Master of Computer Applications (MCA)

Information and Network Security (DMCACO104T24)

Self-Learning Material (SEM 1)

Jaipur National University
Centre for Distance and Online Education

Established by Government of Rajasthan
Approved by UGC under Sec 2(f) of UGC ACT 1956
&

Jaipur National University

Course Code: DMCACO104T24
Information and Network Security

TABLE OF CONTENTS

EXPERT COMMITTEE

Prof. Sunil Gupta
(Department of Computer and Systems Sciences, JNU Jaipur)

Dr. Deepak Shekhawat
(Department of Computer and Systems Sciences, JNU Jaipur)

Dr. Shalini Rajawat
(Department of Computer and Systems Sciences, JNU Jaipur)

COURSE COORDINATOR

Swarnima Gupta
(Department of Computer and Systems Sciences, JNU Jaipur)

UNIT PREPARATION

Unit Writer(s)	**Assisting & Proofreading**	**Unit Editor**
Mr. Ramlal Yadav (Department of Computer and Systems Sciences, JNU Jaipur) (Unit 1-5)	Ms. Rashmi Choudhary (Department of Computer and Systems Sciences, JNU Jaipur)	Dr. Satish Pandey (Department of Computer and Systems Sciences, JNU Jaipur)
Mr. Pawan Jakhar (Department of Computer and Systems Sciences, JNU Jaipur) (Unit 6-9)		

Secretarial Assistance
Mr. Mukesh Sharma

COURSE INTRODUCTION

"Clean code always looks like it was written by someone who cares."
- Robert C. Martin

In the rapidly evolving digital landscape, the importance of securing information and network systems has never been more critical. The "Information and Network Security" course is designed to provide students with a comprehensive understanding of the principles, practices, and technologies essential for protecting information and maintaining network integrity. As cyber threats become increasingly sophisticated and pervasive, this course equips students with the knowledge and skills necessary to defend against various security challenges and ensure robust protection of data and systems.

This course has 3 credits and is divided into 9 Units. The course begins with a foundational overview of information security concepts, introducing key terminology and frameworks. Students will explore the core principles of confidentiality, integrity, and availability—often referred to as the CIA triad—which form the basis of any security strategy. Understanding these principles is crucial as they underpin all security measures and policies implemented in organizations.

A significant portion of the course is dedicated to examining various types of threats and vulnerabilities that can compromise information and network security. This includes detailed discussions on malware, phishing attacks, ransomware, and other malicious activities that target systems and data. By analyzing real-world case studies and recent security incidents, students will learn to identify potential risks and understand their impact on both individuals and organizations.

The course also covers the essential security technologies and tools used to safeguard information and networks. Topics such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and encryption techniques are explored in depth. Students will gain hands-on experience with these technologies through practical exercises and simulations, allowing them to apply theoretical knowledge to real-world scenarios.

Ethical and legal considerations are integral to the study of information and network security. The course addresses issues related to privacy, intellectual property rights, and regulatory compliance. Students will explore various legal frameworks, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), understanding their implications for security practices and organizational policies.

Course Outcomes:

At the completion of the course, a student will be able to:

1. Describe network security services and mechanisms.
2. Apply Symmetrical and Asymmetrical cryptography.
3. Implement Data integrity, Authentication, Digital Signatures.
4. Implement various network security applications, IPSec, Firewall, IDS, Web security, Email security, Malicious software etc.
5. Understand how to deploy encryption techniques to secure data in transit across data networks.
6. Design security applications in the field of Information technology

Acknowledgements:

The content we have utilized is solely educational in nature. The copyright proprietors of the materials reproduced in this book have been tracked down as much as possible. The editors apologize for any violation that may have happened, and they will be happy to rectify any such material in later versions of this book.

Unit : 1

A Model for Internetwork Security

Learning Outcomes:

- Students will be able to understand the basic concepts of Internetwork security
- Students will be able to understand and apply the basic concepts of encryption
- Students will be able to understand the various modes of block ciphers and their operations
- Students will be able to locate the concepts and then apply them in day-to-day scenarios
- Students will be able to understand the various public key distribution algorithms and their means and mechanism wherein they can be applied

Structure

1.1 Introduction

In this unit, we discuss the basic concepts of Internet security and the various means and mechanisms which are involved in the process of implementing security in the various operations which are involved in the course of doing work. Nowadays with the heavy dependency on the internet, security issues pertaining to various operations have begun to surface. For example, during the course of financial transactions or otherwise, incidents pertaining to the siphoning of money to unscrupulous account holders have been reported. Further, these breaches are confined not only to financial transactions but they do have an indirect origin to money. For example, the recent incident wherein the AIIMS server was hacked by unscrupulous persons who demanded ransom for unfreezing the server so that normal operations can be performed.

All these incidents point to the fact that there is an urgent to adopt mechanisms so that security breaches are nullified or prevented. In other words, one cannot afford to remain idle. These incidents will be bound to occur and will pose a greater and exponential challenge to the authorities.

All this boils down to the fact that there is an urgent need to develop measures that would provide adequate assurance for the protection of assets that are operating through the medium of the internet.

Encryption, cryptography, and the like are some of the measures which are adopted for securing our digital assets.

This unit deals with various models for internetwork security.

1.2 Conventional Encryption Principles and Algorithms

Before we dwell on the concepts of encryption and its application, let us first discuss what is meant by internetwork security. In simple parlance, the term internetwork security refers to the process of identifying, defining, implementing, and evaluating the various components of valuable information so that they are secured when they are transmitted over an electronic medium. In other words, it involves the implementation of various techniques which secure these informational components *so that unscrupulous individuals* fail to exploit the information to achieve their mala fide objectives.

Encryption is one such technique that is commonly adopted to prevent unauthorized users from exploiting the information.

Let us first define what is meant by the term encryption. In simple terms, the word is a process for converting information into a form that cannot be read by any other unintended individual when it is carried over the internet or transmitted over the net. The information can only be read by the authorized individual as it is delivered to the intended person or persons only.

Refer to the figure given below

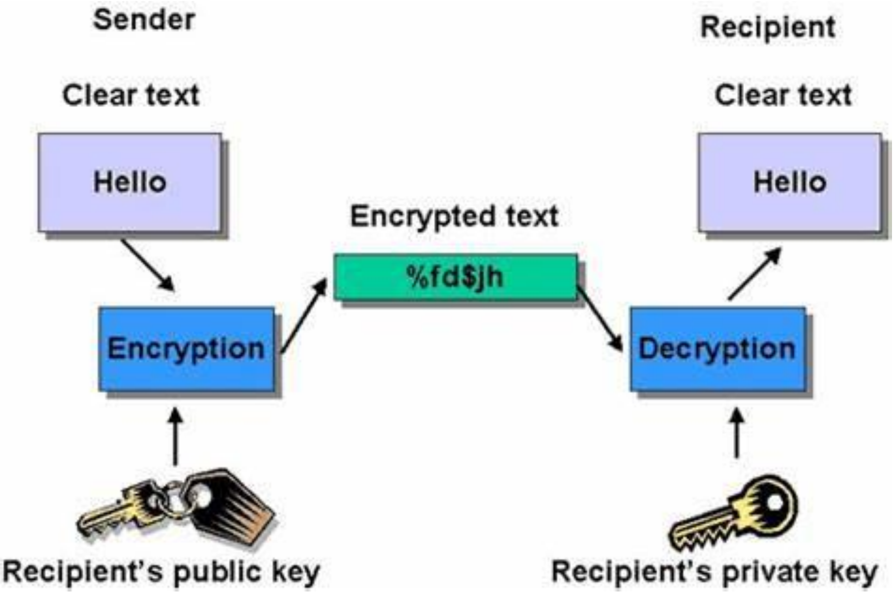


Fig. 1.1 Conventional Encryption Principles and Algorithms

From the figure 1.1, it is evident that when the information is transmitted between the sender and the recipient it is encrypted that is it is converted into a form that cannot be deciphered by anyone else except the recipient. Thus, the word Hello is first converted into an encrypted text comprising of %fd$jh. This action generates information that cannot be read and understood. However, when it reaches the intended person the reverse process takes place that is it is decrypted into a form that can be read by the recipient. Thus we have two fundamental processes one for conversion of the information and the other to re-convert the encrypted information back to its original state.

With this basic concept in place, let us understand the process of conversion of information to an encrypted form.

When we are dealing with the process of encryption we follow a step-by-step procedure for the encryption process.

They are enumerated below:

Step 1: This is the step that is needed for identifying the object which is to be encrypted. It can be a simple text or anything which needs to be protected from exploitation. In other words, the object is the matter which needs to be converted into a form that cannot be read by unintended individuals (Figure 1.2).

Step 2: This is the step that is used for converting the contents of the object through an instruction-based process which is known as an algorithm.

Step 3: This is the step that is used to provide a unique identifier to the converted output so that only the intended person can use it to convert it back into its original form. In other words, the contents or the output of step 2 is used to generate a unique key known as a secret key which can be used to provide a unique identity to the converted object.

Step 4: This is the output generated by step 3. In other words, the Ciphertext is the output of an algorithm along with the unique identifier that is the key

Step 5: The process to uncover or decrypt the contents so that the intended user can read the contents.

The following flowchart depicts the process of encryption (Figure 1.3)

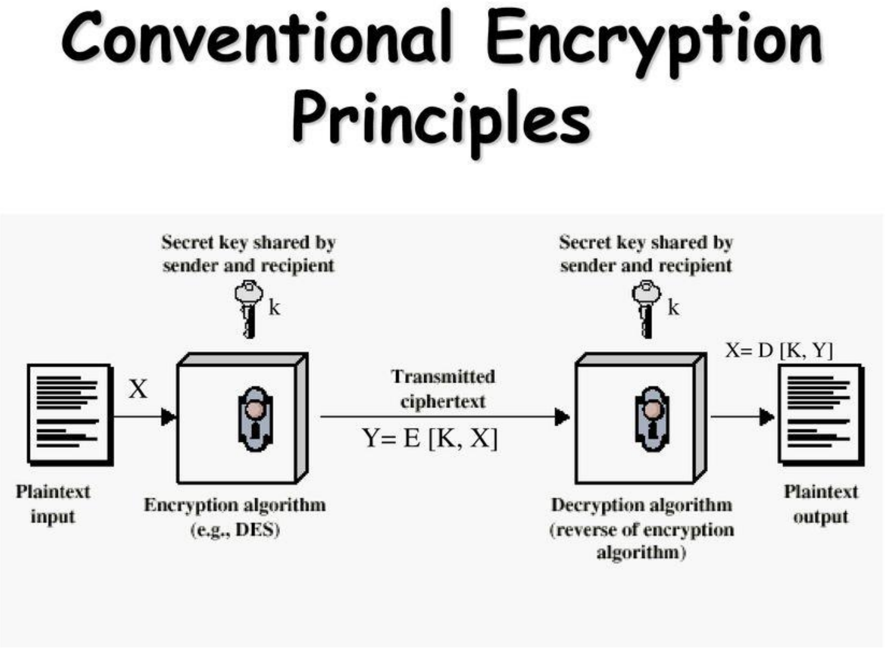

Conventional Encryption Principles
Secret key shared by sender and recipient
k
Secret key shared by sender and recipient
k
X= D [K, Y]
X
Transmitted ciphertext
Y= E [K, X]
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 1.2 : Simplified Model of Conventional Encryption

Having understood the conventional encryption principles let us now try to understand what is meant by the algorithm.

In simple parlance, an algorithm is a step-by-step process to complete a given task. With this basic definition in place, the process of encryption takes place in accordance with this step-by-step process.

Refer to the figure given below to understand the concepts covered above in a pictorial form.

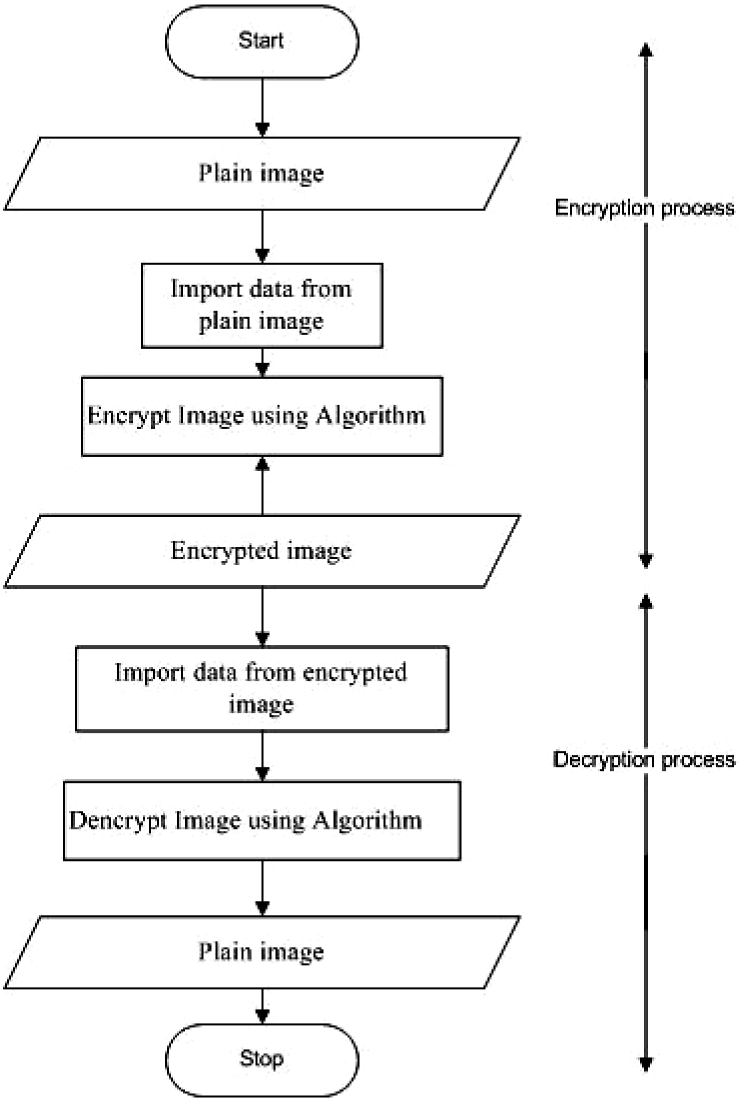

Start
Plain image
Import data from plain image
Encrypt Image using Algorithm
Encrypted image
Import data from encrypted image
Dencrypt Image using Algorithm
Plain image
Stop
Encryption process
Decryption process

Figure 1.3 : Flowchart of encryption process

The figure given above depicts the explanation of how the process works while encrypting the object which needs to be protected. However, the table given below depicts an example of how the encryption process can be actually applied. Worth mentioning is the fact that the examples which are given in the table below are not foolproof techniques. It depends on the object. For example, if the object is in the form of an image, then a different encryption format will be applied.

The following are basic algorithms that are used in the encryption process.

a. The DES algorithm. The term DES stands for Data Encryption standards
b. The AES algorithm. The term AES stands for Advanced encryption standard
c. The RSA algorithm. The term RSA stands for Rivest-Shamir-Adleman. This algorithm was developed by these three authors for the encryption process.

Thus, the above points highlight the commonly used algorithm for the encryption process. Worth mentioning is the fact there are other algorithms that are widely used. However, the usage is not confined to a single algorithm it depends on the type the degree, and the depth of the security needed to encrypt the data.

An example of a process of carrying out encryption as used in real life application

The following steps demonstrate a step-by-step process for converting an object which needs to be protected with the help of an algorithm.

- Identify an object which needs to be protected
- Develop the encryption algorithm
- Apply the algorithm to the identified object
- Pass the encrypted object to the intended destination
- Reconvert the object to generate the original text
- Display the original text

Let us suppose that we want to encrypt the object which is the password for the login id

The object identified is the password.

Let the password be say XYZ

We apply the following process for encrypting the same

- Replace the letters or the numbers with two succeeding letters or the numbers to the original password entered by the user.2

We thus have the following encrypted password.
ABC This is the encrypted password. It uses the algorithm which converts the digits with the next two succeeding digits or characters.

Now, this is the encrypted value that will be transferred to the receiver.

When it is received by the receiver, it is required to be decrypted is needs to be brought back to the same form.

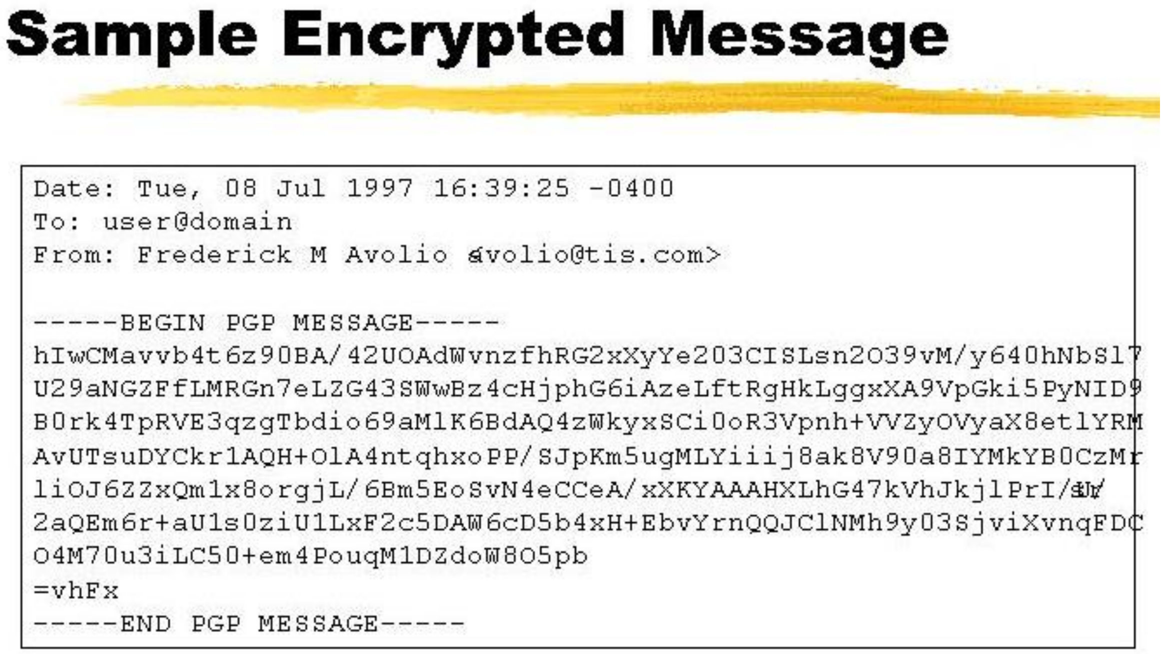
Thus, we apply the algorithm again to reduce it to the original structure.
The algorithm will run in a manner as mentioned in the following points

- Read the characters or letters one by one
- Replace each of the characters with the characters which occurred at two places before.
- Recreate the new character which is ABC

Worth mentioning is the fact that this algorithm is not the final one. The process of encryption can follow any logic. It all boils down to the degree and the depth of the encryption needed for the object which must be secured.

The following table provides some of the generic methods which can be applied in the algorithm for the purpose of encryption

Object of Encryption	**Original Value**	**Encrypted Value**	**Logic**
Password	ABC2	656667656667	Replace each letter with its ASCII value. Repeat these values as the suffix
Credit / Debit Card Details	1234-4567-8901-2345	*ABCD-EFGH-IJKA-BCD*	Put an asterisk before the original value. Replace 1 with A, 2 with B, etc. finally terminate the encrypted value with the asterisk sign



Sample Encrypted Message

```
Date: Tue, 08 Jul 1997 16:39:25 -0400
To: user@domain
From: Frederick M Avolio <avolio@tis.com>

-----BEGIN PGP MESSAGE-----
hIwCMavvb4t6z90BA/42UOAdWvnzfhRG2xXyYe203CISLsn2O39vM/y640hNbSl7
U29aNGZFfLMRGn7eLZG43SWwBz4cHjphG6iAzeLftRgHkLggxXA9VpGki5PyNID9
B0rk4TpRVE3qzgTbdio69aMlK6BdAQ4zWkyxSCi0oR3Vpnh+VVZyOVyaX8etlYRM
AvUTsuDYCkr1AQH+OlA4ntqhxoPP/SJpKm5ugMLYiiij8ak8V90a8IYMkYB0CzMr
liOJ6ZZxQm1x8orgjL/6Bm5EoSvN4eCCeA/xXKYAAAHXLhG47kVhJkjlPrI/sU/
2aQEm6r+aU1s0ziU1LxF2c5DAW6cD5b4xH+EbvYrnQQJClNMh9y03SjviXvnqFDC
O4M70u3iLC50+em4PouqM1DZdoW8O5pb
=vhFx
-----END PGP MESSAGE-----
```

Figure 1.4 : Sample Encrypted Message

The figure 1.4 depicts another method of encrypting an image.

1.3 Block Cipher modes of encryption

Before we dwell further into the various aspect of encryption, let us first try to understand what is meant by block cipher modes of operation. The Cipher as discussed above is the converted or the encrypted object which has a unique identifier attached to it. However, when it comes to the process of generation of cipher we use two types of techniques viz. *asymmetric* and *symmetric*. For the time being, the symmetric technique uses a single key and is used for protecting the confidentiality of the encrypted object while the asymmetric text is used for the sharing of the keys.

Block Cipher mode of encryption falls under the symmetric category.

In simple parlance, the term block cipher refers to the process of conversion of a block of text into a form that uses a combination of the secret key and the encrypted text.

The figure given below depicts the basic concept of the Block Cipher mode of encryption.

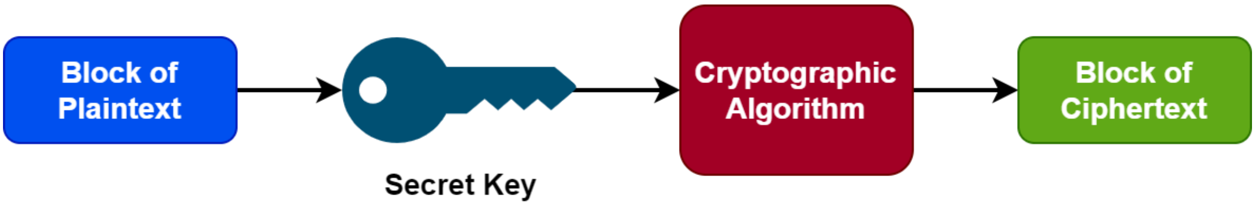


Figure 1.5 : Plain Text to Cipher Text

From the figure 1.5, it is clear that a block of plain text is converted by an algorithm to an encrypted form by adding a secret key or a unique identifier to the block of Cipher text. The same combination of the key and the Cipher text is used during the encryption process.
The common usage of a block of Cipher text.

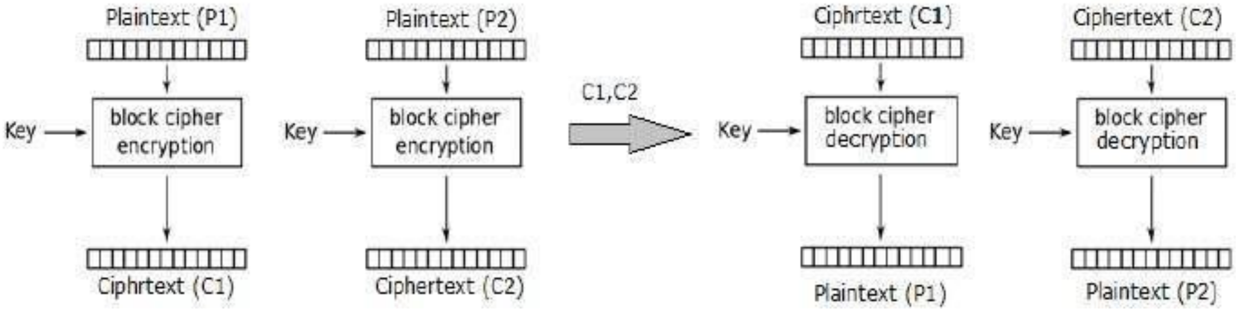


Figure 1.6 : Common usage of a block of Cipher text.

