.

This Act was introduced to prevent cybercrime, facilitating and regulating e-commerce and promoting IT industry. Another objective of this act is to implement security practices in the IT industry in India to meet the international security standards.

The list of offenses and penalties discussed in the ITA is listed in the Table 5.2.1.

Table 5.2.1 list of offenses and penalties of the Information Technology Act 2000

Section	Offense	Description	Penalty	Implementation Example
65	Tampering with documents related to computer source	When a person alters/conceals or destroys information in the source code of a computer program or computer network.	Imprisonment up to 3 years and/or fine of ₹200000	The employees of Tata Indicom were arrested for manipulating the 32-bit code, programmed for the cell phones.
66	Hacking the computer system	When a person gains illegal access to a system with the motive of damaging/destroying/deleting the computer resources.	Imprisonment up to 3 years and/or fine of ₹500000	CBI, charged Kumar guilty for modifying the passwords and contents in the Joint Academic Network, maliciously.
66B	Receiving or retaining stolen computer or communication device	When a person retains a stolen device or has a motive to steal a computer or communication device.	Imprisonment up to 3 years and/or fine of ₹100000	The person retaining any stolen computer devices can be tracked and charged guilty using its IP address.

66C	Making use of another person's password	When another person's unique identification data such as password/digital signature is used.	Imprisonment up to 3 years and/or fine of ₹100000	The identity of the Lifelock's CEO was used to obtain a cash loan of \$500, which he had revealed on a TV show, weeks earlier to the incident.
66D	Cheating, using computer resources	When a person cheats someone else using the computer or its related resources.	Imprisonment up to 3 years and/or fine of ₹100000	A person named Sandeep Varghese set up a site- www.jayplychem.org to send fake emails to customers and eventually cheat them to defame the company. The responsible people were charged guilty by the State of Kerala.
66E	Publishing private image of others	When a person captures/publishes /transmits images of another individual's without his/her consent.	Imprisonment up to 3 years and/or fine of ₹200000	In 2012, the son of a Congress leader was arrested for circulating personal clips of a 16-year old girl.
66F	Acts of cyber terrorism	When a person is involved in cyber acts threatening the unity or sovereignty of India.	Lifetime Imprisonment	The cyber crime investigation cell had traced the IP address of the sender of e-mail, threatening the Bombay Stock Exchange. The IP address was tracked in Patna, Bihar.

67	Publishing obscene information in electronic form	When a person publishes obscene information on the web, causing disturbance to others by making it seen or heard.	Imprisonment up to 5 years and/or fine of ₹100000	Hacking of anyone's mail account and circulating disturbing content falls under this category.
67A	Publishing explicit private content	When a person transmits images relating to another person's private content.	Imprisonment up to 7 years and/or fine of ₹100000	Transmitting private content in the form of images or videos can be charged guilty under this section.
67B	Publishing child abuse content	When a person publishes offensive content of any individual less than the age of 18 years.	First conviction: Imprisonment up to 5 years and/or fine of ₹100000 Second conviction: Imprisonment up to 7 years and/or fine of ₹100000	Janhit Manch has launched the case under this section requesting a blanket ban on all the sites hosting child abuse content.
67C	Failure to maintain records	When a person fails to maintain records as mentioned by the cyber laws.	Imprisonment up to 3 years and/or fine of ₹200000	IT Company not maintaining proper records.
68	Failure or refusal to comply with orders	When a person refuses to comply with the Order issued by the Controller/Certifying Authority, with reference to the cyber laws.	Imprisonment up to 7 years and/or fine of ₹100000	A website owner, having pirated videos or torrents refusing to pull down the site and uses alternate domains.

69	Failure or refusal to decrypt data	When a person refuses to decrypt sensitive data which poses a threat to the unity and sovereignty of the state.	Imprisonment up to 7 years and/or fine	When a professional refuses to decrypt the secretive information from the neighbouring Countries.
70	Securing access or attempting to secure access to protected systems	When a person tries to access a protected system, which is originally declared a protected system by the Official Gazette.	Imprisonment up to 10 years and/or fine	Hacking government site on symbolic days like the republic day or independence day.
71	Misrepresentation	When a person misrepresents information to the Controller or Certifying Authority.	Imprisonment up to 3 years and/or fine up to ₹100000	When an IT company fakes facilities to obtain international standard certificate.