From the figure 1.6, it is evident that the plain text once is converted to a block of Cipher text by attaching a combination of unique keys for other key-based operations involving blocks of text.
A common example of the block Cipher is the Adhar number. This Adhar number is a unique 12-digit number that converts the information captured into numeric information. This Adhar number is used for buying a Car, Jewellery, or property wherein another unique number is generated.

1.4 Location of Encryption Devices

We have been discussing the various aspect of encryption techniques. In this section, we discuss the concept of the location of the Encryption device.

In simple parlance, location-based encryption devices refer to the process of developing means and mechanisms wherein the decryption process can only take place at a defined location. In other words, the decryption can take place at a particular location and or at a particular device only.

A common example of a location-based encryption device is the smartphone which all of us use. In this, we can enable the *finger-based or touch-based* recognition method.

In this method we first record the *touch-based* or *finger-based* to our smartphone and once enabled the phone can only be used by the user whose *finger or touch base* is registered.

In a similar manner, the biometric-based attendance recording system is also a location-based encryption device.

There are numerous examples of location-based encryption devices. Two of these are given figure 1.7 & 1.8:

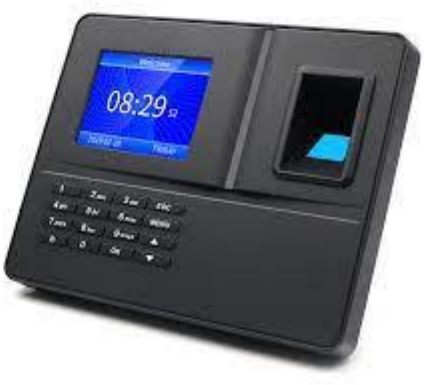


Figure 1.7 : Biometric attendance-based devices

Biometric attendance-based devices operate at a specific location only

Figure 1.8 : Debit and Credit Cards

Cards are applicable at selected POS terminals / ATMs etc.

Having understood the devices which we use on a day to day operations. It is again reiterated that the process of encryption that is protecting the object depends on various factors. For example, the above figures of the attendance marking system and the cards demonstrate one aspect of the encryption process. In other words, this is the process that deals with end-user Let us now discuss the other side of the encryption process. This deals with the aspects of the encryption process at the implementation level..

- **Link layer**

This is the layer that is the lowest layer in the TCP / IP suite. In essence, the link layer is responsible for connecting the device at the physical level to network architecture. The figure given figure 1.9 depicts the basic architecture of the link layer.

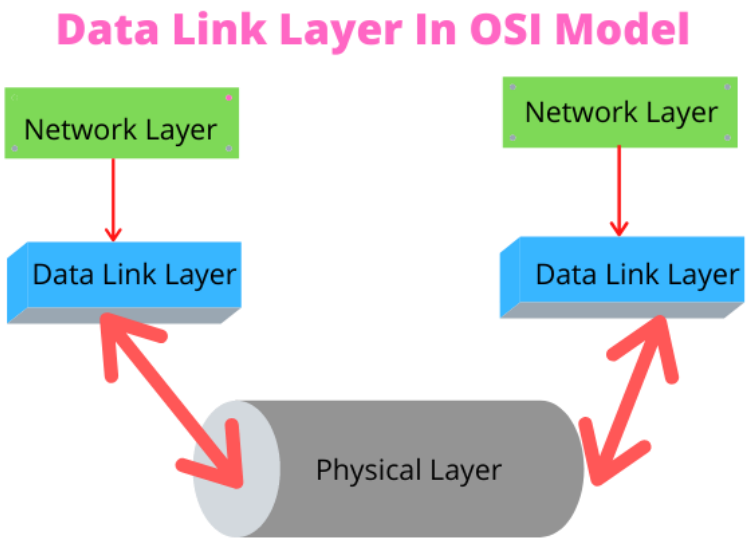


Figure 1.9 : Link layer

The link layer in essence connects the hardware to the physical component of the network architecture. We see that we have routers, nodes, computers, and other hardware components. Each of these is required to be encrypted as they are responsible for carrying the data which *can be exploited.* Hence we need to develop algorithms to protect the data.

For example, the component wired links are responsible for connecting the systems with one another. For example, connecting Hub with the internet service provider. For connecting one printer with the computer by means of a wire with another. All these transmit data and it is this which needs to be protected.

- **End-to-end encryption**

The term is used to ensure that the data which is transmitted from the sender to the receiver is encrypted from the perspectives of end to end. In other words, only the sender and the receiver are in the possession of the data that is they are the persons who can see the data. No one can see the data.

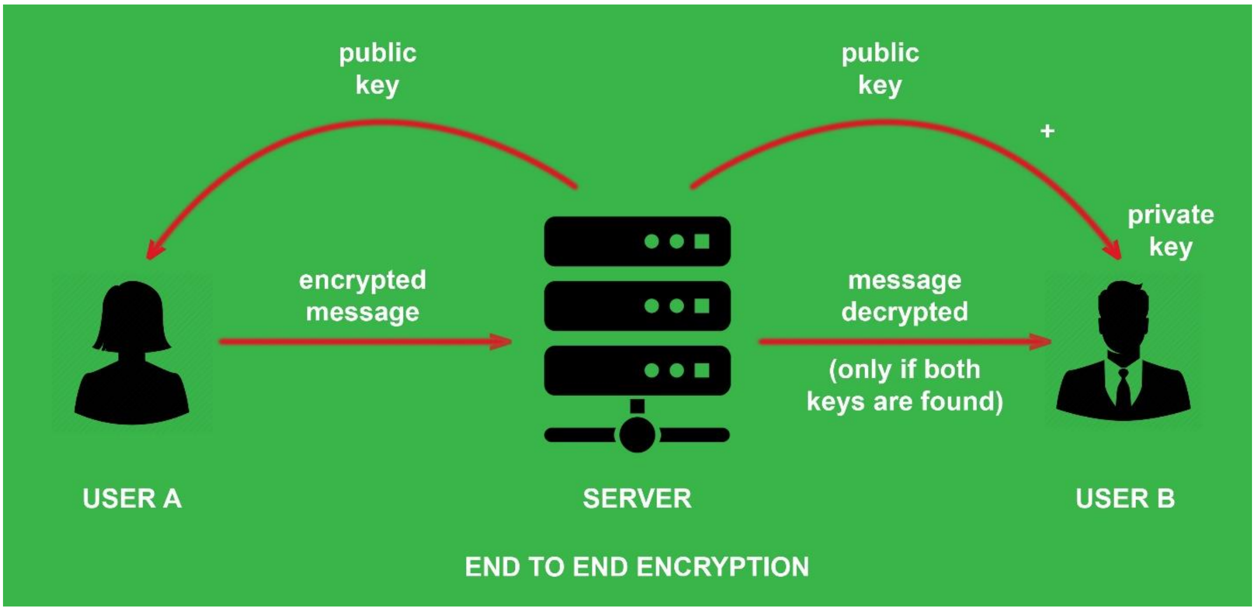


Figure 1.10 : End-to-end encryption

From the figure 1.10, it is evident that in the case of end-to-end encryption only the sender and the receiver are able to read the message. The message is encrypted in a manner wherein no unauthorized person can see the data which is being transmitted.

An example on end to end encryption is the WhatsApp messages which we send. They are end-to-end encrypted.

- **High security**

This is the process of encryption wherein the encryption controls are needed to be applied both at the link layer as well as at the data layer.

From the above discussion, it is evident that encryption is well thought strategic process for implementation. The prime reason why it is a well-thought process is the fact that encryption does not depend on a single perspective. It depends on several perspectives which include the architecture of the network, the architecture of the internet connection, the architecture of the software responsible for data transmission, the architecture of the components involved in the process of maintaining the systems, and the like.

In addition to all these facts, the other thing which is taken into the process of encryption methodology is the determination of the data which must be encrypted. In other words, there is an existence of criterion which needs to be taken into consideration from the perspective of whether it is required to be encrypted or not. That is whether the data is confidential or not. Refer to the figure 1.11.

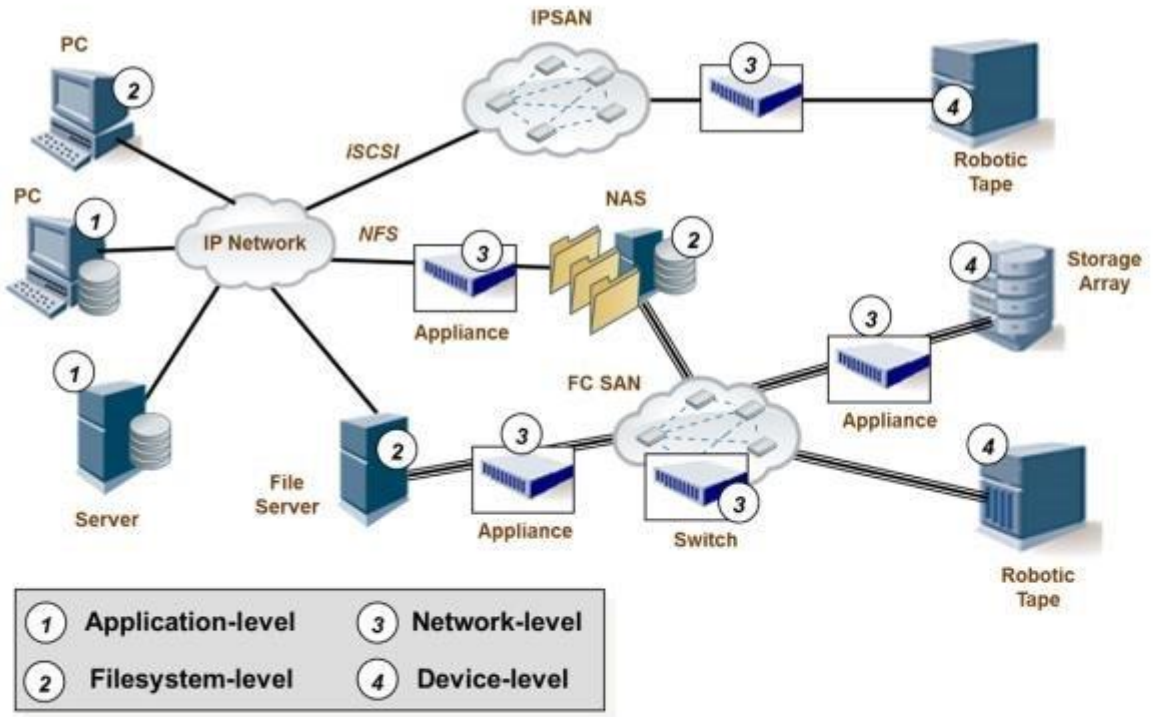


Figure 1.11 : High security

It is evident that we have 4 basic types of layers. *In reality, we may have a more complex and complicated network system.* Thus, it is seen that each of these layers is required to be protected. It may be through a simple encryption algorithm or it may be with a strong algorithm meaning that the process which is applied to the algorithm adopts a very complex and complicated algorithm that is very difficult to unscramble. For example, the use of random numbers generates numbers that are difficult to crack.

1.5 Key Distribution

From the above discussions, it is evident that the key functional area in an encryption process is the keys. It is these keys that provide the encrypted object a unique identifier that can be transmitted or used across several types of applications. For example, we have the credit card or the debit card number which is unique and with this unique number, the encrypted information is transmitted across several networks or POS.

This section deals with the Key distribution.

The term key distribution refers to the process of allocating or generating a key so that the intended purpose is achieved. For example, the Adhar number is the key and within this number, there are several informational points that are encrypted. The main purpose of the Adhar is to link every government service to this number so that misuse of information can be prevented. For example, we need Adhar's number to buy property. Here the Adhar number is linked to the property details so that only the genuine person can have the property in his / her name. In the absence of this linkage, many Benami property transactions that are fake property registration were prevented. Also, it is seen that two different keys are linked together. One of the key numbers comprising of the Adhar number while the other is the property details which are linked to the property key number.

There are basically 4 types of the key in a key distribution *viz.* symmetric, asymmetric, public, and private.

- Symmetric keys are those keys in which a single key is used to encrypt and decrypt the object. An example of a symmetric key is the Roll number of the student who is appearing in an exam
- Asymmetric keys are those keys that use two different keys. One key is used for encryption and the other key is used for decryption. An example of an asymmetric key is the captcha code which we use on websites for logging into the system. Here we use two different keys. One for entering the user id and the password and the captcha for decrypting the correctness of the user id and the password.

- Public keys are those keys that use encryption for encrypting the contents of an object. An example of public keys is the train number of a passenger train
- Private keys are those keys that are used to decrypt the information. An example of a private key is the PNR number of the passenger. Though these keys are interrelated. One cannot decipher the other if one is in possession of one key that is if we know the passenger number we cannot determine the train number and vice versa

- **Knowledge Check 1**

  Fill in the Blanks

  1. The full form of DES is __________________.
  2. The step-by-step instruction is known as ___________.
  3. During the transmission of an information object, one end is the __________ while the other is ___________.
  4. ____________ are the fundamental components of the encryption process.
  5. The full form of AES is _______________.

- **Outcome-Based Activity 1**

  Prepare an excel sheet wherein you identify the application areas which you use and which require the concept of Public and Private Keys. Also, provide the reason for classifying them as public or private keys. The report should be prepared in the following format as given underneath

Application Area	**Public Key**	**Private Key**	**Reasons for Public Key**	**Reason for Private Key**
E-Mail Services	User-ID	Password	It can be shared	It is shared with the -mail service provider only
Bank Locker	Locker - Number	Key number and access code	The locker number is shared with bank employees	Locker id and access code is shared with authorized bank employee only

1.6 Public Key cryptography principles

From the above discussions, it is evident that the entire process of encryption is a well-structured process. This means one needs to plan and develop a means and mechanism for ensuring that the information reaches the intended recipient. This means that the encryption method is so strong that hackers or unscrupulous persons are unable to crack the code and misuse the information. For example, with weak encryption hackers may steal credit card details.

Hence there are some principles that are followed for public key cryptography.

Worth mentioning is the fact that the principles have evolved over time wherein several attempts were made to develop a strong encryption system.

The basic steps that are followed include

- Distributing keys in a manner wherein the sender and the receiver share a key that has been distributed to them and the usage of the key distribution center. An example of this method is the use of OTP which is distributed through a registered phone number. In other words, the key is shared between the parties so that the intended work can proceed accordingly.
- The usage of a digital signature, Digital signature is a mechanism that is developed to encrypt the identity of the individual by means of generating an image and a key that is not shared with anyone except with the genuine user.

The figure given below depicts the basic concept of cryptography principles

1.7 Public Key cryptographic algorithms

It is discussed that the process of encryption is based on the concept of public and private keys. Also, the keys are generated by means of an algorithm. These algorithms are developed for the specific purposes

The following are two commonly used algorithms that are implemented in the process.

- RSA algorithm. This is based on the concept of the difficulty level of the numbers and uses a combination of prime numbers to generate the keys.
- ECC. This algorithm is based on the concept of geometrical curves and using these curves to arrive at a key that is fast and easy to use

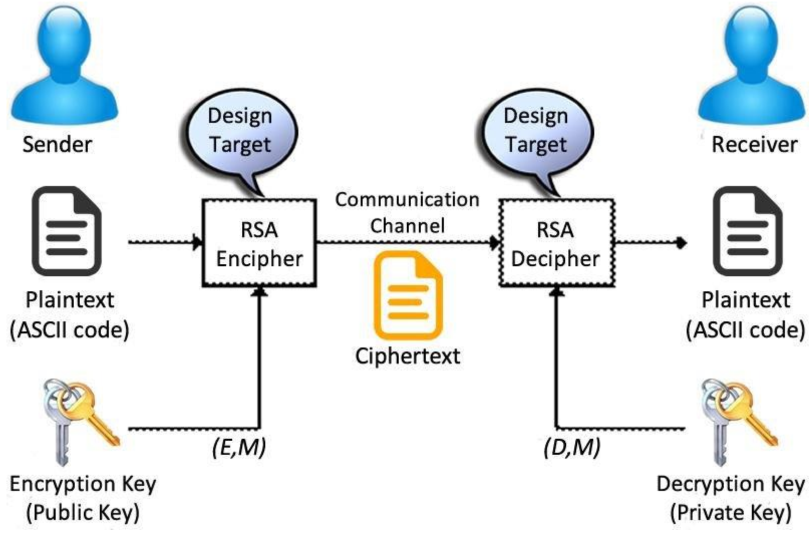
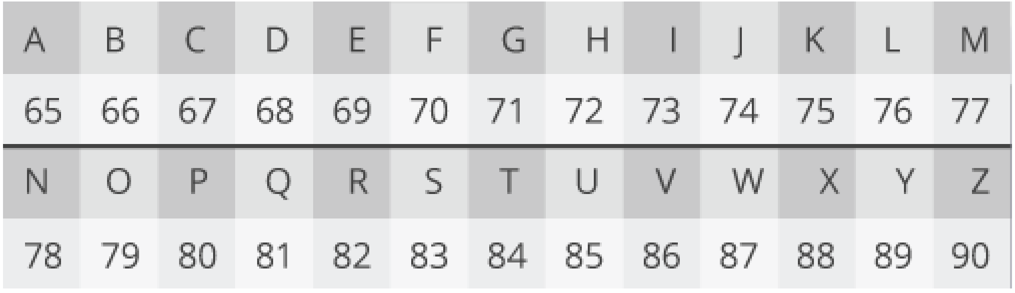


Figure 1.12 : Public Key cryptographic algorithms



A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

1.8 Public Key Distribution

In the encryption process, keys play an important role. The keys are required to be distributed so that the purpose of securing the informational object is achieved. Thus, it is a difficult task to distribute the public and private keys across the networks. Hence there is an imperative need for a mechanism for key distribution.

An example of a key distribution that we face daily is when we press forgot password option in our emails or otherwise. Here the public distribution key is the login or the user id while the private key which is used for decrypting the information is the reset password which is either mailed or any other verification mechanisms are used.

There are several ways in distributing the public key. It may be through public announcements, public key authorities, and the like.

The figures 1.13 & 1.14 depict the concepts and the methods used for public key distribution

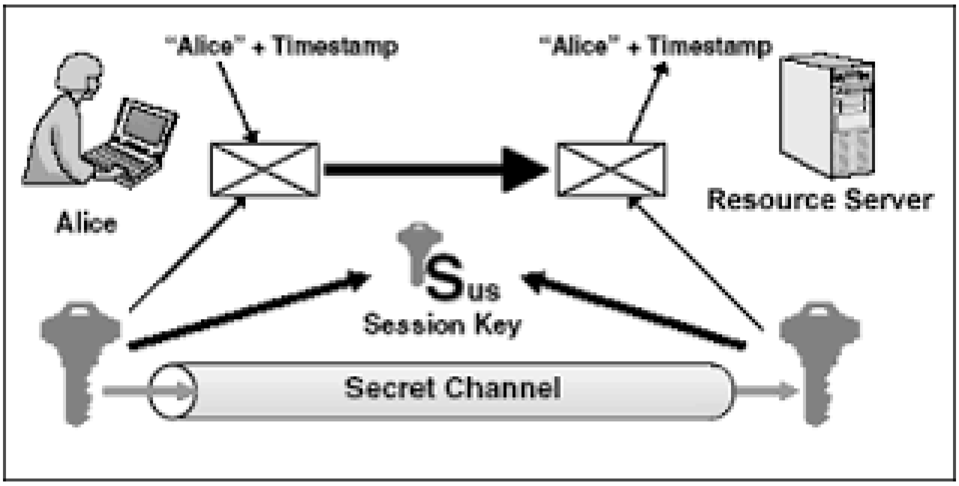


Figure 1.13 : Public Key Distribution

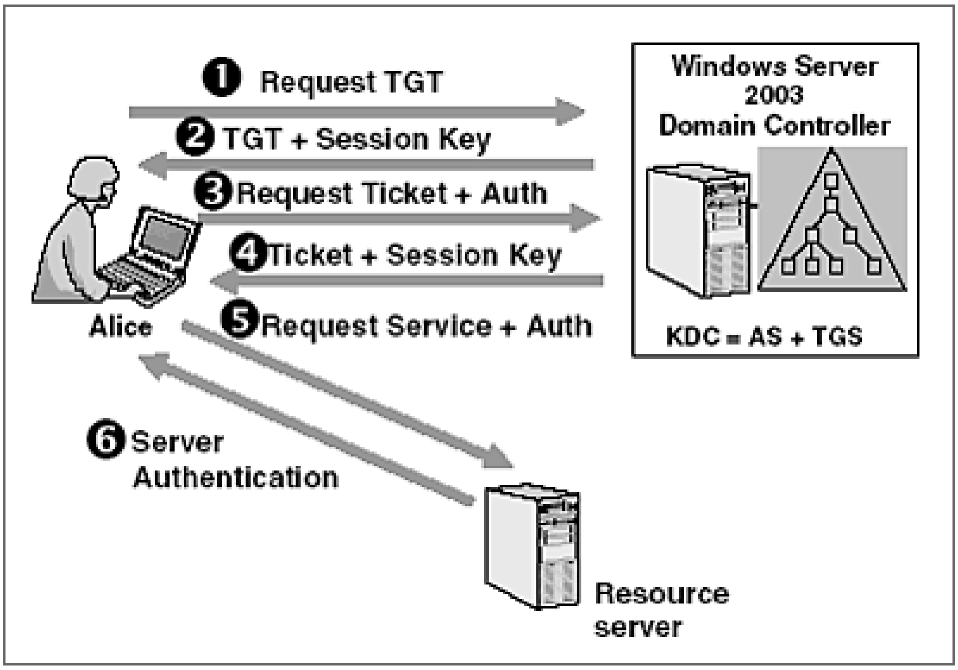


Figure 1.13 : Public Key Distribution

Let us take the different example of public key distribution(Figure 1.14).