Criticism of the Act:

The law does not address the issue of Intellectual Property Rights and does not have information regarding copyrighting, patenting and trade marking.

The law does not contain regulations pertaining to electronic payment gateways.

An *example* instance of implementing the Information Technology Act:

Section 66: In 2001, two men were arrested on the charge of shutting down a website, claiming the reason as non-payment of dues. However, the owner of the site had already paid the dues already. The Delhi police charged the men guilty under, Section 66 of the ITA.

(ii) IT Amendment Act (ITAA)

The Information Technology Amendment Act was introduced by the CERT-In or Indian Computer Emergency Response Team in the year 2008 to make changes and substantial addition to the IT Act 2000. The aim of the ITAA was to address issues which were not addressed by the original Information Technology Act 2000 and to promote further development of the IT industry and the security framework. The section 66A, 67A, 69A and 79

were introduced in the IT Amendment Act. The list of offenses and the penalties (As per the Act) are discussed in the table 5.2.2.

Table 5.2.1 list of offenses and penalties of the IT Amendment Act

Section	Heading	Description	Penalty	Implementation Example	
66A	Sending offensive messages or threatening information	This section prohibits sending of offensive messages through an online communication medium which may cause inconvenience/danger/enmity/hatred/annoyance or any other sort of ill feeling to the receiver.	The convicted person can be charged upto 3 years and/or fine.	Indian cabin crew members were arrested for posting insulting the national flag and were kept in prison for 12 days.	Introduced in the IT Amendment Act 2008.
67A	Prohibiting circulation of explicit offensive content	This section deals with the prohibition of circulating obscene material on the internet.	The convicted person can be charged upto 7 years and/or fine.	MMS sent via whatsapp or social messengers containing offensive content can get the sender arrested and/or pay a fine.	Introduced in the IT Amendment Act 2008

69A	Posting information, inactive in nature	This section allows the Central Government to block any electronic content, if it is found to threaten the sovereignty/integrity/unity/defence of the nation. A set of guidelines and procedures to be adhered to are added to the Act which is called as blocking rules.	The information or post is blocked/banned by the Central Government.	A website which posts memes inciting the mob against the government can be banned under this section.	Substituted in the IT Amendment Act 2008 with detailed
79A	Establishes examiner of electronic evidence	This section establishes an examiner of electronic evidence to provide help in investigating cybercrimes. The nature of evidence includes all evidences transmitted or stored in digital format.	-	While cases dealing with electronic evidence are investigated, help is provided by the examiner of electronic evidence.	Introduced in the IT Amendment Act 2008

Criticism of the Act:

- The penalties of cybercrimes are decreased in ITAA.
- The issues related to safeguarding the civil rights of individuals in the electronic media is not addressed in the Act.

Example instance of implementing the Information Technology Amendment Act:

Section 66A: In 2010, a cartoonist named Aseem Trivedi was arrested under section 66A of the ITA for spreading cartoons related to the widespread corruption in India on the web.

(iii) Scope and Applicability of ITA and ITAA

Scope and applicability of ITA:

The scope of the Information Technology Act applies to:

- Processing of entire or a part of personal data, by using automatic means, which include the electronic storage of data or information in organisations, companies, etc.
- Processing of personal data which forms a part of the filing system like audits, databases

The ITA is not applied to:

- Contract of sale involving an immovable property, which makes transfer of immovable properties like land, invalid vehicle, if done using electronic means.
- Establishing electronic attestation as a means of trust (physical attestation is deemed mandatory). This makes self-attesting or attested by a gazetted officer invalid, if done using electronic means.
- Providing the power of attorney for a property via electronic record, since the transfer of power is deemed invalid, when done using electronic means.

Scope and applicability of ITAA:

The scope of the Information Technology Amendment Act applies to:

- All the areas as stated in the Information Technology Act (2000) which include processing of information using electronic means, transmitting or posting information via messengers
- Any person who commits a cybercrime in or outside India, where the victim or a person who has committed the crime is of Indian origin.

The IT Amendment Act is not applicable to:

- Negotiable instruments as per the Negotiable Instruments Act (1881), which guarantees a specific amount of money to a payer with his name mentioned in the document.
- Defining a seal of trust to establish an identity to a business or organisation and to guarantee its secure nature to the customers.