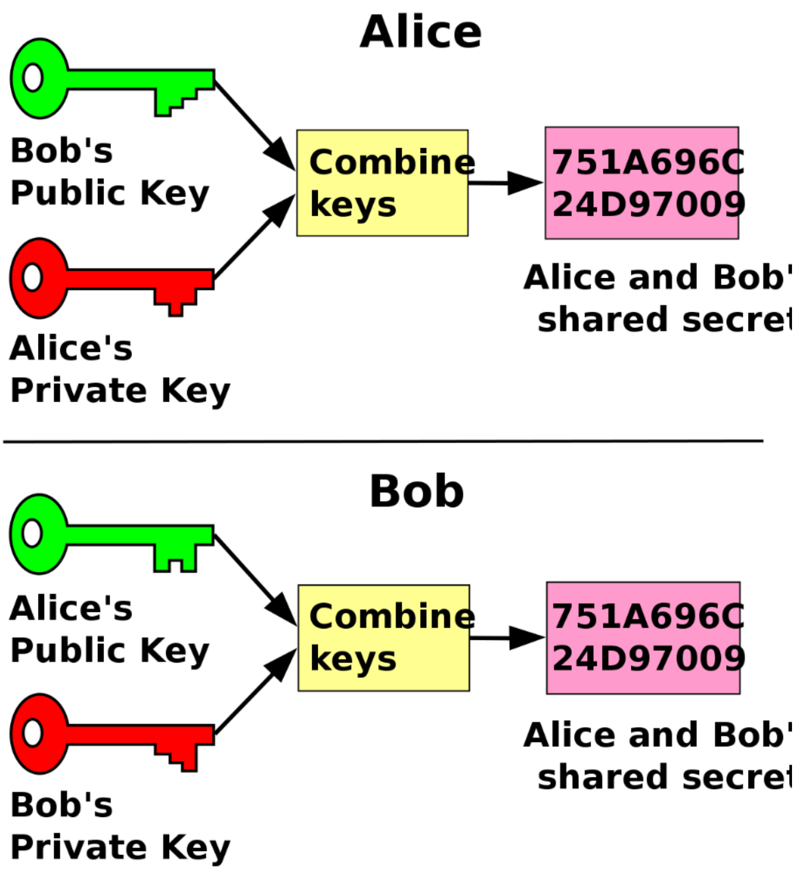


Figure 1.14 : Public Key Distribution Example

Worth re-iterating the fact that the process of encryption is complex and complicated as several aspects are needed to encrypt the data and decrypt the data. The above figure depicts one of the concepts of distributing public keys between two individuals. Here one party's public key is combined with the private key of another party to generate the encrypted data. This encrypted data is then shared and made available to both parties.

During the unscramble process the reverse process takes place and the intended party is able to see the data.

The following table depicts some of the techniques which are carried out for encrypting the data.

Parties	Primary Key	New Key
Bank	IFSC code 00371	9910200371
Customer	DOB 99-10-20	
Center Code	140	AA1140
Copy Code	A	
Serial Number	A1	

The above table depicts the encryption techniques which are commonly used by various agencies. Though they are easy to observe this is not the actual key that is transferred during the process of data transmission.

For example, the new key 9910200371 may further be encrypted as 0021311482

- **Knowledge Check 2**

State True or False

1. Encryption is used for the encoding purpose (True / False)
2. The algorithm is also known as a computer program (True / False)
3. The public key is also known as the network key (True / False)
4. Private keys are known as personal keys (True / False)
5. Algorithms are widely used in day-to-day operations (True / False)

- **Outcome-Based Activity 2**

Take a real-life scenario or an example say of railway reservation booking. Identify the parameters which require encryption. For example, the credit card details required personal keys for making the payment for the reservation.

Prepare the report in the following format.

Application Area	Field requiring Encryption
Railway Reservation through Netbanking	Credit / Debit card details for making Payment OPT Netbanking Password
Visiting a Defence Area	Driving License Adhar Card

1.9 Summary

- Today there is an urgent need for protecting the documents which are transmitted over the internet.
- In other words, the documents are required to be encrypted and decrypted.
- The first step in the process of encryption is the identification of the object which needs to be protected.
- In other words, one must first determine what is it that is needed to be protected by means of encryption.
- Unless and until this aspect is carried out the whole process is defeated.
- The process of encryption commences with the development of algorithms that convert the data into a form that is then transmitted or shared over the medium.
- Further, the development of the algorithm is also complex and complicated.
- This means that the algorithm must be constructed in a manner such that it can implement the encryption process in a manner that is strong and can be implemented easily.
- The main purpose is the ensure that they are able to protect the identity so that it reaches the intended person wherein he can decode the information.
- An example of encryption is the typing of a password on the computer screen wherein the keystrokes are depicted by means of an asterisk and at the backend, they are converted into encrypted form.
- It is to be noted that the process of encryption is complex and complicated as several aspects are needed to develop the encryption algorithm.
- For example, we may have a simple algorithm that adds subsequent characters to the original value or it may have a complex and complicated mechanism such as combining the nickname of the person with the date of birth of the person
- During the process of conversion, the concept of public and private keys is used

- The private key used is used for sharing the keys with the intended person only. For example, the sharing of OTP on the mobile while carrying out financial transactions
- The public key is used for sharing the information publically. For example, the email id of the user for sending emails. It is shared publically.

1.10 Self-Assessment Question

1. What is meant by encryption? Explain with examples
2. Explain with examples the concept of Block Ciphers.
3. What are public and private keys? Explain with examples
4. What are the various principles of public key cryptographic with examples
5. What is the need for encrypting the informational object? Explain with examples from day-to-day operations

1.11 References

- Rivest, R. L. (1994, December). The RC5 encryption algorithm. In International Workshop on Fast Software Encryption (pp. 86-96). Springer, Berlin, Heidelberg.
- Barrett, P. (1986, August). Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor. In Conference on the Theory and Application of Cryptographic Techniques (pp. 311-323). Springer, Berlin, Heidelberg.
- Mahajan, P., & Sachdeva, A. (2013). A study of encryption algorithms AES, DES, and RSA for security. Global Journal of Computer Science and Technology.
- Zhou, X., & Tang, X. (2011, August). Research and implementation of RSA algorithm for encryption and decryption. In Proceedings of 2011 6th international forum on strategic technology (Vol. 2, pp. 1118-1121). IEEE.
- Ateniese, G., Benson, K., & Hohenberger, S. (2009, April). Key-private proxy re-encryption. In Cryptographers' Track at the RSA Conference (pp. 279-294). Springer, Berlin, Heidelberg.

Unit : 2

Approaches of Message Authentication

Learning Outcomes

- Students will be able to understand the basic concepts involved in the process of sending messages through the encryption process.
- Students will be exposed to the basic concepts of the various security features and encryption involved during the process of encryption by using secure hash functions.
- Students will be able to understand the basic concepts of digital signatures, Kerberos, and Directory authentication services.
- Students will be able to understand the basic process of Email security and the means and mechanism involved in the encryption process.
- Students will be able to understand the concepts used in IP security including the architecture, authentication header, and the like.
- Students will be able to understand the concepts involved in the key management processes.

Structure

2.1 Introduction

In the previous unit, we covered the basic concepts of the encryption process. In particular, we covered the aspects pertaining to the process of encryption and the means and mechanism of the functioning of the encryption process using public and private keys that take place when the message is sent from the sender and the receiver. Also, we discussed that the encryption process does not work alone. This means that there exists a process that is responsible for the conversion of the encrypted process to restore it to the original form by means decryption process.

However, despite these adequate measures, there are certain points of consideration wherein the encryption process fails or the process of encryption needs to be strong enough to ensure that the message is not exploited.

In other words, the focus shifts to the process of various measures of encryption techniques. This unit deals with various measures which are deployed in the process of encrypting the messages.

2.2 Secure Hash Functions (SHA-512, MD5) and HMAC

Before we dwell further, let us now discuss the concept of the hash function. It is evident that the process of encryption deals with the conversion of text from the sender into a form that cannot be read normally by any individual. Also, when this formatted text reaches the receiver, it is reconverted into an original form so that the intended person can read the message.

Now we move to the process of conversion of the message. This is achieved by means of the hash function. Worth mentioning is the fact that a hash function is widely used in the encryption process.

What exactly is a hash function and what it does do to the text or the message, we will now discuss.

In simple parlance, a hash function is a technique that makes use of a mathematical function where a numerical input is used to generate another numerical value that is of a fixed length. In other words, if the input value says 5 digits, then the output value may be 16 digits or so.

The output value which is the generated value of fixed length is known as the message digest or the hash value.

Refer to the figure 2.1 to understand the functioning of the hash function

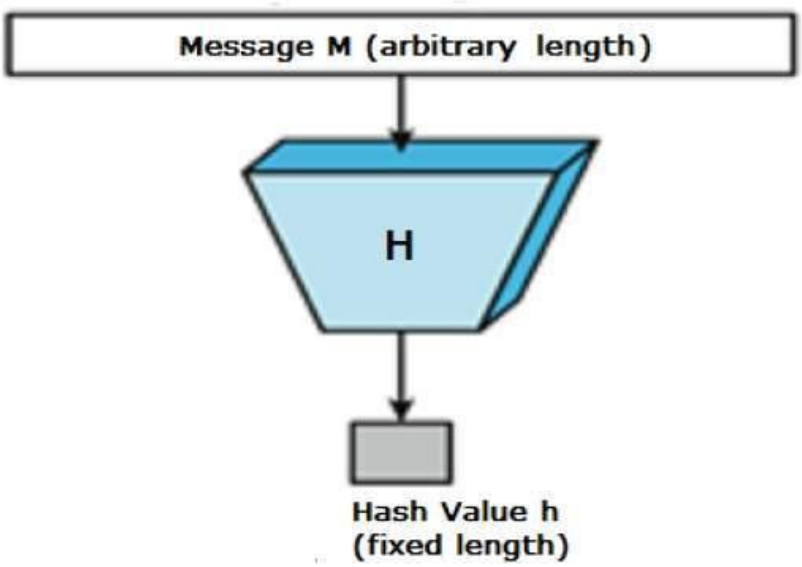


Figure 2.1 : Functioning of the hash function

It is seen that the message M is of arbitrary length and is subjected to a mathematical function which is known as the hash function and is represented in the figure as H this function then generates the hash value which is of fixed length.

Refer to another figure which is more explicit and tries to demonstrate the means and mechanism of the process of hash function wherein the message is in the form of text.

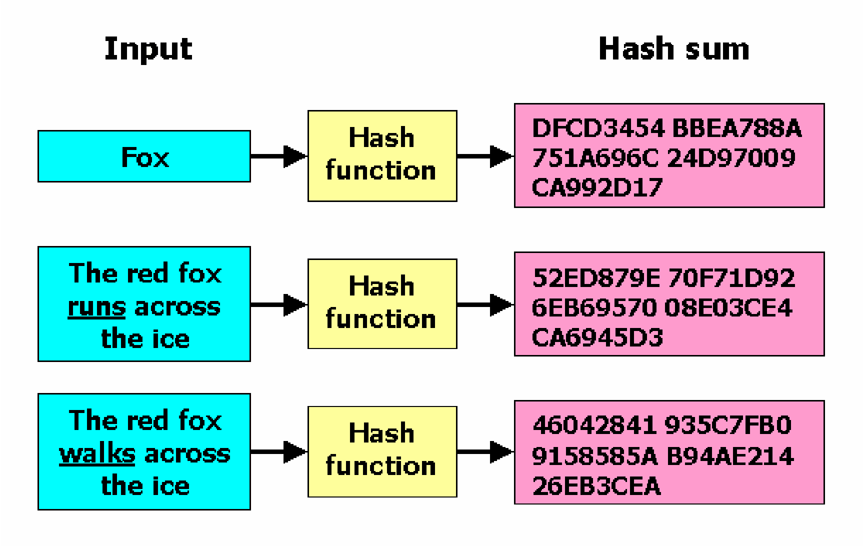

Input
Hash sum
Fox
Hash function
DFCD3454 BBEA788A 751A696C 24D97009 CA992D17
The red fox runs across the ice
Hash function
52ED879E 70F71D92 6EB69570 08E03CE4 CA6945D3
The red fox walks across the ice
Hash function
46042841 935C7FB0 9158585A B94AE214 26EB3CEA

Figure 2.2 : Process of hash function

In the figure 2.2, it is seen that the message is in the form of sentences in the English language which is converted into a numeric form (as the hash function works on numeric values only). This numeric form is obtained by converting the text into bits and bytes which is the language as understood by the computer. It is these bits and bytes that form an input to the hash function and in turn, it is converted to a fixed-length hash value.

Having understood the basic concept of the hash function, let us now dwell on the concept of a secure hash algorithm.

In simple parlance, the Secure Hash Algorithm (SHA) is a group or a family of functions that are designed and developed to work on the data so that it can be secured. It functions by transforming the available data into another form comprising bits and bytes. It is this transformed data that forms an input to which the hash algorithm is applied to generate a fixed length value. Worth mentioning is the fact that the algorithms are designed to function in a one-way mechanism. This means that once the hash value is obtained it is impossible to restore them to their original form.

The following is an example of a simple process of converting a string into a hash value by means of an algorithm

Example -1

Input: hello world

Output: 2dbe9d35c94ecfb415dbe95f307b9ce61ee836ed

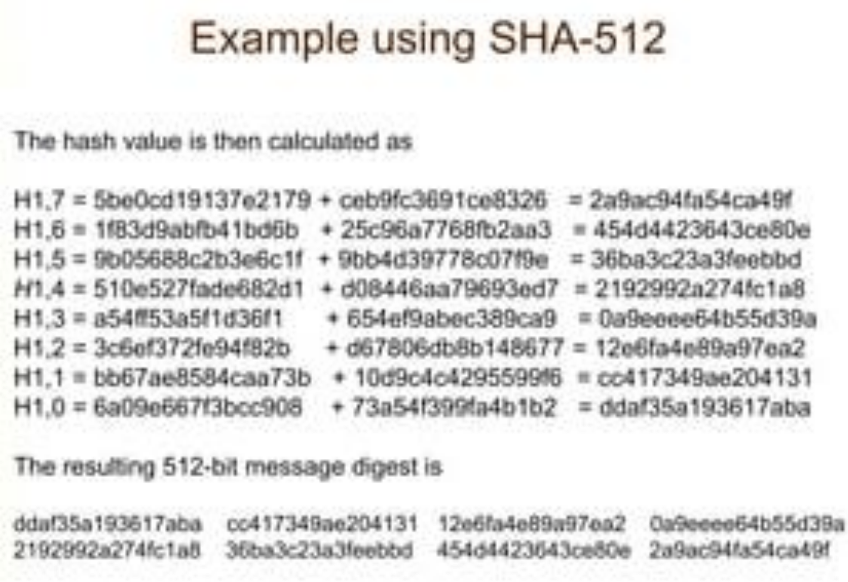
Here it is seen that the input text is hello world. It is converted into a hash function which translates the text into the form of bits and bytes and then the algorithm is applied to generate the final output

SHA-512 Algorithm

We have been discussing at several places that the basic function of generating the final output is done by means of a two-way process. One is the hash function which converts the original message into a form comprising bits and bytes. This input form is then subjected to an algorithm process which then generates the final fixed-length output.

In this connection, it is also stated that in order to provide the highest security, the degree and the depth of the output are provided by the algorithm.

The SHA-512 is one such algorithm. The term SHA refers to the secure Hash Algorithm which is used to transform any text or number irrespective of any length to an output that produces a length of 512 bytes which is 64 bits. This type of algorithm is mainly used in email addresses, password hashing, and digital record verification.



Example using SHA-512

The hash value is then calculated as

```
H1,7 = 5be0cd19137e2179 + ceb9fc3691ce8326   = 2a9ac94fa54ca49f
H1,6 = 1f83d9abfb41bd6b  + 25c96a7768fb2aa3   = 454d4423643ce80e
H1,5 = 9b05688c2b3e6c1f  + 9bb4d39778c07f9e   = 36ba3c23a3feebbd
H1,4 = 510e527fade682d1  + d08446aa79693ed7   = 2192992a274fc1a8
H1,3 = a54ff53a5f1d36f1    + 654ef9abec389ca9   = 0a9eeee64b55d39a
H1,2 = 3c6ef372fe94f82b    + d67806db8b148677 = 12e6fa4e89a97ea2
H1,1 = bb67ae8584caa73b   + 10d9c4c4295599f6   = cc417349ae204131
H1,0 = 6a09e667f3bcc908    + 73a54f399fa4b1b2   = ddaf35a193617aba
```

The resulting 512-bit message digest is

```
ddaf35a193617aba   cc417349ae204131   12e6fa4e89a97ea2   0a9eeee64b55d39a
2192992a274fc1a8   36ba3c23a3feebbd   454d4423643ce80e   2a9ac94fa54ca49f
```

Figure 2.3 : SHA-512 Algorithm

From the figure 2.3, it is observed that the final output is 512 bits

MD5 hash functions

The MD5 is also known as Message Digest Method 5 which is a cryptographic algorithm for hashing and is used for generating 128 message digest of a string of any length. It represents the digests as 32 Hexa decimal numbers and is used in the verification of the digital signature.

The figure 2.4 depicts the concept of MD5 hash functions

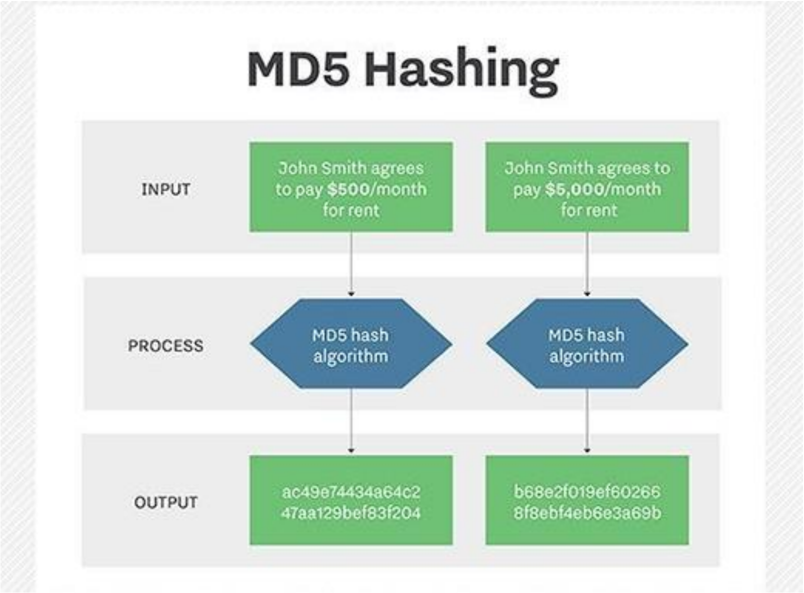

MD5 Hashing
INPUT
John Smith agrees to pay $500/month for rent
John Smith agrees to pay $5,000/month for rent
PROCESS
MD5 hash algorithm
MD5 hash algorithm
OUTPUT
ac49e74434a64c2 47aa129bef83f204
b68e2f019ef60266 8f8ebf4eb6e3a69b

Figure 2.4 : MD5 Hashing Algorithm

HMAC

The full form of HMAC is a Hash-based message authentication code. This is a technique that uses a key that is cryptographic. This ensures that the server and the client are able to read the contents of the message as they are in the possession of private keys for a specific client and the server.

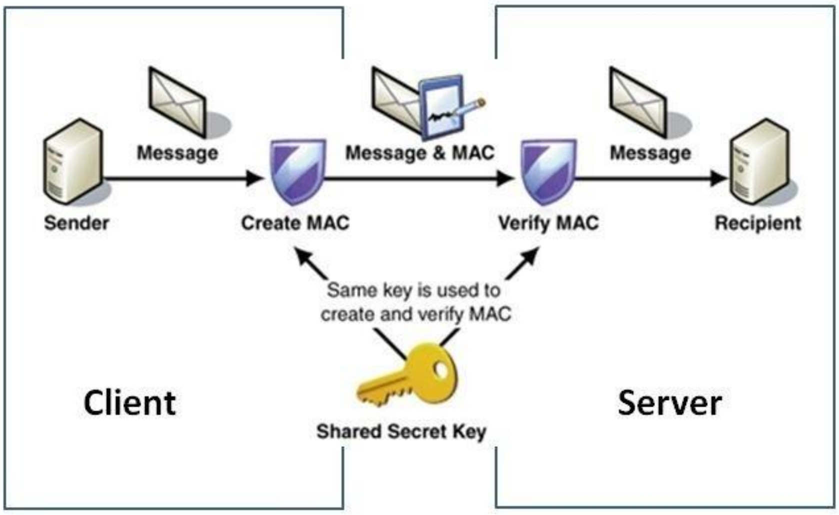
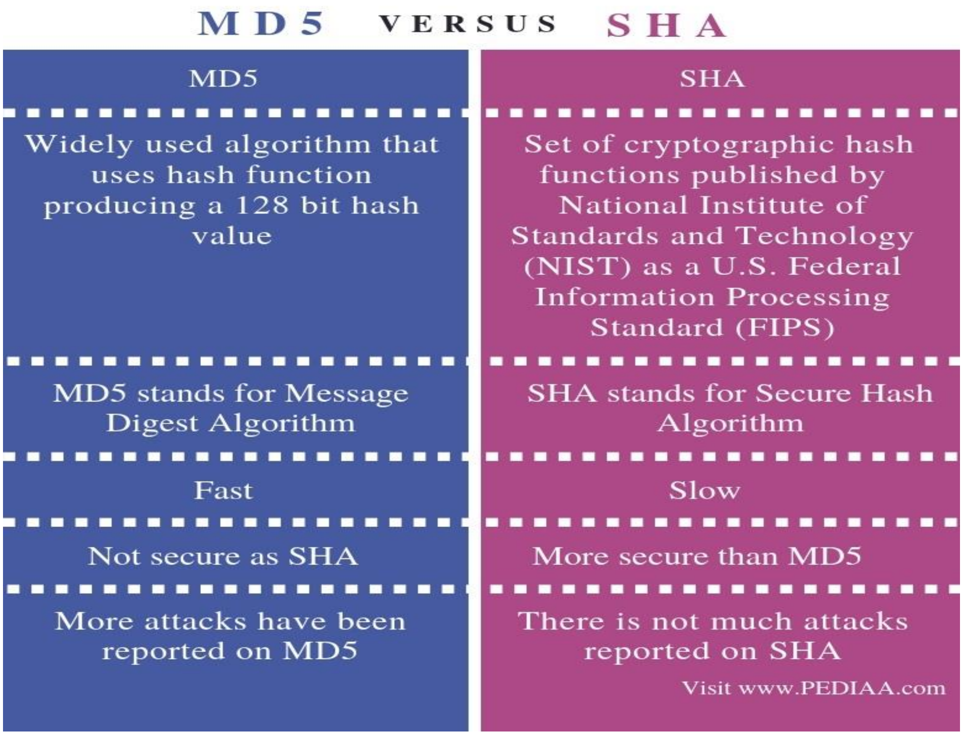


Figure 2.5 : HMAC

From the figure 2.5, it is observed that both the sender and the receiver have a shared secret key. The sender of the message creates the MAC along with the key which is shared with the client. This key is verified at the client's end wherein the contents are verified at the client's end.

Difference between SHA-512, MD5 and HMAC

The following figure 2.6 dipicts the differences between the SHA and MD5



MD5 VERSUS SHA

MD5	SHA
Widely used algorithm that uses hash function producing a 128 bit hash value	Set of cryptographic hash functions published by National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS)
MD5 stands for Message Digest Algorithm	SHA stands for Secure Hash Algorithm
Fast	Slow
Not secure as SHA	More secure than MD5
More attacks have been reported on MD5	There is not much attacks reported on SHA

Visit www.PEDIAA.com

Figure 2.6 : Difference between MD5 & SHA-512 Algorithm

It is seen that SHA-512 is more secure than the MD5 hash function. This is due to the fact that the basic structure is comprised of 512 bytes of encoding which means that an additional layer of security is applied. Also, due to the length of the bytes, it is slow as compared to the MD5 algorithm which is fast enough yet it fails to provide the needed security.