- 

Information Security - I | Risk Assessment and Cyber Laws

5.2.3 Cyber Laws - a Global Perspective

Cyber crimes are generally international since there is no border between the countries, when it comes to cyber crimes. However, the global cyber laws challenge the local or domestic cyber laws. Co-operation is required among the countries to ensure the implementation of global standards with respect to cyberspace.

(i) Contractual Issues in Cyberspace

When an electronic contract or e-contract is drafted, the contract should adhere to the UN General Assembly Resolution passed in January 1997, regarding the validity and the formation of the contract. The acceptance and offer of the contract can be by means of data message or any other electronic media. However, it is up to the law of the country to accept or deny the validity of the contract since it is not in paper format.

International cyber crime may be:

- A social engineering scam where networking chats are used to obtain information
- Intellectual property theft or IP theft, which includes creating pirated software and CD-ROMs
- Highly targeted worms which concentrate on a particular country's industry
- Platform switch where a particular platform's vulnerabilities are exploited forcing the use of another platform
- Introducing and spreading malware – U.S.A ranks first in this cybercrime with 51.5% of such crime originating from the USA.

International cyber laws and responses are listed as follows:

- **G8** – G8 or group of eight is a group of eight pioneer countries in the computer industry: U.S.A., UK, Russia, Germany, Canada, Japan, Italy and France. In 1997, an action plan to combat the threats and attacks in cybercrime and the principles to be followed to protect systems and data, were introduced.
- **United Nations** – The UN General Assembly adopted a resolution to deal with cybercrime in the year 1990. In 2002, a second convention was adopted to prevent the misuse of information technology.
- **Council of Europe** – The Council of Europe, containing 47 member states, adopted a convention on cybercrime in 2001. The convention was aimed at preventing the

Internet criminal behaviours, fighting cybercrime and enabling law enforcement with international cooperation.

- **APEC** - Asian-Pacific Economic Cooperation is an international forum in the Asia-Pacific Region to promote cooperation among member nations regarding information sharing, security and guidelines for the transmission of information. A total of six areas were discussed.
- **OECD** – OECD (Organisation for Economic Cooperation and Development), supported by 34 countries created a set of guidelines and practices to be followed in 1992.
- **European Union** – In 2002, the European Union a “Framework decision on attacks against information systems” which deals with the provisions of cyber laws and protects the information and devises against such attacks.
- **Commonwealth** – A model law was presented by the Commonwealth of Nations, in the year 2002, to provide a legal framework for cyberspace to maintain the harmonious relationship between the Commonwealth nations.
- **ECOWAS** – The ECOWAS or Economic Community of West African States adopted a Directive against Cybercrime, which provides a framework for cyberspace with reference to the criminal law.

(ii) Non-Contractual Issues in Cyberspace

The issues that occur in cyberspace may not be covered in the contract, since cyberspace has a wide scope. The non-contractual issues are kept in mind while using the cyberspace. These issues, when addressed to improve the overall security of the system significantly.

- **When a person with malicious motive persuades you to run his/her program on your computer:**
When a program from a source, which is not trusted, is downloaded or allowed to run in the system, the entire system can be under the control of the program. The program can perform illicit actions which may be viewed as offenses by the cyber laws.
- **When a person with malicious motive can alter the Operating System on your computer:**
Altering the source code of the operating system can alter the system privileges via which the malicious user can be made the administrator of the system or passwords in the system can be altered or accessed.

- **When a person with malicious motive, has unrestricted access to your computer:**

When unrestricted access is provided to a person, then the person can inflict physical damage to the computer like destroying the hard disk or unplugging the system. The person may duplicate the hard disk or replace the keyboard with a transmitter and monitor anything that is typed into the system. To prevent these issues, the system is protected physically using additional protected measures.

- **When a person with malicious motive is allowed to upload programs to your website:**

The person may upload programs to your website which can cause harm to the users. Hence the websites should be designed in such a way that the scope of visitors is limited.

- **Weak passwords are used:**

Even with a strong security system, weak passwords act as a potential threat to the system. Hence, guidelines for passwords are set to make them immune to hacking attempts such as not using common details like name or city in the password, making the password, complex by adding a combination of upper case and lower case letters and punctuation marks.