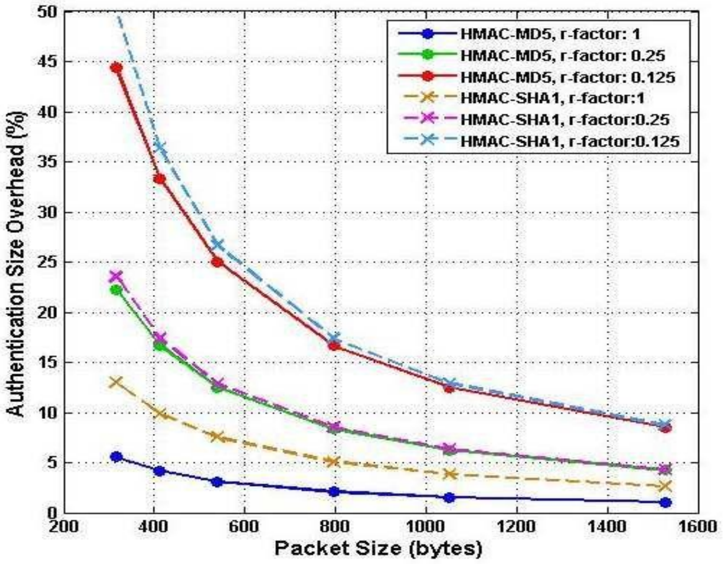


Figure 2.7 : MD5 & SHA-512 Algorithm graph

The above figure 2.7 provides a glimpse of the comparison between the MD5, SHA, and HMAC. It is seen that as the packet size is small the HMAC provides the greatest degree of authentication as compared to MD5 and the SHA. However, as the packet size is increased the degree of authentication keeps on decreasing. But HMAC is always ahead of the other two techniques of encryption.

2.3 Digital Signatures, Kerberos, X.509 Directory Authentication Service

In the previous section, we discussed the various aspects of encryption algorithms. In this section, we cover the aspects pertaining to digital signatures, Kerberos, and the X509 Directory assistance service.

The concept of a digital signature

In simple parlance, the term digital signature is a mechanism that is used to identify, verify, validate and authenticate digital documents. In other words, it is just a signature that we put down on our cheque except that the process involves digital signing. In other words, just as our signature is recorded in the bank and that recorded signature is used for validation and authentication here also in the case of digital signature, we have the same concept. The concept is in terms of the key which is known to the owner of the digital signature as well as to the owner who keeps the digital signature that is the server.

The concept of digital signature came into existence so that the problems of transmitting confidential information if it is tampered with or used inappropriately can be verified and authenticated.

The definition of digital signature in technical terms is a mathematical technique that is used for validating the authenticity of the document.

Also depending on the purpose, there are different kinds of digital signatures.

Figure 2.8 : Digital signature

The figure 2.8 depicted an example of one form of the digital signature the figure 2.9 depicts the process in technical terms of creating a digital signature.

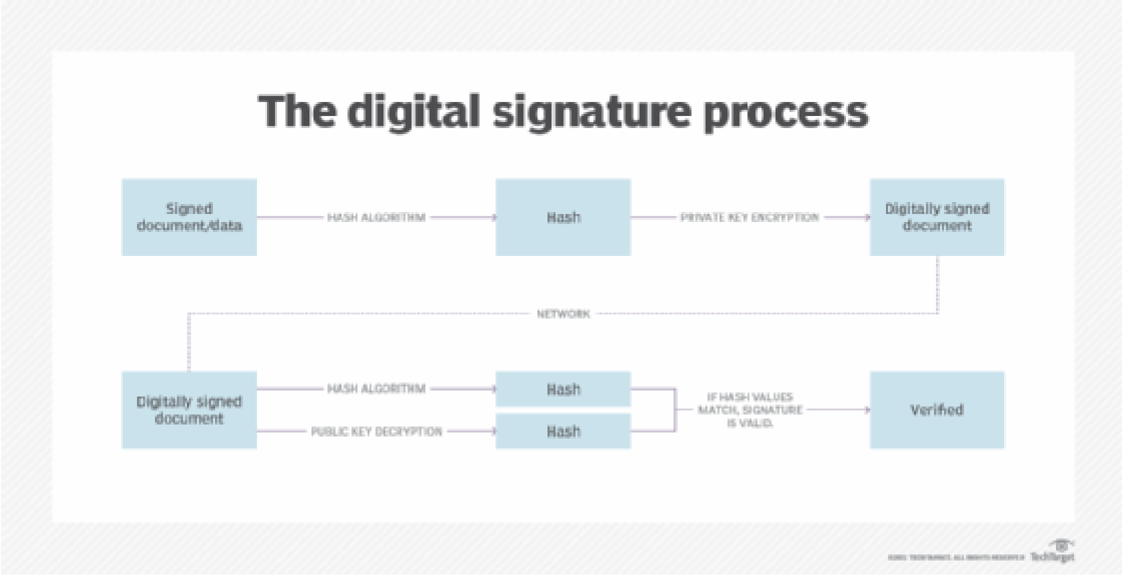


Figure 2.9 : Digital signature Process

The concept of Kerberos

During the process of data transmission, as mentioned several aspects are taken into consideration. For example, we have communication over a network wherein different transmission protocols are being used and which may be secured or not or we may have nodes involved in the network but some of them are trusted nodes or a particular network or not. For example, when we do net banking operations, we may invoke the request from our network in our office. This is a trusted and secure network meaning that whatever we are doing we are assured that the data is safe. However, when we move to eh banking network, this may not be trusted or it may be secured. This means that our transmission details can be compromised meaning that they can be leaked to unintended users.

Kerberos is a network security protocol that is designed to deal with unsecured nodes of the network when the data is transmitted between secured networks. Let us take an example, suppose we are transmitting money to our bank from our client, a machine in our office to another bank that is outside the country, and the network of this bank is secured. However, in order to transfer the money, it has to pass through the network of several countries and these may not be secured and may not be trusted. Thus, Kerberos will verify all these networks which are untrusted and insecure pertaining to the authenticity and if all the nodes and networks are correctly that is secured and trusted then only the transmission will happen otherwise it will decline the transmission or will alert the user about the potential risk over an unsecured transmission.

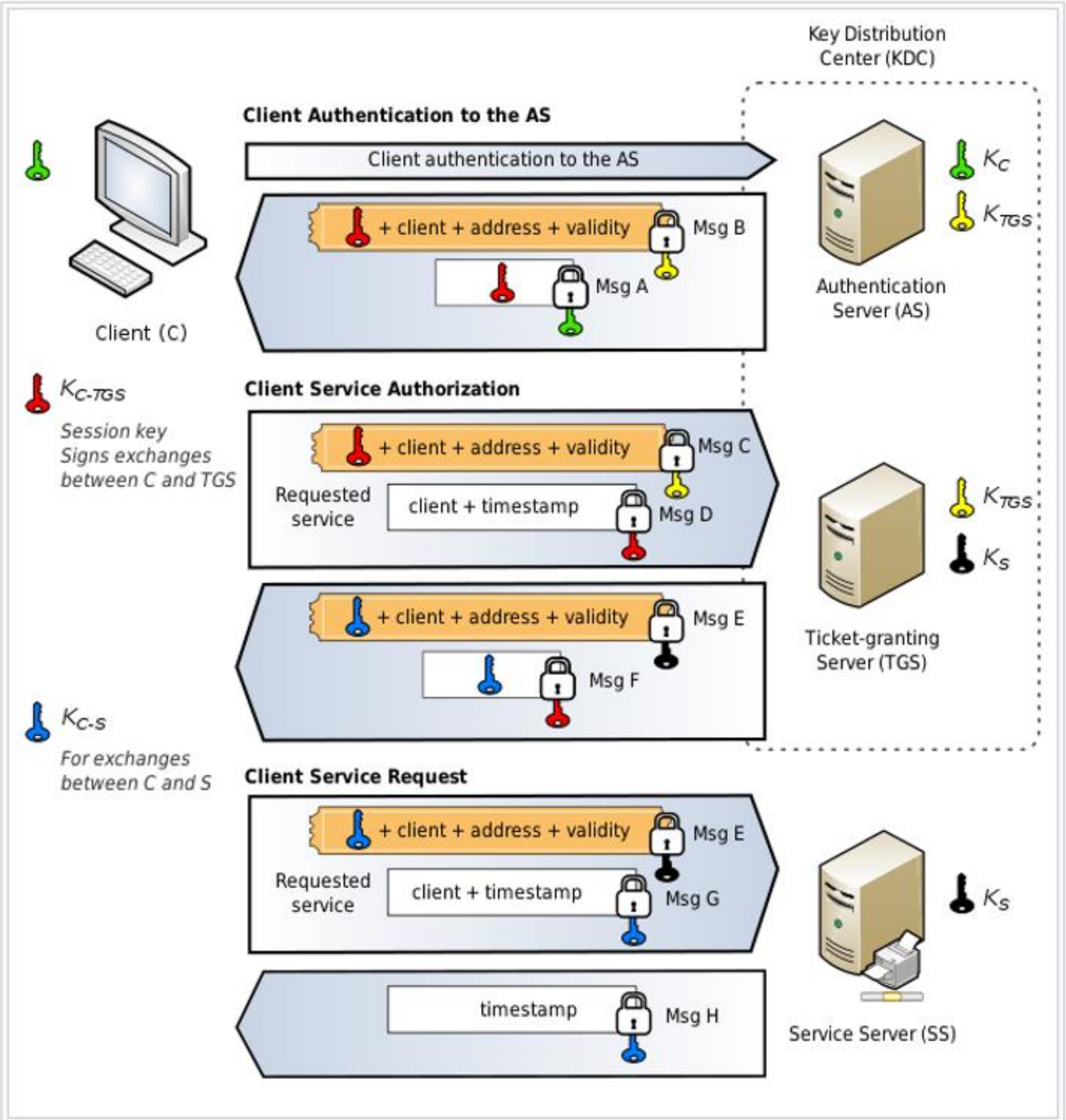

Key Distribution Center (KDC)
Client Authentication to the AS
Client authentication to the AS
+ client + address + validity
Msg B
Msg A
K_C
K_{TGS}
Authentication Server (AS)
Client (C)
$K_{C\text{-}TGS}$
Session key
Signs exchanges between C and TGS
Client Service Authorization
+ client + address + validity
Msg C
Requested service
client + timestamp
Msg D
K_{TGS}
K_S
+ client + address + validity
Msg E
Msg F
Ticket-granting Server (TGS)
$K_{C\text{-}S}$
For exchanges between C and S
Client Service Request
+ client + address + validity
Msg E
Requested service
client + timestamp
Msg G
K_S
timestamp
Msg H
Service Server (SS)

Figure 2.10 : The concept of Kerberos

From the figure 2.10, it is seen that we have an authentication server that is used for validating the authenticity of the network. If it is correct then it is referred to onward processing otherwise it is held back.

X.509 Directory Authentication Service

It is mentioned in several places that the encryption process is an important part of the data and information transmission process. This is due to the fact that there have been instances wherein the data or the information has been compromised. In other words, crucial, confidential, and important information has been stolen and has been deployed for an unintended purpose. Further, there have been several attempts to develop and deploy various measures for adopting authorized services.

X509 directory authentication is one such service that is used in the verification of digital signatures.

X.509 Authentication Service

A common framework for handling digital certificates and public-key cryptography is the X.509 authentication service. It is frequently used to authenticate individuals and devices and protect communications over networks, such the internet. The main features of the X.509 authentication service are as follows:

1. Electronic Certifications
    - Certificate Structure: X.509 certificates provide the certificate holder's public key as well as details about them and the Certificate Authority (CA) that issued them.
    - Fields for Certificates: The subject (entity being authenticated), the issuer (CA), the subject's public key, a serial number, and the certificate's validity term are common fields in X.509 certificates. The function of a CA is to issue, revoke, and administer digital certificates. It is a trusted entity. Prior to granting certificates, it confirms the identity of the entities.
    - Certificate Chain: In a hierarchical system, certificates are often granted by a root CA to intermediate CAs, who then issue certificates to end users or devices.

2. Infrastructure with Public Keys (PKI)
    - PKI Elements: PKI consists of the CA, repositories that store and disperse certificates and Certificate Revocation Lists (CRLs), and registration authorities (RAs) that confirm identification.
    - Revocation of Certificates: If a certificate is compromised or deemed unnecessary, it may be revoked prior to its expiration date. Revocation details are made available through the Online Certificate Status Protocol (OCSP) or CRLs.

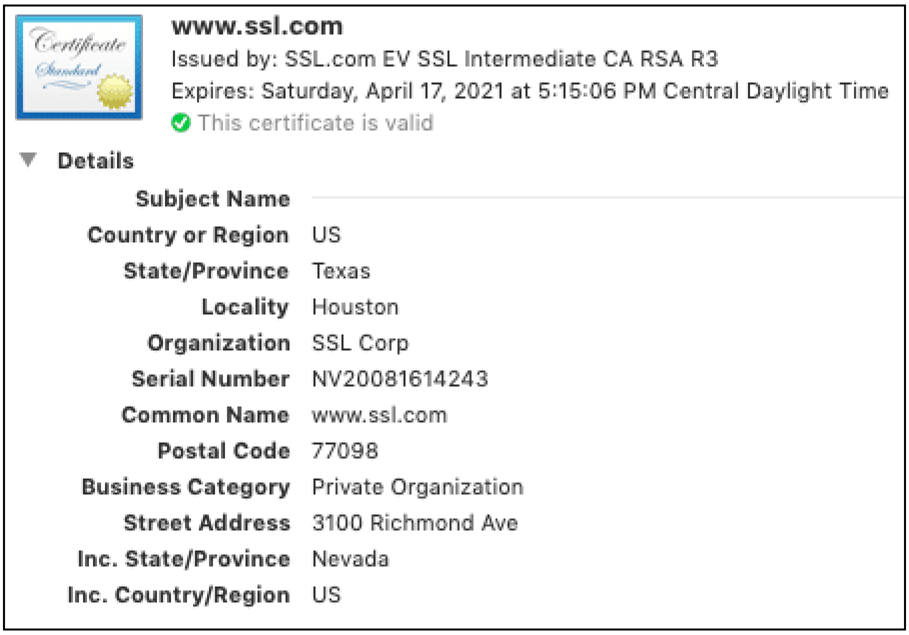
3. Procedure for Authentication
    - Mutual Authentication: To guarantee a safe connection, both participants in a communication can authenticate one another using their digital certificates.
    - TLS/SSL: To secure web communications, X.509 certificates are extensively used in the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols.

4. X.509 Authentication Uses
    - Safe Websites: X.509 certificates are used by HTTPS to encrypt web traffic.
    - Email Security: X.509 certificates are used by protocols such as S/MIME to secure email conversations.
    - Virtual Private Networks (VPNs): To authenticate users and secure connections, VPNs employ X.509 certificates.
    - Digital Signatures: To ensure authenticity and integrity, software and documents are signed using X.509 certificates.

5. Advantages of X.509 Verification
    - Robust Security: Utilizing public-key cryptography, it offers robust encryption and authentication.
    - Scalability: Fits well with hierarchical CA structures in large-scale deployments.
      Interoperability: Broadly compatible with a range of platforms and applications

It is evident that a well-organized and structured framework for authentication is available across the world by a body ITU which is responsible for ensuring the authenticity of digital signatures by means of securing the public and the private key of the issuer and the keeper.

This concept is analogous to our passport services wherein the details including the passport number, place of issue, and the like is stored o kept by the government and the holder of the passport is provided with the passport number for executing the authenticity of the individual and the passport. In other words, for determining whether the passport is genuine or fake.
Refer to the figure given below. The figure depicts the application of the X509 directory of services and is similar to what we have been discussing.



www.ssl.com

Issued by: SSL.com EV SSL Intermediate CA RSA R3

Expires: Saturday, April 17, 2021 at 5:15:06 PM Central Daylight Time

✓ This certificate is valid

▼ Details

Subject Name	
Country or Region	US
State/Province	Texas
Locality	Houston
Organization	SSL Corp
Serial Number	NV20081614243
Common Name	www.ssl.com
Postal Code	77098
Business Category	Private Organization
Street Address	3100 Richmond Ave
Inc. State/Province	Nevada
Inc. Country/Region	US

Figure 2.11 : X509 directory services

From the figure 2.11, it is evident that there is a central repository wherein the certificate is kept. In other words, there is the owner of the certificate and which takes into consideration the management of the certificate which means the date of issue, who has issued the certificate the validity period of the certificate, and the like.

All this is possible by using X509 directory services.

2.4 Email Security: Pretty Good Privacy (PGP)

Email, since it is transmitted over the internet is also subjected to various security protocols. In other words, it also needs to be protected and secured. This means that the contents of the mail are of such a nature that it lands up in the hands of the unscrupulous user it may put into trouble.

Pretty good Privacy or PGP in short is one such technique that is used for encrypting e-mail.

In simple parlance, PGP is a program that is used for encrypting emails with respect to privacy, authentication, digital signature, and other associated activities which are carried out during the transmission of email messages across the internet. This also includes the aspects such as the encryption of files, disks, and images. Also, it takes into consideration the aspects pertaining to files that carry the virus and other forms of malicious software which can be attached to the mail.

Refer to the figure 2.12. The figure depicts the means and the mechanism which are taken into consideration by the PGP.

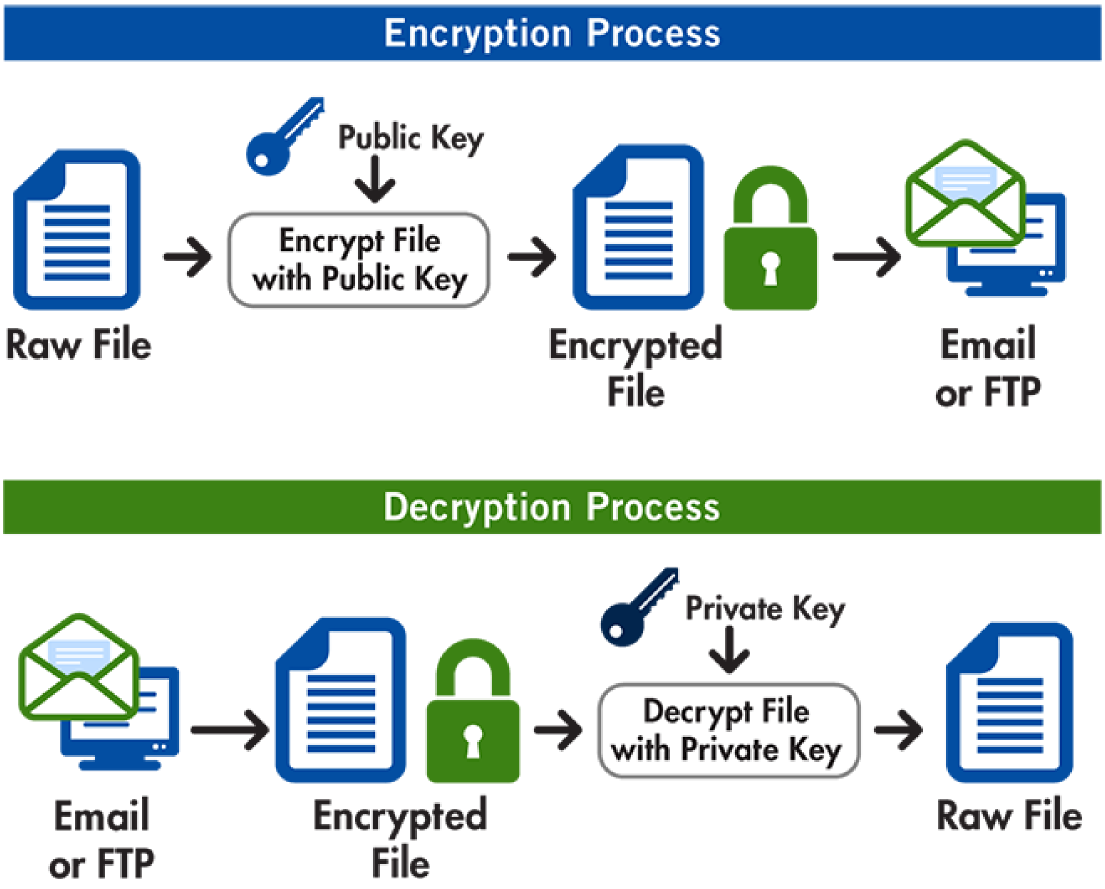


Figure 2.12 : Email Security: Pretty Good Privacy (PGP)

The figure is self-explanatory. The raw file is encrypted with the public key and it is this encrypted file that is transmitted over the internet through email or the FTP. Worth mentioning is the fact that the term FTP stands for File Transfer Protocol and is used for transferring the file in an encrypted format from one node to the other node. Once the file is received by the receiver, an encrypted key is needed to unscramble the file so that the mail can be read. In other words, the FTP ensures that the file uses an encrypted password or key for sending to the receiver also when it is received by the receiver, the same key is needed for unscrambling the same that is for reading purposes only.

2.5 IP Security: Overview, IP Security Architecture

From the above discussions, it is evident that security forms a core aspect of the information transmitted or shared over the internet. This means that the information must be protected at any cost. In other words, it must be ensured that the information is received by the intended persons only and also it is sent by the authorized persons only.

In order to achieve this objective a well-structured framework is constructed. This structure deals with the security aspect only and is known as IP security architecture. Further, due to large applications and the transmission of information over the internet, there is no foolproof method for developing the security system architecture.

For example, we have to secure the application, or we have to secure the firewall, or the routers which transmit the internet communication from the service provider is also needed to be secured. Hence the need for an architecture that will serve the objective of the organization.

Having understood this basic concept, let us try to understand one such architecture with the help of the figures 2.13

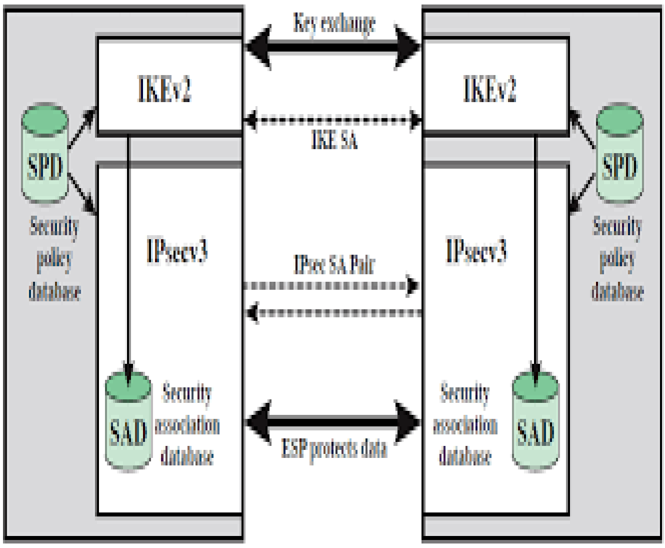
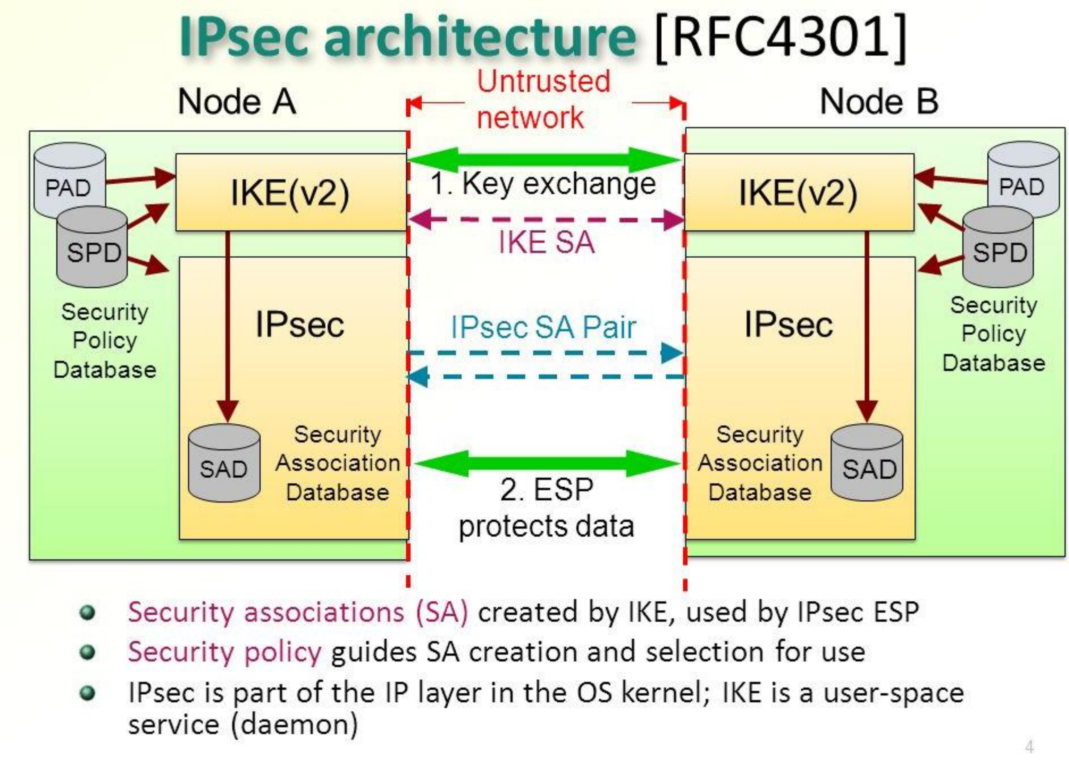


Figure 2.13 : IP Security Architecture

This figure 2.13 deals with the aspects of security in terms of the security policy and the security policy deals with the various aspects of implementing the same. The security policy document covers aspects such as the various controls which are needed to be deployed at the various nodes and touchpoints such as biometric sensors and the like. The document provided a vivid description in terms of defining passwords for various devices, controls, and other forms of security at crucial points including the access permissions to the stakeholders. It is the most crucial document.