- **Computer device is considered as secure as its administrator designs it to be:**

The administrator of the computer has authority to configure the OS, manage the users in the system and assign privileges to the user. Based on the security policies set by the administrator, the system can be either a secured system or easily accessible system for the attack launchers

- **The encrypted data is as secure as the decryption key:**

However complex the encryption algorithm is, the security it provides is based on the decryption key. The decryption key should not be stored in the computer as it is easier to access the information which is encrypted.

- **Out of date virus scanners are more or less equal to no scanner at all:**

Updating virus scanners regularly are mandatory as new viruses are being created every day. The virus scanner scans the data against the virus signatures stored in the virus scanner for the detection of virus. Hence an outdated virus scanner is considered rather useless as it wouldn't have the signatures of the newly created viruses.

- **Absolute anonymity is not possible on the web:**

Privacy is difficult to maintain on the web since there might be cookies loaded in your computer whenever you visit a site and avoid the malicious looking sites. Anonymity to a certain extent is possible by using kiosks to surf sites, mask your original IP address and use different ISP or Internet Service Provider for different purposes.

(iii) Challenges in the Enforcement of Cyber Laws and Recommended Strategy for Effective Environment

The existing cyber laws find it difficult to enforce secure state in cyberspace as the rate of cybercrime keeps escalating, while the cybercrime laws are not updated periodically. The challenges faced in the enforcement of cyber laws are listed as follows:

- **Branch of law**

Cases are dealt normally by Criminal law, Civil law or Regulatory law. While the civil system deals with disputes between parties charging monetary penalty or by assigning ban on certain actions. The regulatory agencies have the authority to impose fines or ban business of an organisation. While implementing cyber law, the challenge faced is, if the dispute comes under regulatory or civil law or a combination of both jurisdictions.

Recommended Strategy: The recommended strategy would be to determine the authority of both the law divisions or create a new law division dealing with just cyber crimes.

- **Type of Case:**

Depending upon the severity and nature of the case, cases are assigned to courts with necessary authority. There is no separate type of court to deal with cyber crimes which make it difficult to assign the court to deal with such type of cases. *For example*, a person may be charged guilty by state law and then by the federal law by two courts.

Recommended Strategy: The overhead of conducting trials in different courts can be prevented by assigning courts specially dedicated to cyber law enforcement.

- **Geographical area:**

The geographic jurisdiction of the convicted is required to pursue charges against him. This aspect is difficult to determine in cybercrime, since the geographical location of the convict may be difficult to determine. Even if the location is determined, the convict and the victim may not be in the same Country. Laws for cybercrime vary from Country to Country. What is treated to be an offense in the victim's Country may not be an offense in the convict's Country. In this case, no action can be taken against the victim, since the geographical location he/she falls under, does not consider the charge against the victim, a crime.

Recommended Strategy: The best option would be to establish International standards in the cyberspace, which is adhered to, by all nations.

- **Identity of the convict:**

The identity of the convict is necessary to launch complaints. In cybercrime, the identity of the victim is very difficult to determine even with the help of IP addresses. There are lots of options available in the current scenario to mask the identity of the convict, making the task of obtaining anonymity, easier. This gives the freedom to the people to perform offensive actions in the cyberspace.

Recommended Strategy: The International conventions should be followed to track identity of all the users in the cyberspace by assigning them a unique id.

- **Nature of evidence:**

Unlike real world crimes, cybercrimes have lesser evidence which can be easily destroyed. Similarly, fake evidences can be fabricated for cybercrimes. The victim can easily create evidences of a crime which never happened or the convict can destroy electronic evidence or logs related to the crime.

Recommended Strategy: Care should be taken while investigating evidence in cyberspace.



Self-assessment Questions

- 6) Which of the following is not an International cybercrime?
 - a) Spreading Malware
 - b) Intellectual Property Theft
 - c) Maintaining anonymity in the cyberspace
 - d) Social Engineering Scam

- 7) What resolution was taken by the United Nations against cybercrime?
 - a) To deal with cybercrime and prevent misuse of technology
 - b) To promote cooperation in cyberspace
 - c) To create guidelines for information exchange
 - d) To protect against attacks

- 8) Which of the following is true regarding cyberspace?
 - a) An Outdated virus Scanner is useless
 - b) A decryption key need not be secure
 - c) An Administrator does not have a say in the security of the system
 - d) Absolute anonymity is possible