The diagram 2.14 depicts another aspect of the security architecture. This architecture is described in terms of the technical aspect of the various devices which are connected over the network.

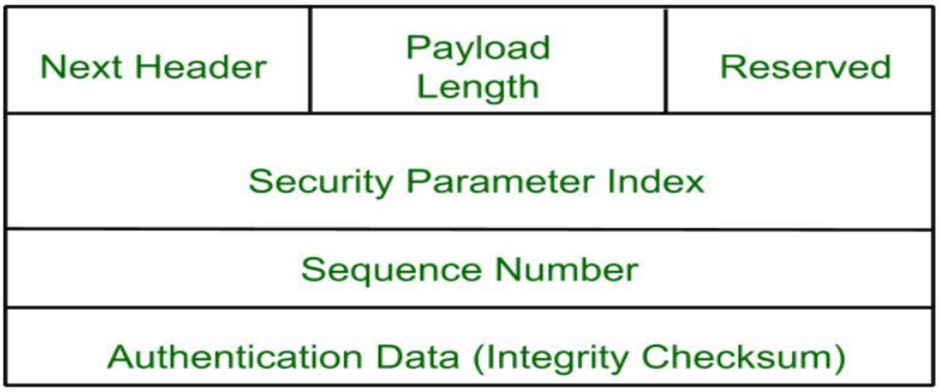


- Security associations (SA) created by IKE, used by IPsec ESP
- Security policy guides SA creation and selection for use
- IPsec is part of the IP layer in the OS kernel; IKE is a user-space service (daemon)

Figure 2.14 : Email Security: Pretty Good Privacy (PGP)

In the figure, it is seen that the security database is responsible for keeping the contents as defined in the security policy document.

The figure 2.15 depicts the security controls deployed at the packet level.



Next Header	Payload Length	Reserved
Security Parameter Index		
Sequence Number		
Authentication Data (Integrity Checksum)		

Figure 2.15 : Security controls

From the figure, it is seen that various controls are deployed at the packet level including the header, the payload length, and the like. It also takes into consideration the checksum integrity constraints. Worth mentioning is the fact that this is a mechanism that is deployed to ensure that the contents of the data are not tampered with in terms of extracting partial information and the like.

- Knowledge Check 1

  Fill in the Blanks.

  1 The full form of PGP is _______________.

  2 The full form of SHA is ______________.

  3 The full form of HMAC is _____________.

  4 A digital signature is used for _____________ the documents.

  5 IP security is a _________________.

- **Outcome-Based Activity 1**

Prepare a flowchart for converting a message into an encrypted format.

2.6 Authentication Header

In the previous section, we have covered the various aspect of data security. We have also covered the aspects pertaining to the packets which are transmitted in the packet-switching network. The authentication header is a protocol that applies to the packets which are transmitted over the net.

In particular, this protocol deals with the various aspects of the packet including the origin, the next link to the packet, and the like. In other words, it provides the complete details of the said packet.

Refer to the figure 2.16

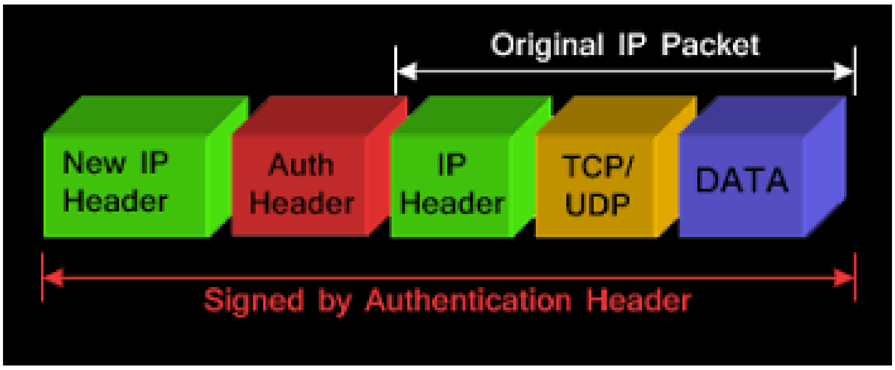


Figure 2.16 : Authentication Header

From the figure, it is evident that the complete information which is authentic is provided by the authentic header. This includes the origin and destination of the packet and the data it contains. Worth mentioning that the authentication header does not provide the details of the data *it provides information for the packet only.*

2.6.1 Encapsulating Security Payload

Just as we have different types of security concepts, we also have different types of networks, and each of these networks has a different process for managing security. Let us discuss the concept of a virtual private network wherein the concept of encapsulating security payload is widely used.

In simple terms, a virtual private network is a type of network which is used by organizations that have offices across the world. The network provides the facilities for cost reduction and the means and mechanism to remove geographical distances. For example, an office in India has several branch offices in the USA as well as in India. The VPN or the virtual private network connects each of the offices in the USA as well as in India so that they feel that they are connected and are working as a unit.

Now coming to Encapsulating Security Payload (ESP) is a protocol that is responsible for providing security in the VPN network. Like the body which is responsible for the repository of digital signatures, the ESP is a member of the protocol that keeps track of ESP.

It is this ESP that secures the VPN network.

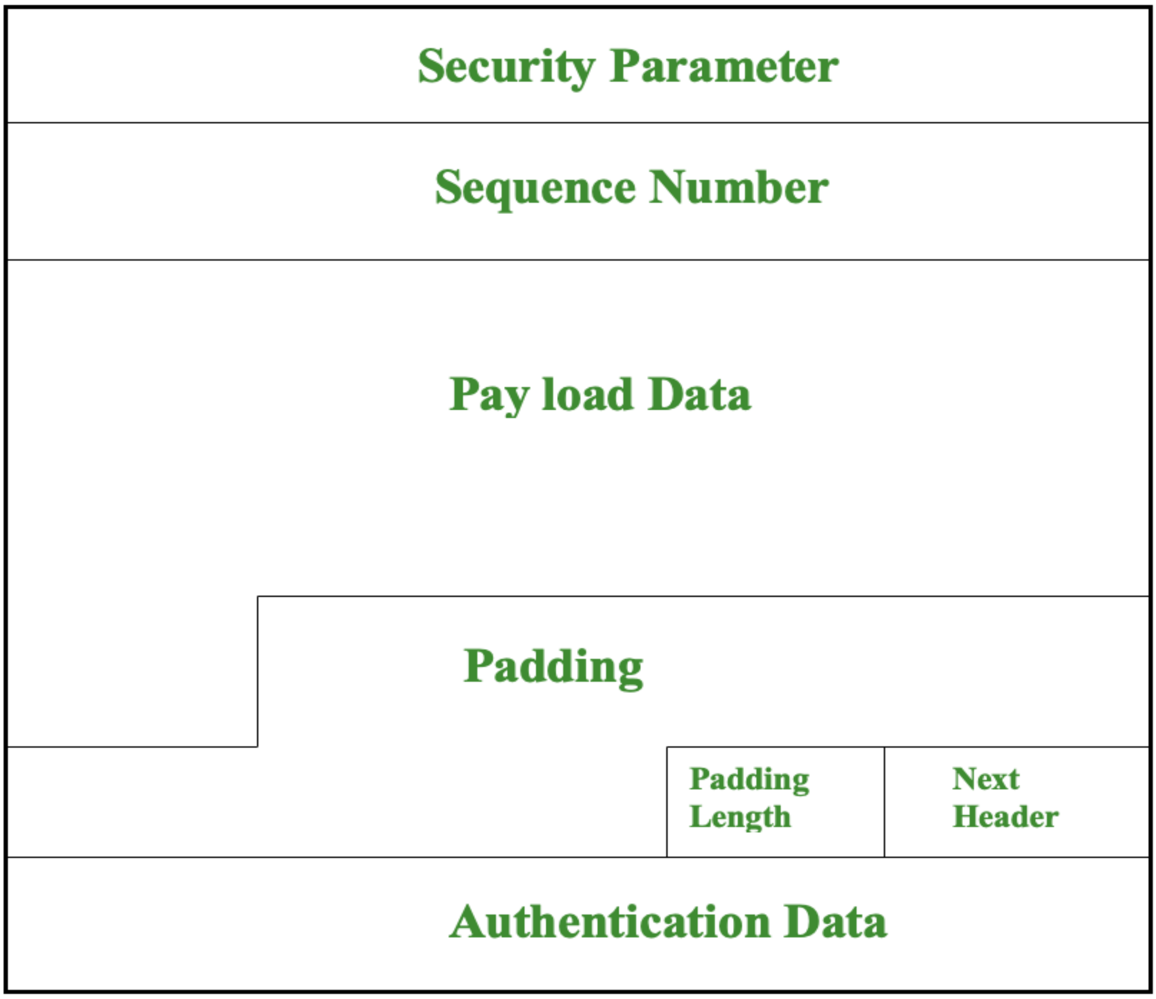


Figure 2.17 : Basic configuration of the ESP

The figure 2.17 depicts the basic configuration of the ESP

2.6.2 Combining Security Associations and Key Management

In the previous sections, we discussed the various aspects. However, one thing that has been re-iterated again and again is the fact that there is no hard and fast method for implementing encryption security controls. This section deals with the variety of aspects of how different methods are used for the encryption process.

Refer to the figure given below

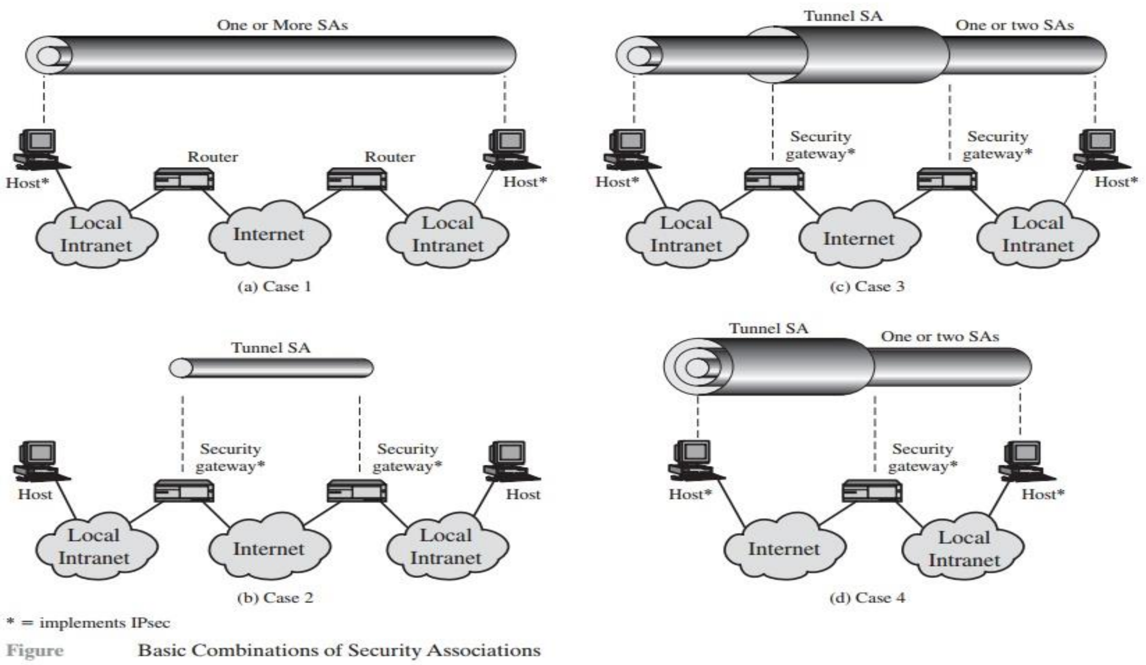


Figure 2.18 : Combining Security Associations and Key Management

From the figure 2.18, it is seen that in a given network several combined controls are implemented. For example, we have tunnel SA approach in another network we have tunnel SA with one or two SA approach.

This just shows that one needs to take into consideration several aspects of security based on the environment.

- **Knowledge Check 2**

State True or False.

1. Hashing is a process for converting the message into an encrypted format (True / False)
2. Kerberos is used for securing the components of the network (True / False)
3. Email security is carried out by means of digital signature (True / False)
4. IP security architecture deals with the process of encoding by means of an algorithm (True / False)
5. The authentication header is concerned with the router (True / False)

- **Outcome-Based Activity 2**

  Prepare an excel which will contain the components of the network. For each of the components try to identify the technique which will be used for protecting the component. Prepare the sheet in the following format:

Component	Encryption Technique
Router	Authentication Header
Password for banking transaction	SHA
LAN network	Authentication Header

2.7 Summary

- Today there is a great need to protect the data as it travels across the network
- In order to ensure that the data is protected several techniques are deployed
- The technique that is commonly used are Hash functions, Digital signatures, Kerberos, and the like
- The process of protecting the data depends upon several factors
- This includes the business objectives, the type of the network
- The type of business operations that are transmitted across the network
- There is no hard and fast rule which will protect the data
- This includes protecting the data at the content level
- Protecting the data at the packet level
- Protecting the data at the network level
- Protecting the data at the digital signature levels
- There are several algorithms that are used to protect the data
- There is a hash function that is responsible for converting the message or the text into an encrypted form which will form an input to the algorithm.
- The algorithm converts the encrypted data into a form that takes into consideration the contents which are exactly transmitted across the network

2.8 Self-Assessment Questions

1. What is meant by the Hash function? Explain with the help of an example
2. What is meant by the term authentication header? Explain with example
3. What is meant by the term MD5? Explain

4. What is meant by Directory Authentication Service? Explain its importance
5. What is meant by IP security architecture? Explain

2.9 References

- Rivest, R. L. (1994, December). The RC5 encryption algorithm. In *International Workshop on Fast Software Encryption* (pp. 86-96). Springer, Berlin, Heidelberg.
- Westhoff, D., Girao, J., & Acharya, M. (2006). Concealed data aggregation for reverse multicast traffic in sensor networks: Encryption, key distribution, and routing adaptation. *IEEE Transactions on mobile computing*, *5*(10), 1417-1431.
- Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J. A., ... & Felten, E. W. (2009). Lest we remember: cold-boot attacks on encryption keys. *Communications of the ACM*, *52*(5), 91-98.
- Ateniese, G., Benson, K., & Hohenberger, S. (2009, April). Key-private proxy re-encryption. In *Cryptographers' Track at the RSA Conference* (pp. 279-294). Springer, Berlin, Heidelberg.
- Hargreaves, C., & Chivers, H. (2008, March). Recovery of encryption keys from memory using a linear scan. In *2008 Third International Conference on Availability, Reliability, and Security* (pp. 1369-1376). IEEE.
- Maughan, D., Schertler, M., Schneider, M., & Turner, J. (1998). Internet security association and key management protocol (ISAKMP) (No. rfc2408).
- Valkonen, J., Asokan, N., & Nyberg, K. (2006, September). Ad hoc security associations for groups. In European Workshop on Security in Ad-hoc and Sensor Networks (pp. 150-164). Springer, Berlin, Heidelberg.

Unit : 3

Web Security

Learning Outcomes:

- Students will be able to understand the basic concepts involved in the web-based security system
- Students will be able to understand the various requirements of the web security system.
- Students will be able to understand the concepts involved in the application of the security basics in the OSI model.
- Students will be able to understand the concepts involved in the application of the Secured Socket layer and the difference between Transport layer security.
- Students will be able to understand the Secure electronic transaction.
- Students will be able to understand the basic concepts of Firewalls and their applications.
- Students will be able to understand the concepts of Firewalls and the Intrusion Detection System.

Structure

3.1 Introduction

In the previous unit, we covered the various aspects of the security mechanism that are commonly deployed when transactions are carried out over the internet. In other words, whatever is transmitted over the internet, needs to be protected so that only the intended persons are able to carry out their activities. However, when things move over the internet there are unscrupulous individuals who are always looking for *stealing* the information which is transmitted over the internet. Thus, information flowing in the networks needs to be protected. There are several ways to protect information. The common methods that are deployed include encryption, digital signature, hash mechanisms, and the like. Further, due to the nature and complexity of the network design, there is an imperative need to protect the various components of the network as *information can be accessed from any node* in the network.

The figure 3.1 depicts the areas that are being discussed.

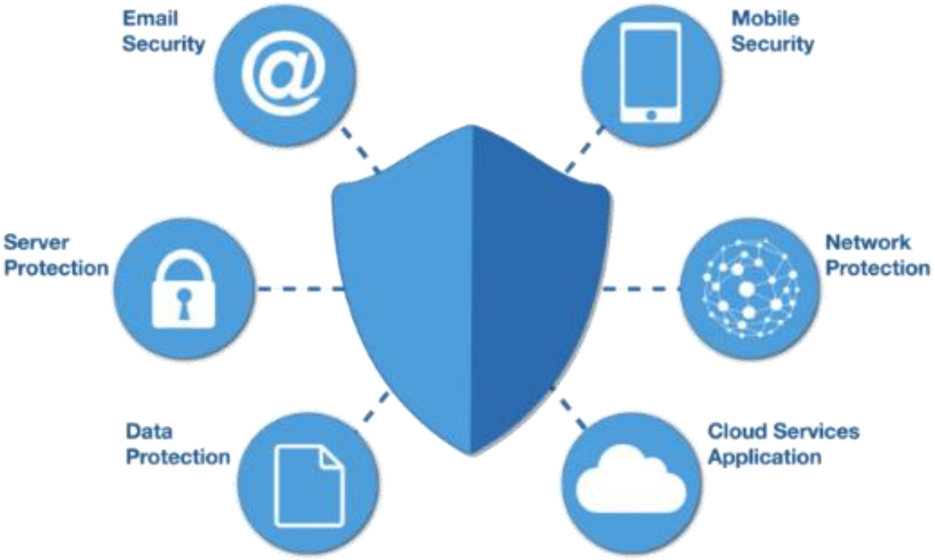


Figure 3.1 : Web Security

Referring to the figure, it is seen that various components are required to be protected so as to ensure that only intended users are able to use the data or the information.

In this unit, we will discuss web security.

3.2 Requirements

Before we dwell further, let us now discuss the concept of web security. A web as we all know is the collection of files stored on a server. These files are required for executing various tasks when the website is made available for public use.

Refer to the figure 3.2 which depicts the basic concept of the web.

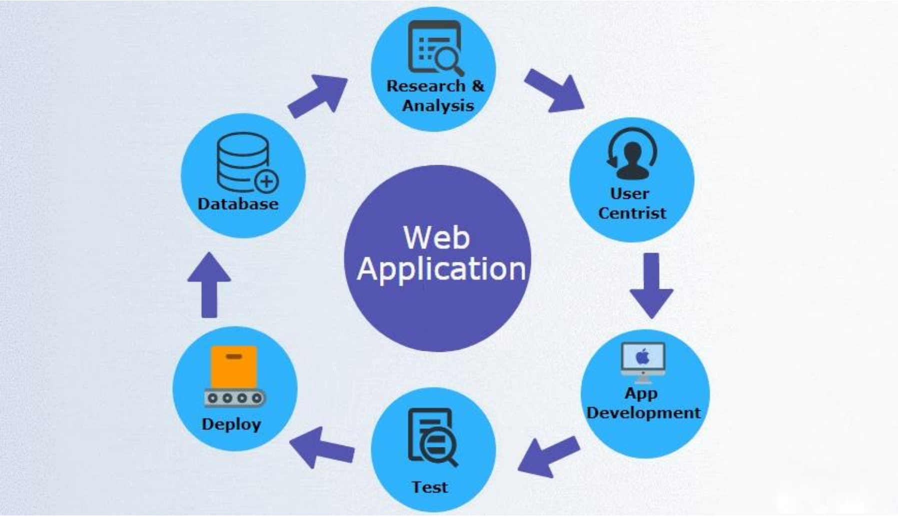


Figure 3.2 : Web Application

From the figure, it is evident that the web comprises various components which are the database, the server represented by deployment, and the application. *All these are required to be protected when the data or the information flows through the internet. In other words, whatever is being passed around in the form of data or information from any of the components needs to be protected.*

Thus, it is not only the data that needs to be protected it is the components that also are required to be protected as *they are the agents of data or information carriers across the internet.*

Having understood the concept of the basic structure of a web or a web application or website, let us now discuss the requirements for protecting the web. In other words, web security. Worth mentioning is the fact that when we talk about web security it means the various measures and the set of protocols that are adopted for providing security to the web application including the servers and the web devices which form a part of the internetwork.

These measures are targeted to ensure that cyber hackers and other individuals who have malicious intent fail to exploit the information or the data which is carried across the system.

Let us now discuss the requirements for web security.

In simple parlance by the term requirements, it is meant what constituents are needed to provide the security

Refer to the figure 3.3. This figure demonstrates the various requirements for web security.

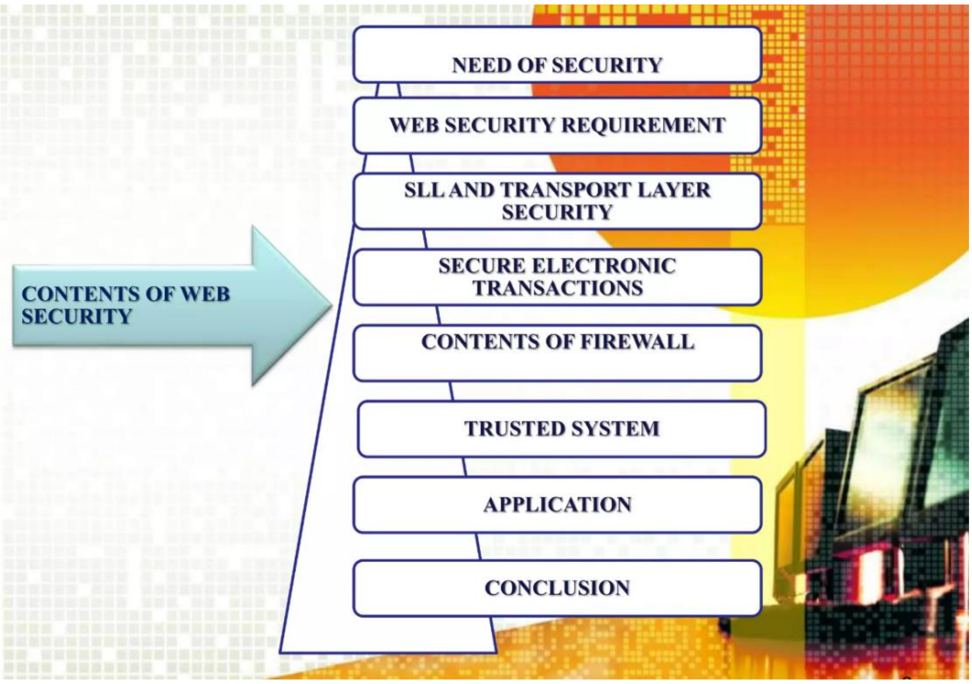


Figure 3.3 : Contents of Web Security

From the figure, it is evident that there are several phases or stages for web security implementation and the requirements are specific to each of the phases or stages.

Let us now discuss some of these as depicted in the figure.

- The first step is the need for security. In essence, this refers to the fact that we need first to identify or define what security measures are needed to be deployed in the web system. By this, it means what components, messages devices, and the like are required to be secured and the degree and depth of the security that is needed to be deployed. It all covers the documentation of the security requirements including the passwords policy, the access permissions, and the like. This is the most important and crucial stage in the web security requirements

- The next stage is the web security requirement. Once the first step complies with the next crucial stage is the web security requirement. In essence, this stage identifies and defines the degree and depth of the security measure that is required to be implemented. For example, whether we have to deploy MD5 encryption or we have to deploy a firewall and the type of the firewall and on what layer of the server and the like.
- The next stage is the SLL and the transport layer security. This is another important aspect of the security measures that are adopted during the implementation of security protocols. In essence, this stage is responsible for deploying the security at the various layers of the OSI model. In other words, as the data is transmitted on the protocol which is based on the layer concept and the OSI model, we need to implement the security aspects at these levels. The SSL stands for secured security layer. This is the set of protocols that programs are responsible for the data transmission of the data packets as well as the transmission of the data itself.
- The contents of the firewall. This is another layered security protocol that is required to be implemented. In essence, the firewall is a layered protocol that is the software that is designed to function over the router or the hub, or the server which is responsible for ensuring that at the macro level the security controls are implemented. Worth mentioning is the fact that there are different types of firewalls and each of these firewalls is designed to serve a specific type of security measures. They are also required to be updated frequently.
- Trusted system. This is the other type of requirement which is needed by the web server for implementing security measures. In essence, a trusted system is a system that in the given scenario is designed to provide adequate security measures to the user so that he is confident enough that the information or the data that is being passed over the network is safe enough. In other words, it is secured from known threats and mechanisms commonly adopted by hackers.
- Application. These are the security controls that are deployed at the application level itself. In other words, the application itself has incorporated measures for providing security.

  Finally, it is to be noted *despite all these precautions and controls none of these are foolproof as the hackers are coming up with innovative means and mechanisms for breaking into the web application system*

3.3 Secure Socket Layer (SSL) and Transport Layer Security (TLS)

In order to understand the future sections of this unit, refer to the figure which is used for the transmission of the data or the information across the network.

This diagram depicts the basic concepts of the layers through the data flows across the network.

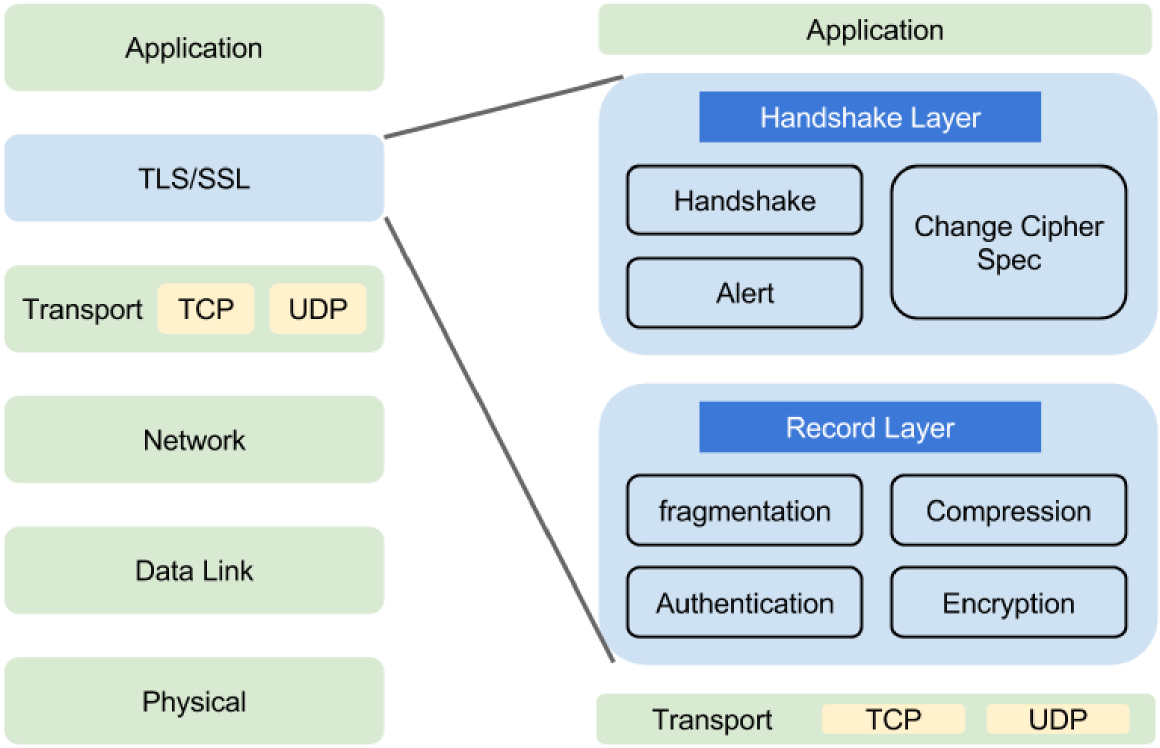


Figure 3.4 : Secure Socket Layer (SSL) and Transport Layer Security (TLS)

From the figure 3.4, it is seen that whenever we are invoking the internet or in fact any network there is invariably a set of layers that are used in the process of transmission of data or information.

- The first layer is the application layer. This is the layer in which the web application is deployed on the server
- The next layer is the TLS / SSL layer. This is the layer that provides security to the transport layer and the secure socket layer
- Transport TCP / UDP. This is another layer that is used for transmitting the packets across the network

- Network. the network layer is responsible for protocols that are deployed across the network
- Datalink. This is the layer that connects or links the various contents of the data
- Physical layer. This is the actual physical layer.

With this basic structure in place, it is evident that the SSL and the TLS layer sit at the top of the application layer. Let us now discuss these layers in detail.

The SSL stands for secure socket layer and the TLS stands for transport layer security.

In general, SSL is a standard methodology that makes use of the technology to provide an internet connection safe and secure to the contents which are sent between two different systems. This is done to ensure that the cyber hackers are unable to perform malicious operations on the sensitive data which is sent across to the networks.

Refer to the figure 3.5 which depicts the concepts of the workings of the SSL

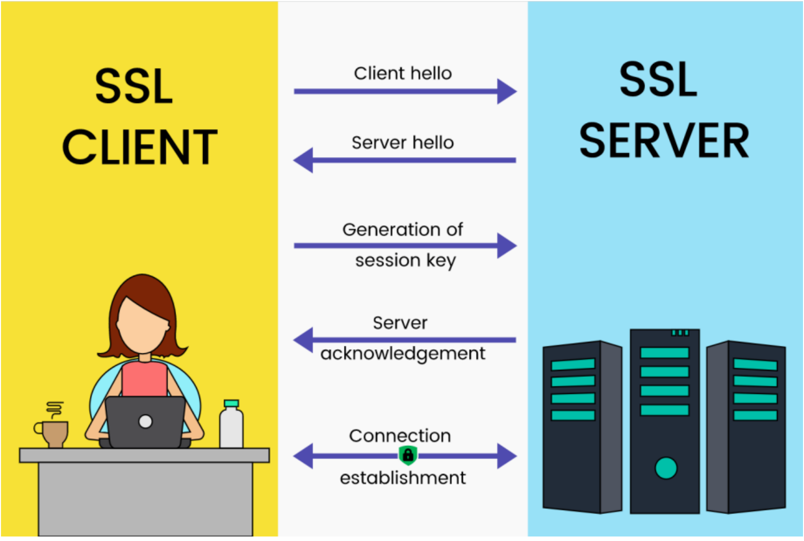


Figure 3.5 : SSL Client and Server Side

From the figure, it is seen that both devices are having secured socket layers. This means that the protocols which provide security to both the devices that are the client and the server are already in place.

The first step is the establishment of a connection between the client and the server. Once the connection is established then various controls which demonstrate the security measures are established. This includes the session key which is acknowledged by both parties.

In order to understand the concept of TLS refers to the figure given below:

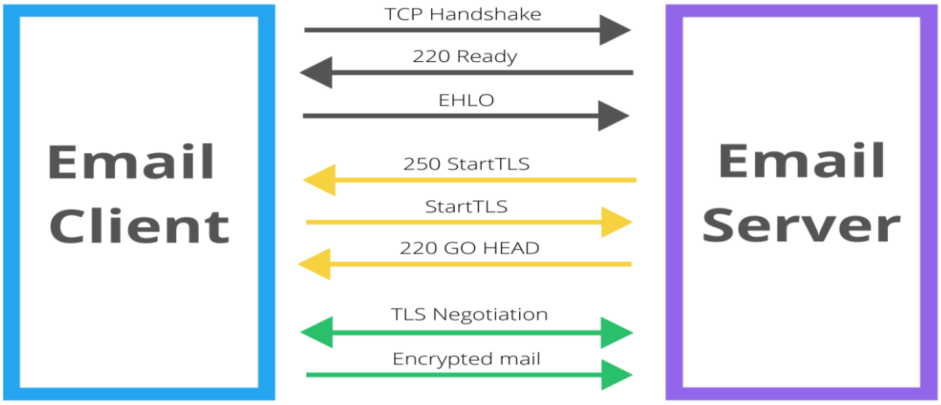


Figure 3.6 : Email Client and Server Side

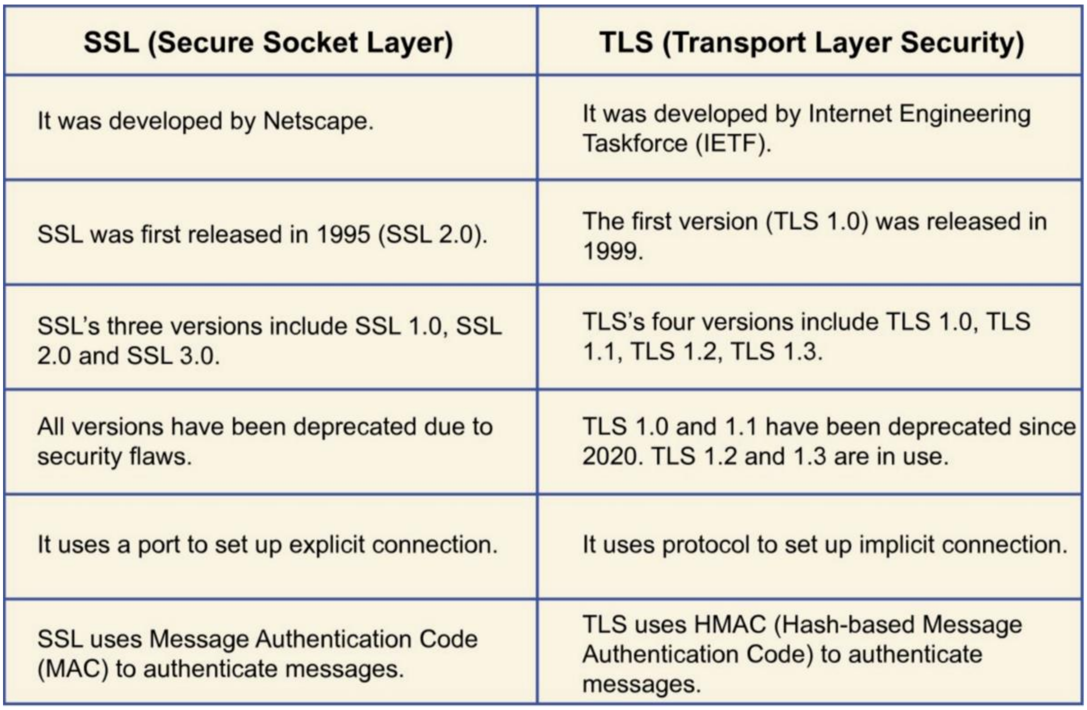
Here from the figure, it is evident that when it comes to the process of TLS or the transport layer security, we take the case of the email client and the email server. At the start, it is the TCP handshake. This means that by using the Transmission control protocol the connection is established between the client and the server. In other words, the necessary connection permissions are obtained and both devices are ready for sending and receiving the email documents. When the process is completed the TLS protocol is started which establishes the secure connection. This means that once the credentials for the handshake are established the Transport layer security protocols are established and the encryption algorithms are activated for the transmission of the message through the TLS protocol. Thus, we see that we have a two-layer security system in place. One is at the message level and the other is at the transport or the transfer level by means of TSL protocol. So even if the hacker is able to exploit the TSL layer, he will not be able to decode the message as it has been encrypted by means of the hashing algorithm.

Difference between SSL and TSL

Having understood the functions of the SSL and the TSL in the sense that they are responsible for providing security at the transport level or the transmission level\, let us no discuss the difference between the SSL and the TSL

In general, when it comes to the functional part, they are basically the same except that TSL provides a more robust security due to the fact that in the case of SSL a hardware port is used to establish the secure connection which is explicit while in the case of the TLS an implicit connection is used as it is based on the protocol and not on any port so *the chances of providing stronger security are inherent*.

Refer to the figure 3.7 which provides more differences in terms of the other aspects of TLS and the SSL



SSL (Secure Socket Layer)	TLS (Transport Layer Security)
It was developed by Netscape.	It was developed by Internet Engineering Taskforce (IETF).
SSL was first released in 1995 (SSL 2.0).	The first version (TLS 1.0) was released in 1999.
SSL's three versions include SSL 1.0, SSL 2.0 and SSL 3.0.	TLS's four versions include TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.
All versions have been deprecated due to security flaws.	TLS 1.0 and 1.1 have been deprecated since 2020. TLS 1.2 and 1.3 are in use.
It uses a port to set up explicit connection.	It uses protocol to set up implicit connection.
SSL uses Message Authentication Code (MAC) to authenticate messages.	TLS uses HMAC (Hash-based Message Authentication Code) to authenticate messages.

Figure 3.7 : Difference between SSL & TLS

3.4 Secure Electronic Transaction

In the previous sections, we discussed the various issues pertaining to web security. However, as the web progressed, the scope of the benefits of the web to society increased tremendously. This means that the initial purpose of the web was magnified and it engulfed the commercial world. |for example, it moved to electronic commerce, e-banking, e-business, and the like. In other words, it brought the shop home wherein the buying and selling began to take place. All these new features necessitated the need for implementing new security features in the web application wherein electronic transactions are taking place. Thus, the need for securing electronic transactions taking place over the internet.

In simple parlance the term secure electronic transaction refers to a system wherein the integrity and the security of the electronic transactions made over the network are secured and protected. In other words, sufficient and necessary measures are implemented to ensure the safety and security of electronic transactions are in place. The e-commerce websites wherein buying and selling are conducted widely implement secure electronic transactions.

Worth mentioning is the fact that when we deal with the secure electronic transaction, we invariably are in contact with several components. Some of these components include the cardholder, internet, certificate authority, merchant, payment system, payment gateway, and the like.

Refer to the figure 3.8.

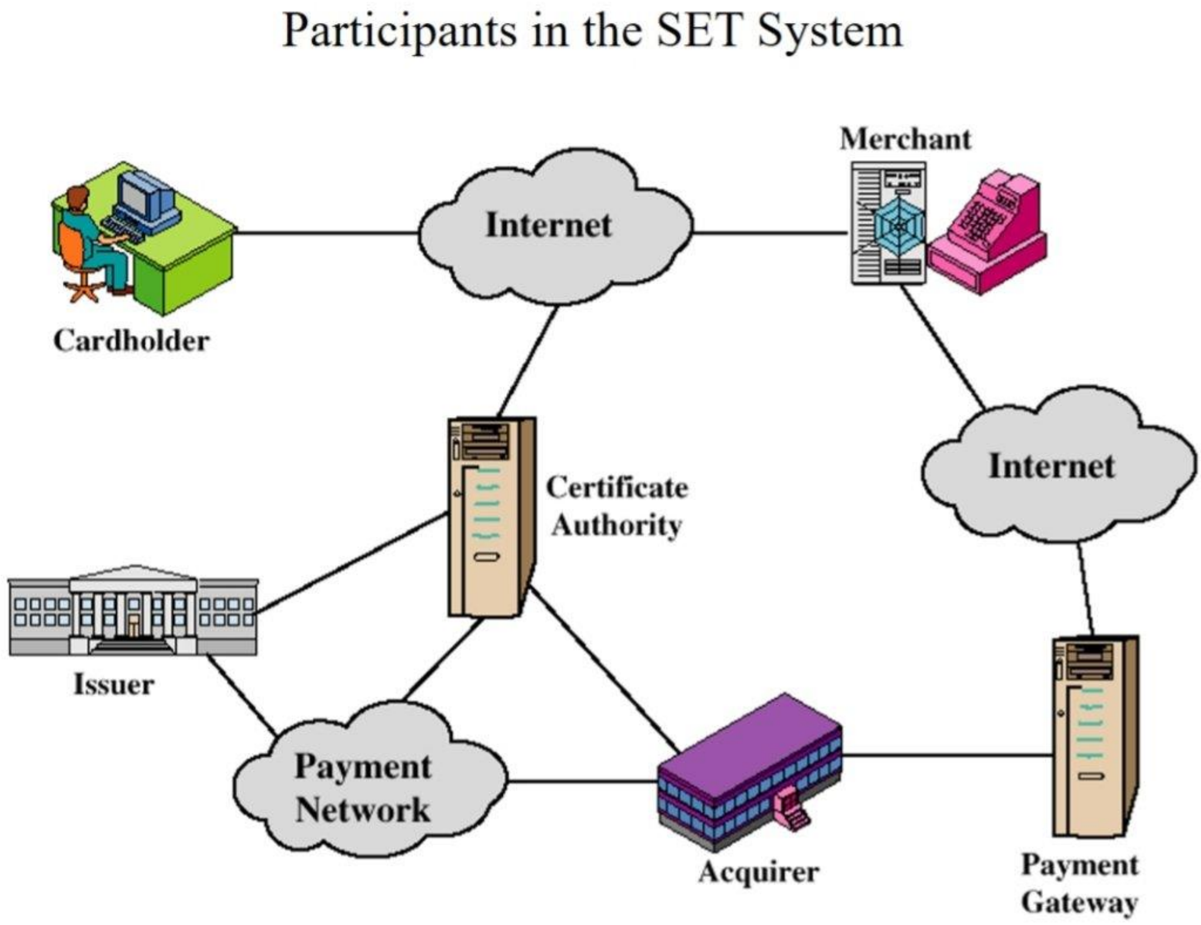


Figure 3.8 : Secure Electronic Transaction

From the figure, it is seen that there are several components in the network which are involved in the process of carrying out secure electronic transactions. Here it is seen that security is provided at each component so that the electronic transaction is secured at each point of contact.

The working of the secure electronic transaction is initiated at the cardholder's end. The cardholder logs onto the electronic system by using the internet. The secured website begins with HTTPS the word S in the HTTP means that adequate security measures are incorporated and are certified by the certifying agency or authority. The said is linked with components of the network such as issuer, merchant, payment gateway, and the issuer. All these are secured in terms of implementation of adequate security controls the entire transaction is provided further security wherein the user is required to enter the pin code, the password, and the login-id. All these are adequate measures for additional security.

In addition to the above discussion, as the span of electronic transactions expands which means that electronic transactions are carried over different networks more secure measures through protocols are required to be implemented.

A typical example is that a person sitting in New Delhi orders a book from the internet to an e-commerce website that is hoisted on a US server. Also, the money is displayed in the dollar. This is a complex network wherein involves several layers of security. One layer for the US website, one layer for Dollar and rupee conversion, and one layer for determining the validity of the payment through the card on the like.

All these complexities generate the need for an extra layer of security.

The following figure 3.9 depicts the need for extra security at several places or points in a network.

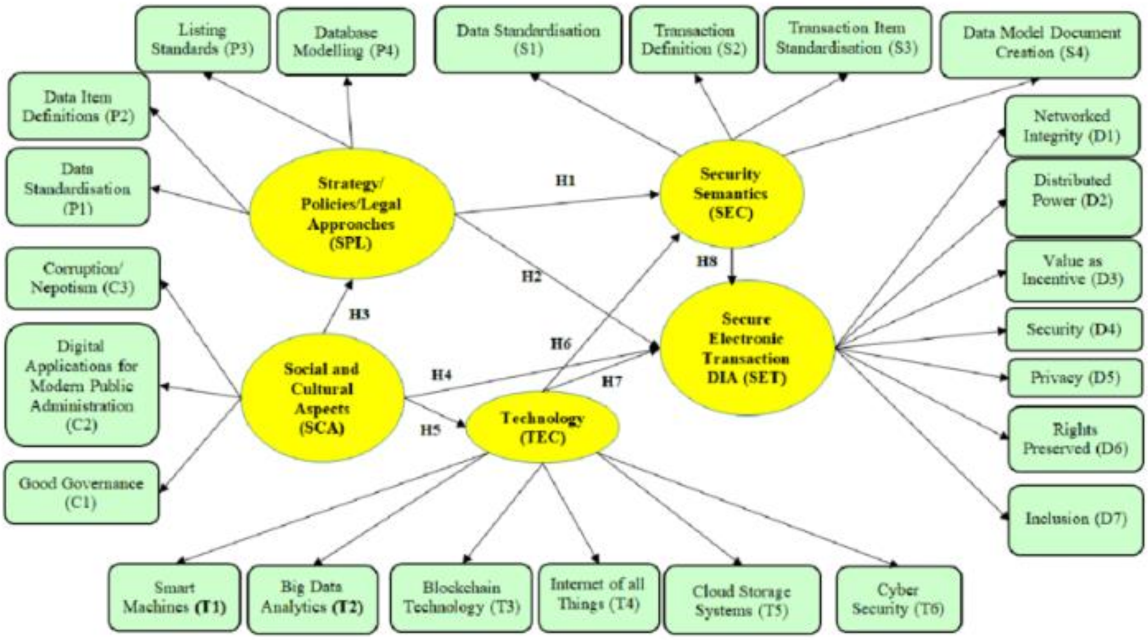

Listing Standards (P3)
Database Modelling (P4)
Data Standardisation (S1)
Transaction Definition (S2)
Transaction Item Standardisation (S3)
Data Model Document Creation (S4)
Data Item Definitions (P2)
Data Standardisation (P1)
Networked Integrity (D1)
Distributed Power (D2)
Strategy/ Policies/Legal Approaches (SPL)
H1
Security Semantics (SEC)
H2
H8
Value as Incentive (D3)
Corruption/ Nepotism (C3)
H3
Secure Electronic Transaction DIA (SET)
Security (D4)
H6
Digital Applications for Modern Public Administration (C2)
Social and Cultural Aspects (SCA)
H4
H7
Privacy (D5)
H5
Technology (TEC)
Rights Preserved (D6)
Good Governance (C1)
Inclusion (D7)
Smart Machines (T1)
Big Data Analytics (T2)
Blockchain Technology (T3)
Internet of all Things (T4)
Cloud Storage Systems (T5)
Cyber Security (T6)

Figure 3.9 : Framework for implementing security in electronic transactions

The above figure provides a framework for implementing security in electronic transactions. It is evident that several layers are involved in the process. The most important among them are the technological factors, digital factors, and security and privacy issues. This also includes the access permissions which are needed to be provided at various points or nodes in the network

3.5 Firewalls

We have been discussing the security aspects of a web network. The basic aspect of which the web works is the fact that the web involved the flow of data between different networks or amongst different devices or nodes in the same network. In other words, the information flows or receives from one network to another network.