- 9) What is of the following is a challenge faced while enforcing cyber laws?
 - a) Geographical Location of the Convict
 - b) Identify the Convict
 - c) Both a and b
 - d) Electronic evidences are not accepted by law

- 10) Which of the following is true regarding cyber evidence?
 - a) Evidence can be easily faked
 - b) Evidence can easily be destroyed along with the related logs
 - c) Both a and b
 - d) Electronic evidences are not accepted by law

5.2.4 Fair Model

The FAIR model or the Factor Analysis of Information Risk is a model or framework used in Information Security practices to understand, analyse and measure the information risk. FAIR model plays a vital role in the security of the organisation since it integrates the security aspect with the risk associated with the organisation. The more secure the organisation is, the lesser is the associated risk. Each step in the FAIR model deals with how valuable the asset is and how secure the asset is, against a threat agent and the risk associated with the asset, which can be caused by the threat agent. In information security, the FAIR model can be used to assess the level of security provided to the assets and is the security level provided for the asset is proportional to its value.

The basic FAIR analysis consists of four stages which are:

- **Stage 1 – Identifying the scenario components**

This stage deals with identifying what is at risk and which threat poses such a risk.

This stage involves two processes which are:

- Identifying the assets in the organisation which are at risk
- Identify the community which poses a threat

- **Stage 2 – Evaluating the LEF (Loss Event Frequency)**

The second stage deals with deriving various factors associated with the risk, such as Threat Event Frequency (TEF), Threat Capability (TCap), Control Strength (CS) and Loss Event Frequency Factor (LEF). Based on the value of the factors, the risk rating can be classified as VH- Very High, H- High, M-Moderate, L-Low or VL-Very Low.

Stage 2 involves the following 5 processes:

- Estimating the probable TEF factor (Threat Event Frequency)
- Estimating the Capability of the threat
- Estimating the Control Strength for the threat or CS
- Deriving the associated vulnerability
- Deriving the Loss Event Frequency factor (LEF)

- **Stage 3 – Evaluating the PLM (Probable Loss Magnitude)**

At this stage, the probability of the loss event is calculated which is between 0 and 1.

The processes that constitute this phase are as follows:

- Estimating the case of worst loss
 - Estimating the probable loss magnitude factor or PLM
- **Stage 4 – Deriving and Articulating Risk**
The risk factor is obtained from the LEF and PLM values and articulated in the worst case.

Deriving and articulating the associated risk

Example scenario:

Consider a bank, whose risk is assessed using the FAIR model.

- **Stage 1:** The asset in bank organisation taken into consideration is the bank user database which contains details of the user login and passwords. The community which poses a threat is potential hackers, competitive organisation employees trying to obtain the user details.
- **Stage 2:** In this stage, the threat event frequency for the bank database is calculated based on the number of times, the bank database has been attempted to be hacked or accessed by malicious attackers.

The capability of the threat, based on the vigour of the attacks is calculated,

The control strength or security provided to the asset (bank database) is estimated. The control strength of the database implies the ability of the database to withstand attacks. Based on this factor, it is determined if the security measures to the asset are enough.

The vulnerability of the database is calculated using the control strength and threat capability factors calculated in the previous steps. If the bank database has been provided with the required security measures, then the database has lesser vulnerability.

The threat event frequency or the number of times the bank database has been tried to be hacked from a particular source is recorded. The security measures are made vigilant for sources or attackers whose TEF is on the higher end.

- **Stage 3:** In this stage, the worst case scenario of the bank database being hacked is discussed. The loss or monetary value associated with the bank database is calculated. The probable loss magnitude is calculated, keeping various factors in mind. Since the sensitivity of the bank database is much higher, the PLM is also high.
- **Stage 4:** The risk associated with the bank database is derived using all the factors derived in the previous steps. Using this analysis, it can be determined, if the security measures practiced for the bank database are enough to deal with the threat agents.