Now an issue may arise in seeking an answer to the issue wherein one of the networks is secured network while the other network is unsecured. In other words, what security mechanism exists wherein networks are of different types? In other words, can an information network prevent the flow of data between different networks?

This is achieved through firewalls.

In simple parlance, a firewall is a network security mechanism that is designed to track and monitor the incoming or outgoing traffic in a network. This monitoring and tracking is carried out by means of a defined criterion.

The figure 3.10 depicts the concept which is being discussed here.

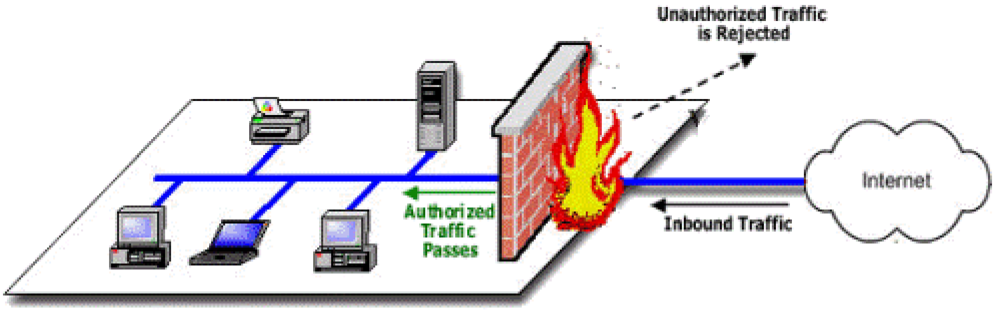


Figure 3.10 : Function of a firewall

From the figure, it is seen that the prime function of a firewall is to prevent the data from unauthorized or unsecured networks from entering the secured network system or vice versa.

Types of firewalls

We have discussed the function of the firewalls. The basic function is to prevent the outflow or the inflow of data from one network to another network. The firewall can be a software firewall or a hardware firewall.

The software firewall functions on the basis of the controls implemented by the software which prevent the information flow while the hardware is operated by means of hardware devices.

The figure 3.11 depicts examples of hardware and software firewalls.

However, one thing that needs to be taken care of is the fact that both the hardware and the software firewalls are susceptible meaning that they can be broken. Hence these are to be regularly updated.

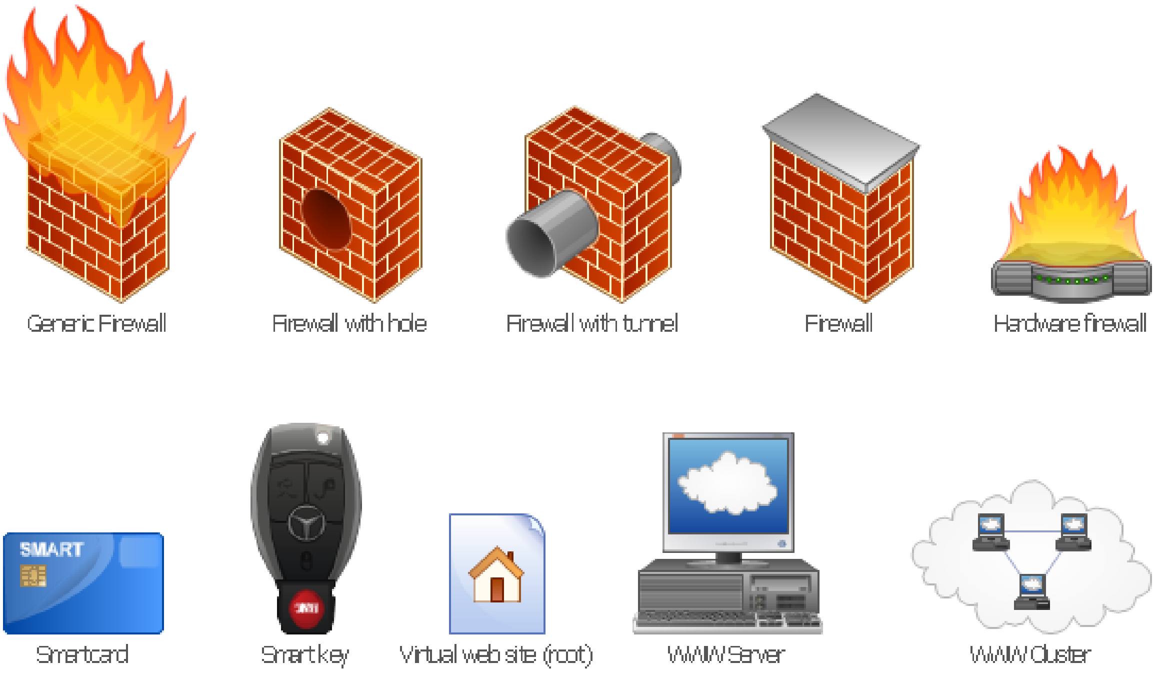
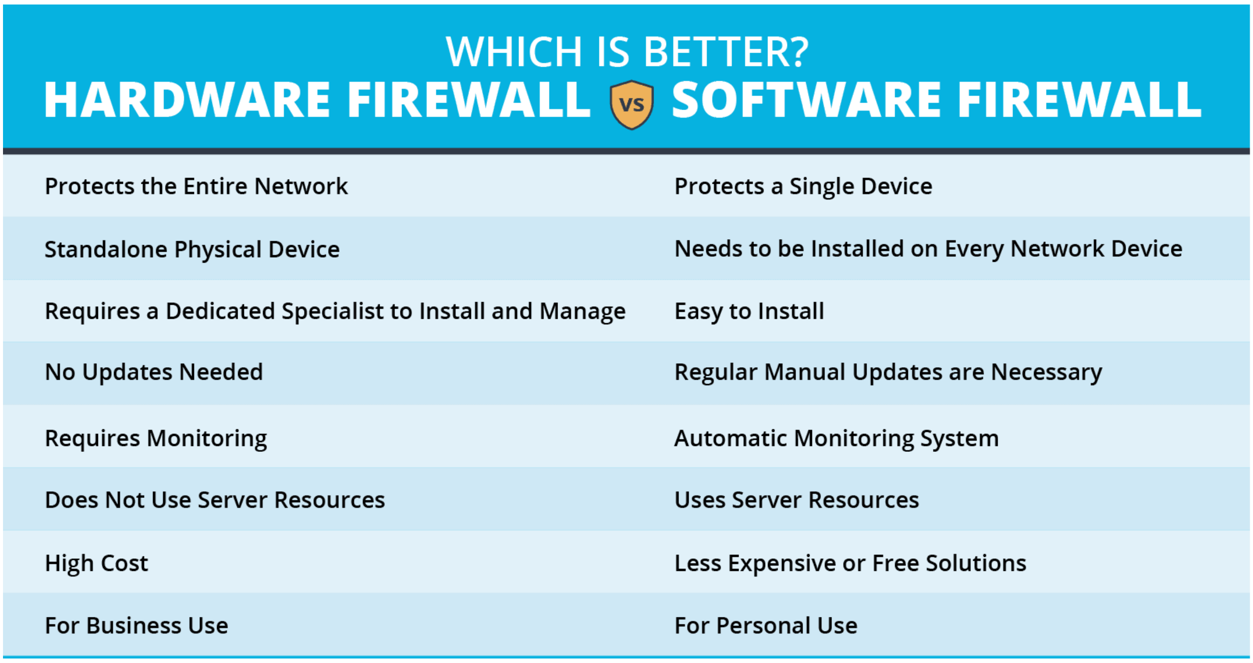


Figure 3.11 : Types of firewalls

Difference between hardware and software firewalls

Having understood the basic functionality of the firewalls and that there are two types of firewalls, let us now differentiate the hardware and the software firewalls.

Refer to the figure 3.12 for the various points of difference between the hardware and the software firewalls.



WHICH IS BETTER?

HARDWARE FIREWALL	VS SOFTWARE FIREWALL
Protects the Entire Network	Protects a Single Device
Standalone Physical Device	Needs to be Installed on Every Network Device
Requires a Dedicated Specialist to Install and Manage	Easy to Install
No Updates Needed	Regular Manual Updates are Necessary
Requires Monitoring	Automatic Monitoring System
Does Not Use Server Resources	Uses Server Resources
High Cost	Less Expensive or Free Solutions
For Business Use	For Personal Use

Figure 3.12 : Difference between the hardware and the software firewalls

From the figure, it is evident that the hardware firewall is applicable to the entire network while the software firewall is responsible for protecting a single device. On the other hand, the process of installing a hardware firewall is difficult as it requires the services of a specialized network professional while in the case of a software firewall anyone can install it as it is like the software installation.

- **Knowledge Check 1**

Fill in the Blanks

1. The full form of SSL is _____________.
2. The firewall is comprised of ___________ and the ___________ components.
3. Every web-based application makes use of _______________.
4. The trusted system is the one in which there is ____________ policy.
5. The secure electronic system is the most important electronic system.

- **Outcome-Based Activity 1**

Prepare an excel report which identifies a web-based application and within the sheet identify the type of security system implemented in place. For example, in the fee collection of a college, the various controls which are needed are SSL, IDS, and other controls.

3.6 Firewalls Design Principles

From the above discussion, it is evident that firewalls are essential in the process of protecting the flow of information from one network to another network.

However, designing a firewall takes into consideration several aspects. Some of these are discussed below

- **The crucial aspect of setting the security policy in the organization**

This is the most important consideration which needs to be taken into consideration while designing the firewall. The important components of this parameter are the business processes the business objectives and the amount of money that the organization is willing to invest in implementing the firewall. For example, if the company is into financial services, then the degree and the depth of the firewall measures will include the hardware and the software components also. However, if it is in e-commerce operations then the degree and the depth might be moderate and in that case, the software firewall will do the work.

- **The components where the firewalls are needed to be installed**

This is another important aspect wherein the firewall are needed to be installed. For example, if the marketing persons are always on the move, then the hardware firewall is to be installed on their laptop so that unauthorized data may be prevented from moving into and out of the system.

The figure 3.13 depicts other design principles which are taken into consideration.

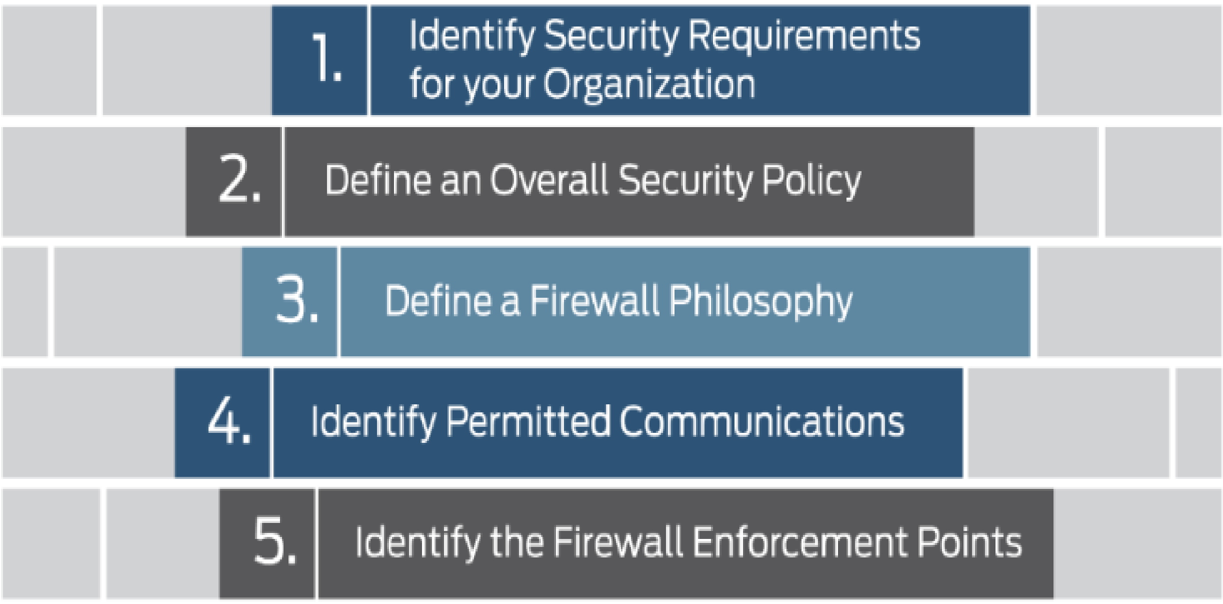

1. Identify Security Requirements for your Organization
2. Define an Overall Security Policy
3. Define a Firewall Philosophy
4. Identify Permitted Communications
5. Identify the Firewall Enforcement Points

Figure 3.13 : Design Principles of Firewall

However, one thing that needs to be taken into consideration is the fact that the steps mentioned in the figure are not foolproof.

It all depends on the business objectives.

3.7 Trusted Systems

A trusted system in a network is a system that provides access to only authorized users only. They are specially designed to provide the highest level of security to the users though this is not the case every time. Trusted systems have breached though their rate of breach is less than other systems.

The following points enumerate the elements of the trusted systems.

- **Multilevel security**

This is the most important design consideration of trusted systems. Multilevel security is applied by taking into consideration the following points.

  - Top secret level security. This is the security wherein the controls are provided to trusted and authorized persons only. These are only a handful of persons who are entrusted with the key responsibility. For example, in a government bank, the chief manager and his deputy manager are in the process of having controls pertaining to top-level security such as the master key of the bank or the code.
  - Confidential level security. This is the security level that is of trusted nature. In this type of trusted system, only the authorized persons who are entrusted with the task of carrying out the work are provided the confidential details.

- **Access level security**

This is the security that is concerned with the process of providing access controls to authorized users. This may include aspects such as:

  - Read control. This control may be in the form of reading the records pertaining to a particular product from the files stored in the database.
  - Write control. This may be in the form of creating a new record in the database.
  - Delete control. This control may be in the form of deleting the information from the database.
  - Control is based on the rank and the types of work that are needed. This control may be in the form of allowing specific permissions to say database manager to install updates.
  - Controls are based on the nature of the job or the function that an individual is required to execute.

Refer to the figure 3.14 which provides the visualization of what is being discussed here

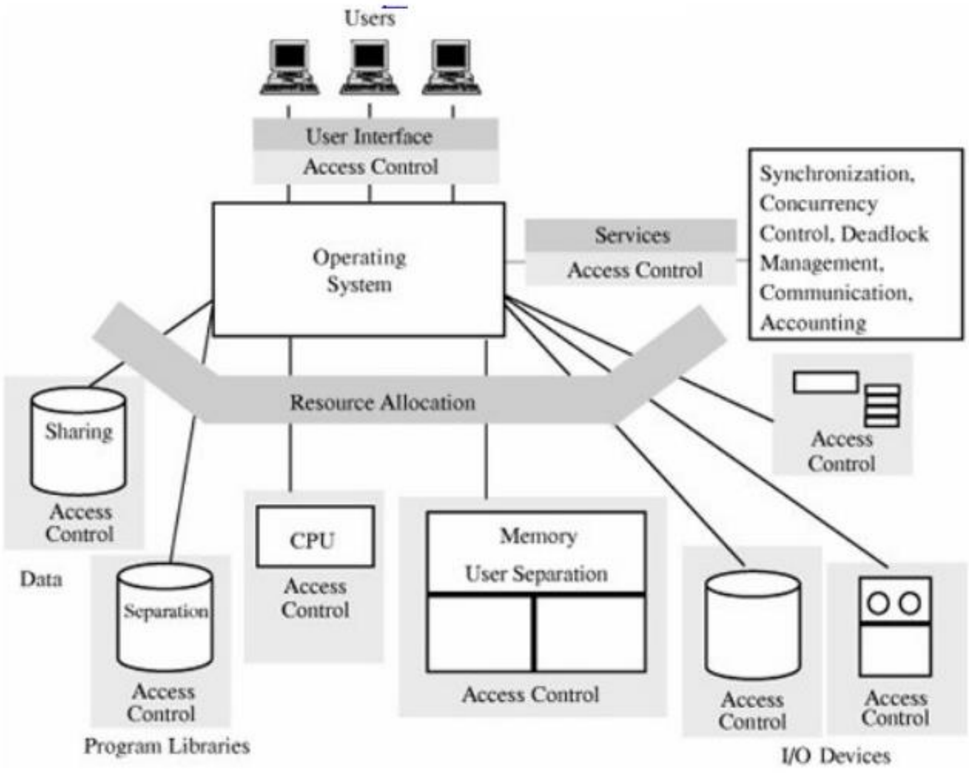


Figure 3.14: Security Functions or a Trusted Operating System

From the above figure, it is seen that a trusted system has several layers of security installed at various places.

For example,

- We have access control at the data-sharing repository
- We have user access control at the operating system level
- We have access control at the program libraries' interfaces
- We have access control at I/O devices.

Further, it is seen that the context is the trusted operating system and at the services access controls we have the following additional controls.

- **Accounting.** There are trusted management controls that are provided to only a few persons who are designated to carry out auditing tasks. These are the specific tasks that provide information to the various services accessed by authorized individuals only. In case of the breach then appropriate action is taken. For example, if an individual working in an HR department tries to access the salary of other employees from the portal, then the audit lock trial will reveal the journey as to what all he has accessed and what damages if any he has done to date. This includes other aspects of determining how the individual got hold of the password.

- **Concurrency.** This is the trusted control mechanism wherein many of the trusted or authorized persons are using the services simultaneously and keeping track of whether they are using the services for which they are authorized or not
- **Deadlock management.** This is the aspect wherein a single individual has logged in from many devices thereby not allowing other authorized persons to take the services.

Zero trust security

We have been using the term degree and depth so often in this unit let us now discuss what is meant by this.

In simple parlance, the term zero trust means that the security controls are implemented in the highest category and any breach or loss of trust invites a penalty. In other words, the degree and the depth of the trust are of the highest order.

An example of zero trust is entering into a highly secured zone such as a border between two countries without any authority. These are highly secure places.

Refer to the figure 3.15. The figure depicts the implementation of various controls in which the degree and the depth are of the highest order. This is evident in the implementation of the CDM system, industry compliance, data access policy, PKI, ID management, and the like

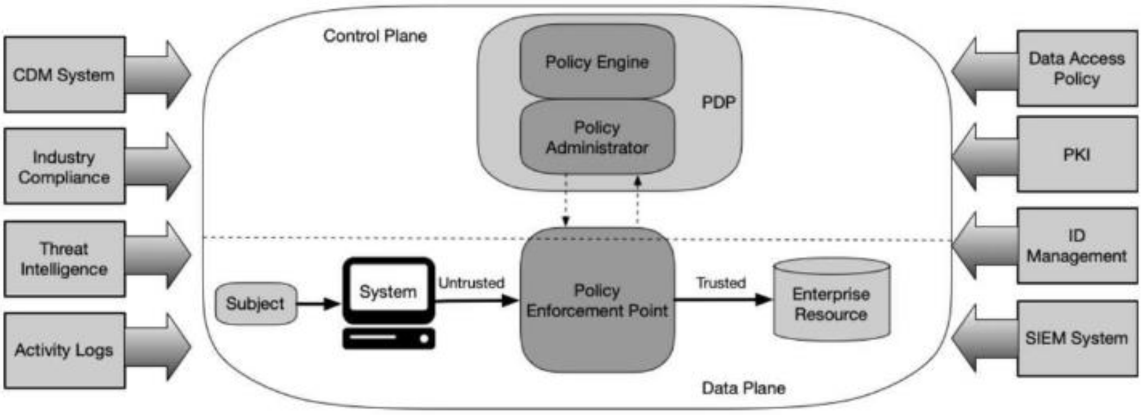


Figure 3.15 : Zero trust security

3.8 Intrusion Detection Systems

We have been discussing the trusted system. However, web security is such as issue wherein one must take utmost care to implement security measures. Any lapse or complacency will be a deterrent to the security controls.

Now coming to the crucial aspect, as mentioned no system is foolproof and there are various attempts to breach the network. The incidents pertaining to the breaching of the network are required to be taken care of and adequate measures are needed to thwart their attempt.

Intrusion detection systems (IDS) are designed to achieve this purpose only.

In simple parlance, the IDS is a device or software which is designed to track and monitor the system for any malicious activity and report it to the administrator of the in-charge of the system.

Functions of IDS.

As mentioned, the core function of IDS is to determine any intrusion and report it to the in charge of the network.

However, based on the nature and the type of the intrusion, the IDS are designed to function in the manner which is best appropriate to the situation.

Refer to the diagram which depicts the basic concepts which are being discussed here in this context.

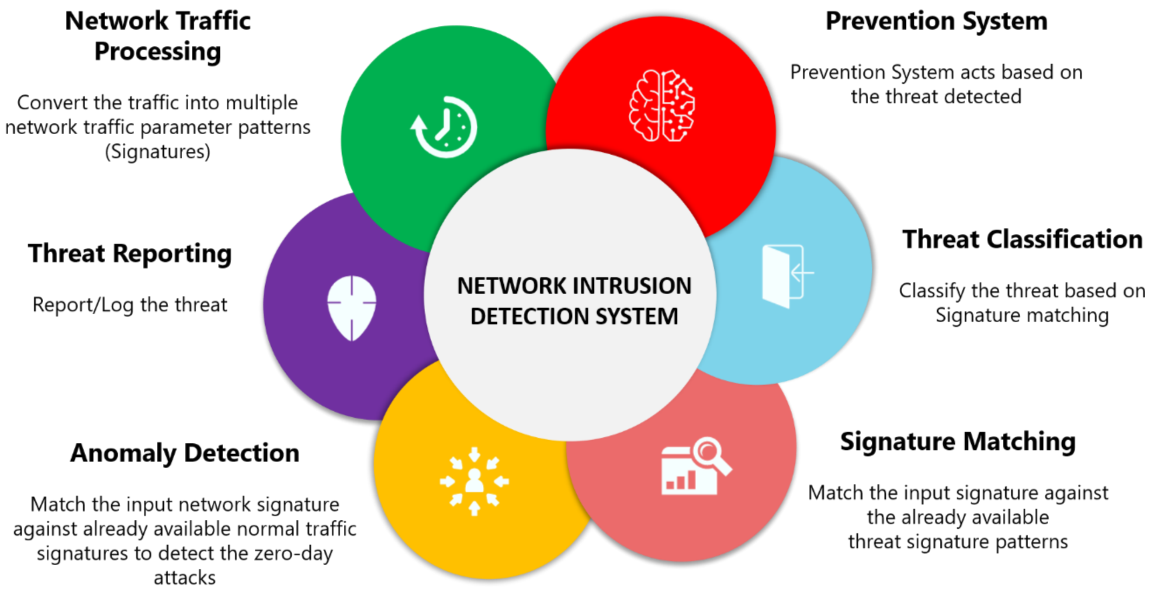

Network Traffic Processing
Convert the traffic into multiple network traffic parameter patterns (Signatures)
Prevention System
Prevention System acts based on the threat detected
Threat Reporting
Report/Log the threat
NETWORK INTRUSION DETECTION SYSTEM
Threat Classification
Classify the threat based on Signature matching
Anomaly Detection
Match the input network signature against already available normal traffic signatures to detect the zero-day attacks
Signature Matching
Match the input signature against the already available threat signature patterns

Figure 3.16 : Functions of IDS.

From the figure 3.16, it is evident that there are varied types of intrusions, and based on the type of intrusions appropriate IDS techniques are implemented.

Let us discuss briefly some of these IDS

- **Anomaly detection**

This is the technique that is used in the network signature wherein the signatures are mismatched and this is reported to the administrator to take the appropriate action.

- **Signature matching**

This is the technique that matches the input signature against the already available threat signature patterns. In other words, the signature which is stored in the database is matched against the incoming signature and if an anomaly is detected it is appropriately reported.

- **Threat classification**

This is the technique in which the incoming signatures are matched with the signatures of the database and based on the degree of the mismatch the IDS are classified.

- **Knowledge Check 2**

State True or False.

1. The web-based system always follows a set of protocols for implementing security in electronic transactions (True / False)
2. The SSL is the short form of a Secured Socket Layer and sits on the top of the application layer (True / False)

3. The firewall is used for protecting the web-based application (True / False)
4. The trusted systems are always secured systems (True / False)
5. The intrusion detection system is used for detecting viruses in a computer system (True / False)

- **Outcome-Based Activity 2**

Taking an example of a web-based e-commerce system that involves the transaction of money identify the various controls which are required to be identified, designed, and implemented in the system. For example, if the web-based application makes my trip dot com then the various controls which are required to be implemented are SSL/ TLS, Firewalls, and the IDS secured systems.

3.9 Summary

- Today with the dependency on the internet and e-commerce operations.
- The e-commerce operations are able to provide transactions of monetary nature.
- These transactions are susceptible to being exploited by unintended persons and hence there is a need for the implementation of a strong security system in web-based applications.
- In order to implement the security system, the first stage must be the requirements stage.
- This is the stage that is responsible for understanding the requirements of the security system in web-based applications. This means that one must be able to identify and define the security components which are needed in the entire system.
- As the web-based system comprises several components at the various layers of the OSI model appropriate security controls are needed to be identified, defined, designed, and are to be implemented in a manner such that they are able to provide security during electronic transactions performed in the web-based operations including the monetary transactions.
- Firewalls are special security means and mechanisms which are implemented in the web-based system to prevent the flow of data from the secured networks to the unsecured networks.

- In order to implement the firewalls certain points of consideration are required to be needed so that the design of the firewalls is in such a manner that will provide almost foolproof security to the web-based application.
- The trusted system is one such system in which there is zero tolerance for the lapses in the security.
- The intrusion detection system is a means and mechanism for identifying the intrusions that are invading the system which unauthorized network components.

3.10 Self-Assessment Question

1. What is meant by web security? Explain with examples
2. What is meant by SSL? Explain with examples
3. What is an intrusion detection system? Explain
4. What is a firewall? Explain its importance
5. What is a secure electronic transaction? Explain with examples

3.11 References

- Stein, L. D. (1998). Web security. Addison-Wesley, Massachusetts, 26, 1-4.
- Garfinkel, S., & Spafford, G. (1997). Web security & commerce (pp. 349-374). Cambridge, MA: O'Reilly.
- Akhawe, D., Barth, A., Lam, P. E., Mitchell, J., & Song, D. (2010, July). Towards a formal foundation of web security. In 2010 23rd IEEE Computer Security Foundations Symposium (pp. 290-304). IEEE.
- Rubin, A. D., & Geer, D. E. (1998). A survey of Web security. Computer, 31(9), 34-41.
- Von Ahn, L., Maurer, B., McMillen, C., Abraham, D., & Blum, M. (2008). ReCaptcha: Human-based character recognition via web security measures. Science, 321(5895), 1465-1468.
- Vieira, M., Antunes, N., & Madeira, H. (2009, June). Using web security scanners to detect vulnerabilities in web services. In 2009 IEEE/IFIP International Conference on Dependable Systems & Networks (pp. 566-571). IEEE.
- Meier, J. D. (2006). Web application security engineering. IEEE Security & Privacy, 4(4), 16-24.

- Schechter, S. E., Dhamija, R., Ozment, A., & Fischer, I. (2007, May). The emperor's new security indicators. In 2007 IEEE Symposium on Security and Privacy (SP'07) (pp. 51-65). IEEE.

Unit : 4

Auditing for Security

Learning Outcomes

- Students will be exposed to the basic concepts of information security.
- Students will be exposed to the basic concepts of information security auditing.
- Students will be exposed to the means and mechanisms needed for conducting information security audits.
- The students will be made aware of the process of the conduct of audit including the formulation of the audit calendar, audit scope, and the like.
- Students will be made aware of the various types of information security audits.

Structure

4.1 Introduction

The commercial world of today is highly complex and complicated. This is due to the fact that information technology advancements have ensured that the businesses which have adopted technology as a part of their business processes have gained significantly. This means that businesses have ensured that information technology is an essential component for running their business operation.

By adopting information technology many business processes have been simplified. As information technology became an integrated component, a large amount of data is being generated. This data is crucial from several perspectives. The most crucial aspect is the fact that this data contained information about the customers, the marketing strategy, the financial dealings of the company, and various other aspects of running the business. Hence, it needed to be protected as it contained vital information.

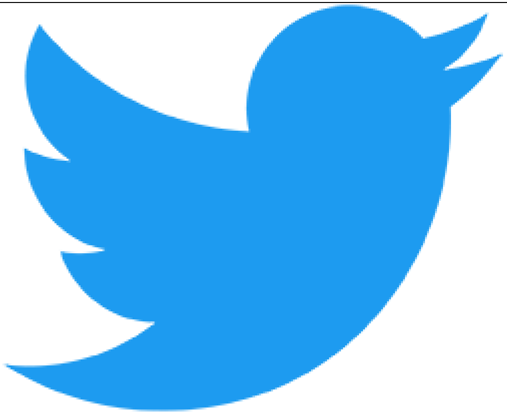
Hence, we have the terms information security. In simple terms, the data or the information is required to be protected at any cost. If this information is exploited by competitors, then the survival of the business would be questioned.

We have several instances wherein the organizations have failed to protect the data or the information and have thus suffered huge losses and market confidence.

Refer to the figures 4.1, 4.2 & 4.3 which depicts the organizations which have suffered due to data breaches or lapses in information security processes.

Date: March 2018
Impact: 1,100,000,000 records
Summary: Aadhaar, India's biometric database, was breached via a security gap at a state-owned organization. As a result, every registered Indian citizen had their information leaked. Their identity numbers, names, bank details, and other personal information were put up for sale on WhatsApp for less than £6.

Figure 4.1 : Aadhaar, India's biometric database



Date: July 2022

Impact: 5.4 million

Summary: In July 2022, an attacker compiled information from 5.4 million Twitter users due to a now-corrected system vulnerability. The attacker stole email addresses and phone numbers and connected them to user accounts. Twitter maintained that no passwords were stolen but urged all Twitter users to use two-factor authentication for their accounts.

Figure 4.2 : Twitter

Date: December 2019

Impact: 250,000,000 records

Summary: Two hundred fifty million records spanning 14 years were exposed without password protection. The information contained customer email addresses, geographical locations, descriptions of the support claims and customer service cases, customer email addresses, and more. The database started being exposed on December 5, 2019, due to a hiccup in security rules and was fixed on December 31, 2019.

Figure 4.3 : Microsoft

The above figure provides a glimpse of the organizations which have adopted technology as the backbone of their business operations. It is seen that *when it comes to the exploitation of data, no organization is safe.* It can be a government organization such as Aadhar or a technological giant such as Microsoft or a Social media organization like Twitter. *Information is susceptible and open for exploitation to serve the nefarious intentions of the hackers*

These examples demonstrate an important aspect that *organizations constantly need to evaluate their information security systems and upgrade them as well so as to stay ahead of hackers.*

Worth mentioning is the fact that the words data and information are synonymous in this document though, in technical terms, they are different. Hence the student should not get confused between data and information.

4.2 Basic Terms related to Audits, Security Audits

Before we dwell further into the audit process, let us now discuss the various terms used in the audit process.

- **Audit**

It is a planned activity that is carried out by trained resources with the objective of determining compliance with the established quality management system.

- **Audit plan**

An audit plan is a document that provides a detailed description of the audit process. It includes the scope of the audit, the resources to be audited and the resources which will carry out audit activities, and the application processes.

- **Audit scope**

The scope of the audit refers to the process of defining the limits or the boundaries within which the audit will take place.

- **Auditor**

The person who conducts the audit as per the audit plan.

- **Auditee**

The person who provides the objective evidence to the auditor as per the defined process.

- **Objective evidence**

This is the evidence which is provided by the auditee based on the applicable processes and the process required for carrying out information security. In other words, this is the *actual* data which is generated from the operations of the processes.

- **Information**

This is the result of the processed data. In other words, the raw data which is the data that has no value is processed meaning that another set of data is combined to generate useful information. Let us take an example to illustrate the concept of discussion. Suppose we write 1245 this is the data as it contains no meaning as different things can be referred to this number. A person may say that this is a roll number another will say that this is a product number and the like, however, if we say that the product number is 1245 then this is information as it has been processed to generate information which is useful that is something can be done to this information.

- **Process**

A process is a method of carrying out a particular activity. A process has an input to which we apply some processing techniques to generate the required output. For example, when we want to open a bank account, we fill in the necessary account opening form. This form is the input. The processing of this input is the verification, the checking of the details as entered in the form such as Aadhar number, pan number, etc., and the presence of the supporting documents such as KYC documents. Once all of these are correct then the account is opened which is the desired output.

- **Procedure**

The procedure is a step-by-step method of doing things. For example, for an account opening the procedure will run like this.

  - Go to the bank where you want to open the account
  - Take the account opening form from the teller
  - Fill in the details
  - Attach the supporting documents
  - Review the form
  - Submit the form to the teller
  - Go back home
  - Wait for confirmation from the bank

- **Information Security**

This is the implementation of the system which will provide an assurance that adequate measures have been taken to protect the information which is crucial to the running of the organization’s business processes.

- **Assurance**

This is the degree and depth of confidence that is provided to ensure that the data is protected. In other words, it is the confidence that is reflected and targeted to meet the security requirements.

- **Information Security Risk**

Risk is the happening or non-happening of an event. Risk is always targeted for the future. If the risk occurs then there is a potential loss to the business in terms of time, cost, quality, scope, and *any other parameter which will impact the business.* Every happening of risk is a loss. Since it is a loss if the risk occurs, nevertheless measures are needed to be taken to estimate the loss, and appropriate mitigation measures needed to be developed so as to minimize the loss.

- **Risk mitigation**

This is the set of measures that are needed to minimize due to happening of the risk. An example of mitigation measures is the positioning of fire extinguishers at visible places in an organization.

- **Security policy**

This is the policy that is formulated by the organization to implement information security in the organization. It includes defining security policies in terms of password management, access permissions to individuals, read, and write permissions, and the like.

The figure 4.4 depicts the various definitions which are applicable to the information security system.

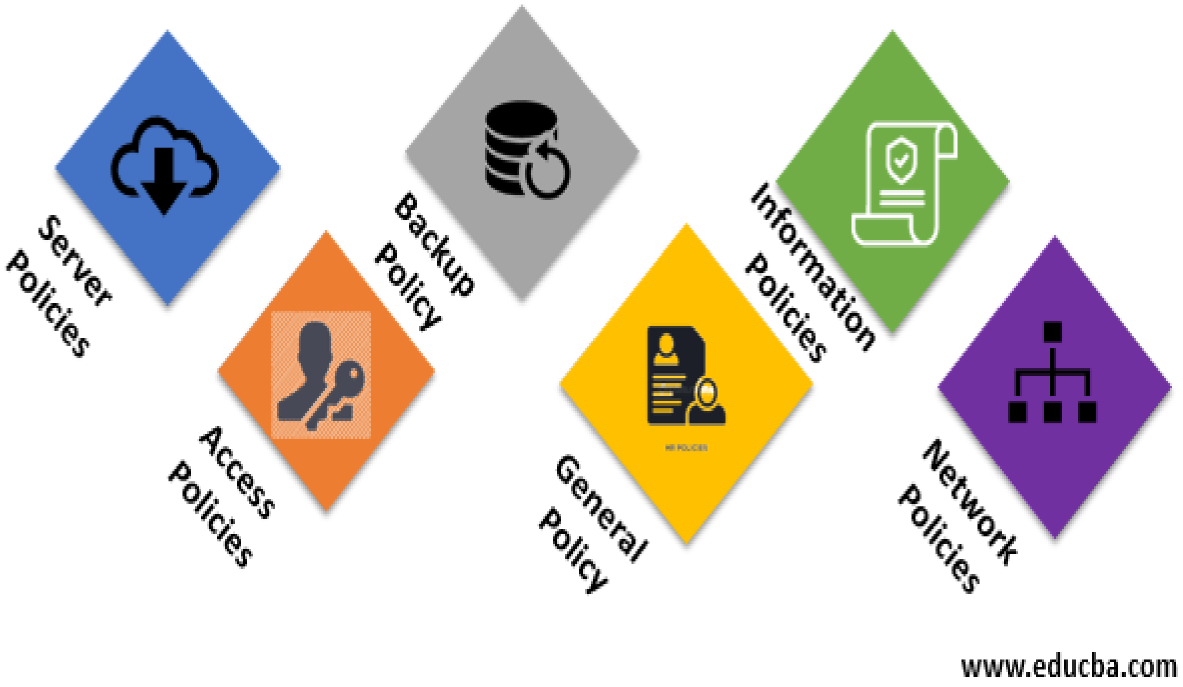


Figure 4.4 : Security policy

1. Policy on Information Security
This high-level document describes the organization's whole information asset security strategy. It contains goals, a scope, and roles and duties and forms the basis for all other security policies.

2. Access Control Policy outlines the steps involved in giving and removing access to data and information systems. To guarantee that only those with permission can access sensitive data, it incorporates user authentication, authorization, and accountability mechanisms.

3. The organization's Acceptable Use Policy (AUP) outlines what conduct is appropriate and inappropriate when utilizing its information systems and resources. This policy aids in preventing improper use of IT assets.

4. Data Protection Policy Describes how sensitive and personal information is gathered, stored, processed, and safeguarded by the company. It guarantees adherence to data protection regulations such as GDPR or CCPA.

5. Policy for Incident Response
Outlines the steps involved in locating, handling, and recovering from security incidents. It contains procedures for handling the incident response team, communicating with stakeholders, and reporting incidents.

6. Password Policy Specifies how strong passwords must be created and maintained, ncluding how they must be difficult, expire, and be handled to prevent unwanted access.

7. Remote Access Policy outlines the security precautions to be taken while gaining remote access to the company's systems and network. It covers secure communication techniques, remote desktop protocols, and VPN use.

8. Email Security Policy outlines the guidelines for utilizing the company's email systems, along with precautions against the spread of viruses, spam, and phishing scams.

9. Mobile Device Policy: This policy addresses accessing organizational data and systems using mobile devices, like tablets and smartphones.

1.3 The need for Security Audits in Organization

In the previous sections, we have discussed the various terms and definitions which are applied to information system management and practices. In this section, we will discuss the need for security audits in organizations. The following point enumerate the need for conducting security audits in the organization.

- To determine the degree and the depth of compliance with the information security system

  This is the most important aspect which generates the need for conducting security audits in the organization. As mentioned earlier, today's organizations are heavily dependent on technology and the data generated through the operational processes, so there is an imperative need to secure the data. By carrying out the security audits, the degree and the depth determine the areas which require greater measures for implementing information security. In other words, the security audits provide a realistic picture of the compliance level of the security system in place. For example, in the case of net-banking operations, with the tokenization process now made mandatory greater security compliance is now observed. Earlier, data on credit and debit card details were leaked to unauthorized individuals. With tokenization, the card details are encrypted. Hence are secure. This aspect came to light only by conducting security audits
- To provide trust and confidence to the customers

  Security audits are designed to provide trust and confidence to the customers that their data is safe and secure. In other words, the customers must be assured that the card details and other information shared with the vendor are safe and secure
- To maintain market leadership

  Security audits assist the organization in maintaining market leadership. This means that it is through security audits an organization is able to determine what security measures are needed and how hackers are developing new and innovative ways to steal data. To maintain market leadership an organization must anticipate and develop new strategies for thwarting the attempts of hackers. Security audits provide the ground reality of the security in place as well as enable the organization to take proactive steps to maintain leadership in the market
- To enable the stakeholders about their duties and responsibilities toward security compliance

  A security audit is applicable to the entire organization. It is not confined to any one particular unit of the organization. This means that the various stakeholders need to be compliant enough with respect to their roles and responsibilities *for security can be breached at any point of contact* and security audits highlight the grey areas. let us take an example of what is being discussed in this context. Suppose say an organization has developed a security policy that the stakeholders should deposit their cell phones with the staff at the reception. Suppose a stakeholder deliberately or unconsciously takes his or her cell phone inside the building. This is a security breach. In this case, the staff members are trained to handle these incidents and what needs to be done. Should they report to an information security officer? Or the mobile be searched for confidential information of the company and that should be deleted? Should the cell phone be handed over after deleting the information? Or some monetary penalty be imposed?

Hence it is seen that the action will be taken over as per the security policy and that the various stakeholders know their roles and responsibility

- To determine the steps needed for scaling the security management practices when the business operations are expanded.

  This is another important aspect of conducting security audits. Today the demand for the business is to expand. This expansion can be in terms of product expansion, location expansion, or in terms of expansion beyond borders. A security audit provides an estimate of the quantum of work that needs to be generated so that the business expansion plans can seamlessly integrate with the implemented security system. The security system is not confined to information technology that is in terms of physical security also as it also has CC cameras which too generate data.
- To provide a degree of compliance to regulatory bodies

  The security audit demonstrates the degree of compliance to the regulatory bodies which have evolved over a period of time in terms of implementation of best security practices. Hence, any organization which has ISO 27001 compliant must conduct regular information security audits
- To prevent the organization from cyber-attacks by hackers

  This is the most important aspect of the need for conducting security audits. A strongly implemented information system provides adequate assurance that the system is secure enough to be breached by the hackers

The figure 4.5 provides a glimpse of the need for implementing security audits in organizations.

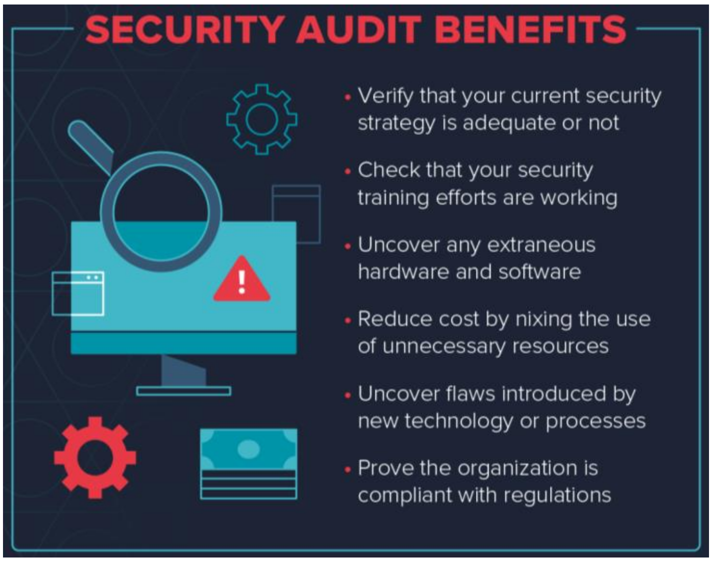

SECURITY AUDIT BENEFITS
• Verify that your current security strategy is adequate or not
• Check that your security training efforts are working
• Uncover any extraneous hardware and software
• Reduce cost by nixing the use of unnecessary resources
• Uncover flaws introduced by new technology or processes
• Prove the organization is compliant with regulations

Figure 4.5 : Security Audit Benefits

4.4 Organizational Roles and Responsibilities and Security Audits

In the previous sections, we discussed the role of security audits in an organization. In this section, we will discuss the various roles and responsibilities which an organization is required to demonstrate.

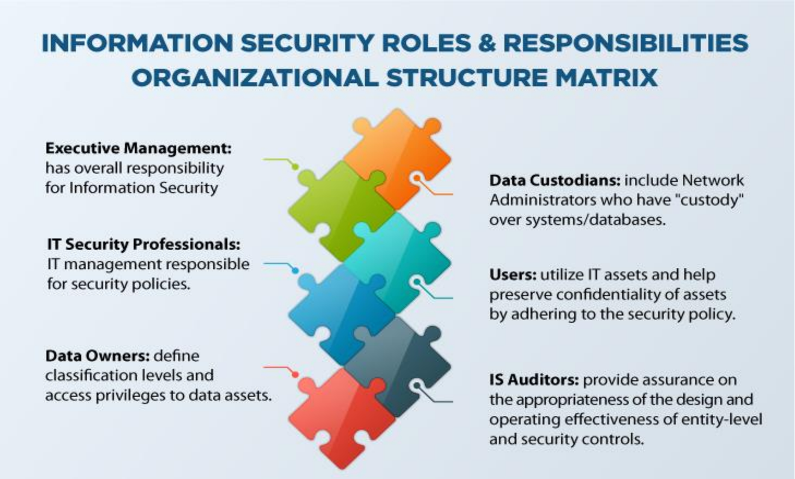
The following points demonstrate the roles and responsibilities of organizations toward security audits.

- Appointing the champion or the owner who will spearhead the security considerations in the organization.

  This is one of the most crucial aspects of the organizational security structure. The champion is generally given the title of Chief information security officer (CISO) or any other designation. This is the person who has the greatest responsibility for implementing the security system in place.
- Defining and implementing well-defined security requirements and organizational structure

  This is the most important function and responsibility of an organization wherein a proper and well-defined organizational structure must be in place first. In the absence of this most crucial aspect, the security system is bound to be a failure. The CISO is responsible for defining, altering, and appointing members of the department who will spearhead the security requirements of the organization,

Refer to the figure 4.6. From the figure, it is imperative that a well-defined structure must exist for effective and efficient security information in place.



INFORMATION SECURITY ROLES & RESPONSIBILITIES
ORGANIZATIONAL STRUCTURE MATRIX

Executive Management: has overall responsibility for Information Security

IT Security Professionals: IT management responsible for security policies.

Data Owners: define classification levels and access privileges to data assets.

Data Custodians: include Network Administrators who have "custody" over systems/databases.

Users: utilize IT assets and help preserve confidentiality of assets by adhering to the security policy.

IS Auditors: provide assurance on the appropriateness of the design