(i) Purpose of Risk Modelling

The main aim of the FAIR model is to address the security issues or the weaknesses in the security practices. The objectives of the FAIR model include:

- Provide a model for quantifying the information risk of the organisation in the financial point of view after a detailed understanding and analysis of the risk associated.
- Applying risk assessment to all the assets or objects in the organisation.
- Challenge or defend the determination of risk in the organisation using advanced analysis.
- Establish the same language, as a medium of communication, regarding risk management and information security.
- Determine how resources like time and money will affect the security profile of the organisation.
- Building a basis for information risk management, aiding the development of a scientific approach to risk management.
- Creating new risk analysis and assessment methods and strengthen the existing methods.
- Introducing and following consistency in risk analysis and modelling.

(ii) Benefits of Fair

The benefits of using the FAIR risk model in an organisation include:

- The FAIR model makes use of one language and mode of communication when it concerns to risk.
- The objects or assets in the organisation are consistently studied and risk factors are applied.

- An advanced risk model is made use of, to challenge and defend all the possible risk decisions.
- Makes the employees and stakeholders understand the impact of time and money on the security profile of the organisation.
- The FAIR model adds a financial dimension to the RISK Management framework of the organisation.
- The enterprise risk of the organisation is viewed in its totality to gain a better understanding.

(iii) Fair Model Components

The components constituting the FAIR model are explained in the following section.

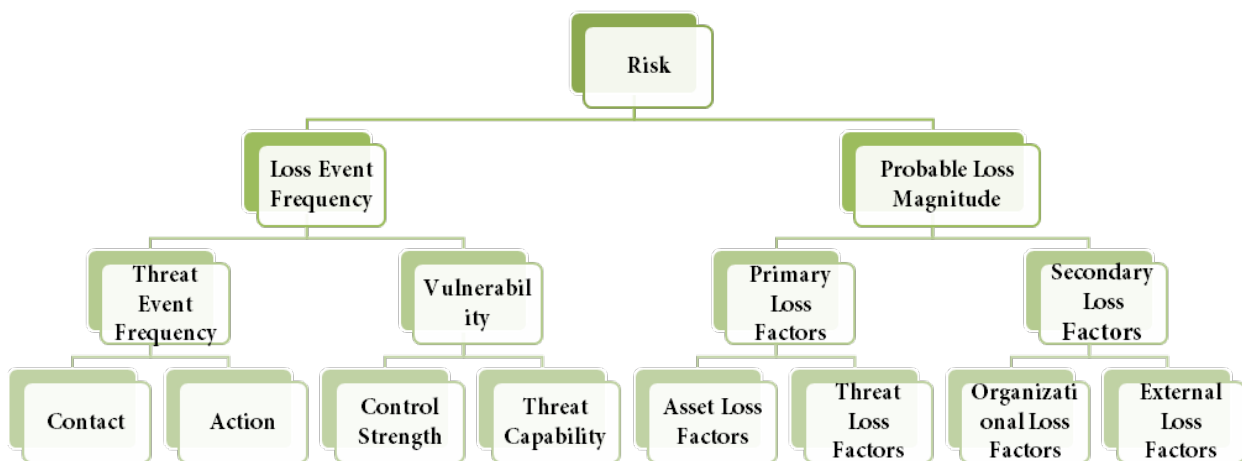


Figure 5.2.1: FAIR model and its components

The above figure 5.2.1 illustrates the hierarchical view of the components of the FAIR model.

- **Risk**
Risk implies the probable magnitude or frequency of future loss in the organisation. The FAIR model comprises of two main branches, namely:
 - Loss Event Occurrence
 - Loss Magnitude
- **Loss event Frequency(LEF)**
The Loss Event Frequency is the number of times a threat agent can harm the asset in a given timeframe. Loss Event Frequency can be calculated using two factors which are Threat Event Frequency and Vulnerability.

- **Threat Event Frequency(TEF)**

The Threat Event Frequency factor is the number of times there is a threat caused due to the particular agent in the given timeframe. LEF holds the successful threats that cause harm to the asset, whereas all the threats, including the unsuccessful ones are recorded in the TEF. TEF is calculated based on the following factors:

- **Contact** – The number of times, the threat agent comes in contact with the asset. The contact can be logical as in a network or physical. Contact is dependent on various factors relating to the object. The types of contact between the threat agent and the asset can be one of the following modes:
 1. **Random** – the threat agent randomly comes in contact with the asset during its course of unplanned activity.
 2. **Regular** – the contact between the threat agent and asset takes place due to the regular planned activity of the threat agent.
 3. **Intentional**- the threat agent comes in contact with the asset for seeking specific target.
- **Action** – Once the threat agent has established contact with the asset, the action part starts. Action may or may not take place depending upon the type of the threat agent. The probability of the action part to take place depends upon the following primary factors:
 1. **Value**- the threat agent's perception of value obtained in performing the action.
 2. **Level of effort** – the effort needed by the threat agent to perform the act.
 3. **Risk** – the negative consequences that will be incurred by the threat agent in performing the act.

- **Vulnerability**

The vulnerability factor is the probability of the actions launched by the threat agent and the inability of the asset to prevent it. Vulnerability is relative to the type of threat or risk involved.

In short,

Vulnerability of the asset = (force applied by the threat agent) – (ability of the object to resist the threat)

The vulnerability of an object can be computed using the following factors:

- **Control Strength** – The strength of the object, whose vulnerability is calculated. *For example*, control strength of passwords can be calculated in percentage based on the nature of the password and the number of hacking attempts, the password can resist.
 - **Threat Capability** – The capability of the threat agent against the asset is measured using this factor. The threat agent may be capable in one type of attack on a specific asset and lag in the other types of attacks.
- **Probable Loss Magnitude (PLM)**

The Probable loss magnitude measures the most likely outcome caused by the threat agent. However, PLM has been difficult to calculate since:

- Assigning precise values to the assets at risk is difficult
- Loss magnitude is determined by various factors
- Loss can be in numerous forms
- Many forms of loss can be triggered by a single event
- Relationships between different forms of loss is complex
- Assets hold different values and liability

Loss of an asset due to a threat agent can result in any of the following losses:

- **Productivity** – reduction in the ability of the organisation to produce its primary value in terms of goods or services.
- **Response** – the expense incurred by reacting to a loss event.
- **Replacement**- cost incurred while replacing an asset which is equal to the intrinsic value of the asset.
- **Fines and Judgements** – legal actions taken against the organisation.
- **Competitive advantage** – loss of competitive advantage of the system, including sensitive information or production strategy of the organisation.
- **Reputation** – the goodwill or external perception of the organisation is spoilt making the organisation look unethical or incompetent.

- **Primary Loss Factors**

The primary loss factors involved during an attack of threat agent on an asset are the factors, internal to the organisation. They can be categorised as:

- **Asset Loss Factors**

The asset loss factors associated with the organisation are value/liability of the asset and the volume of the asset.

The asset volume means the number of assets at risk. The more the number of assets at risk, the greater is the loss of magnitude.

The asset value or liability is calculated in terms of

1. **Criticality**- the critical characteristics of the asset at risk. Eg: A corrupt database holding all the user details is considered a critical asset.
2. **Cost** – the materialistic value of the asset
3. **Sensitivity** – the nature of the asset and the harm it may cause, when exposed.

- **Threat Loss Factors**

The threat loss factors taken into consideration in the FAIR model are:

1. **Action:**

The threat agent can take up any of the following actions, while launching an attack on the asset:

- Unauthorised access to the asset
- Misuse or malicious usage of the assets
- Disclosing sensitive information about the organisation
- Modifying or making unauthorised changes in the data or information about the asset
- Denying legal access to the asset by destroying it

2. **Competence:**

The competent nature of the asset plays a vital role in the attack. When a threat agent causes a file storing sensitive information to be deleted causes lesser loss to the organisation rather than exposing the file to the rival organisation.

If the threat is external/internal to the organisation plays a vital role as it is important to identify the source of threat and the loss caused due to the source.

- **Secondary Loss Factors**

The secondary loss factors involved during an attack of threat agent on an asset are the factors, external to the organisation. They are categorised as:

- **Organisational Loss Factors:**

The organisational loss factors taken into consideration are:

1. **Timing** – the timing of the event has significant impact on the loss caused. *For example*, an event occurring during the peak season of the organisation has greater impact than one occurring during the off season.
2. **Due diligence** – due diligence refers to the liability of the organisation. The organisation is checked for following the best practices and preventive measures.
3. **Response** – the way the organisation responds to the event. The three components in the response are containment (limiting the impact of the event), remediation (ability of the organisation to eradicate the threat agent) and recovery (ability of the organisation to restore normal state).
4. **Detection** – the events are to be detected to fabricate a response. Proactive detection of events reduces the loss caused.

- **External Loss Factors:**

The external loss factors taken into consideration are:

1. **Detection** – external factors can detect the event if it is found to be severe and is considered to be a loss.
2. Legal and regulatory landscape includes the fine and regulations imposed by the case law and contract law.
3. Competitive landscape causes loss when the competitor takes advantage of the situation created due to the event.
4. Media reaction influences the reaction of stakeholders and other viewers to the event.
5. External stakeholders can cause loss to the organisation by stopping business with the organisation. Such a decision may be since the external stakeholders feel that the view or vision of the organisation has become

incompetent or their interests are served in a better way, elsewhere or the stakeholder has been directly affected due to an incident.



Self-assessment Questions

- 11) How many stages and processes does the FAIR model have?
 - a) 4 stages and 10 processes
 - b) 4 stages and 9 processes
 - c) 4 stages and 8 processes
 - d) 4 stages and 13 processes
- 12) Which dimension is added by FAIR model to information security?
 - a) Strategic
 - b) Financial
 - c) Risk
 - d) International
- 13) Which of the following does Threat Event Frequency depend on?
 - a) Asset loss and Threat loss
 - b) Organisational loss and External loss
 - c) Control and Action
 - d) Control strength and Threat Capability
- 14) Which of the following are Primary Loss Factors?
 - a) Asset loss and Threat loss
 - b) Organisational loss and External loss
 - c) Control and Action
 - d) Control strength and Threat Capability
- 15) Which of the following are Secondary Loss Factors?
 - a) Asset loss and Threat loss
 - b) Organisational loss and External loss
 - c) Control and Action
 - d) Control strength and Threat Capability



Summary

- Cyber crime is of two types where the computer is the target of crime or computer is used as a weapon to attack.
- The major cyber laws in India include Information Technology Act or ITA (2000) and the Information Technology Amendment Act or ITAA (2008).
- The Information Technology Act was introduced to prevent cybercrime, facilitating and regulating e-commerce and promoting IT industry.
- The ITA law does not address the issue of Intellectual Property Rights.
- The drawbacks of ITSS include decreased penalty and not safeguarding the interests of individuals in the cyberspace.
- The contractual issues in the global space require cooperation among countries to implement the global standards.
- Challenges faced while enforcing the cyber laws include the branch of law, type of case, geographical area, the identity of the convict and nature of evidence.
- The FAIR model is used in Information Security practices to understand, analyse and measure the information risk.
- The benefit of the FAIR model is to add a financial dimension to the RISK Management framework of the organisation.



Terminal Questions

1. Explain various cyber laws prevailing in India.
2. Describe some common global cyber laws and issues related to it.
3. What are the purpose and benefits of using the FAIR model in cyber law?



Answer Keys

Self-assessment Questions	
Question No.	Answer
1	b
2	b
3	c
4	c
5	d
6	c
7	a
8	a
9	c
10	c
11	a
12	b
13	c
14	a
15	b



Activity

Activity Type: Online/Offline

Duration: 30 Minutes

Description:

Form a group of five and give presentation on the history of Cyber Laws in India.

Bibliography



e-References

- *Cybercrime laws*. Retrieved 12 Feb, 2017 from <http://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/>
- *E-contract in Cyberspace*. Retrieved 12 Feb, 2017 from <http://www.legalserviceindia.com/article/article/a-study-of-formation-and-challenges-of-electronic-contract-in-cyberspace-1943-1.html>
- *Laws of security*. Retrieved 12 Feb, 2017 from http://www.wciapool.org/pdf/Tab_5_10_Immutable_LawsofSecurity.pdf

Image Credits

- Figure 5.2.1: <http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf>



External Resources

- Singh, S. (2011). *Cyber laws*. New Delhi: Global India Pubns.
- Punia, C. K. (2009). *Cyber laws*. New Delhi: Sumit Enterprises.
- Singh, Y. (2005). *Cyber laws: a guide to cyber laws, information technology, computer software, intellectual property rights*. Delhi: Universal law publication.



Video Links

Topic	Link
Cyber Laws in India	https://www.youtube.com/watch?v=TAz-E06SdBk
Cyber Law need and importance	https://www.youtube.com/watch?v=1vQhSm5_UqY
Future of Cyber Law	https://www.youtube.com/watch?v=9hXHm3alzDs



Notes:

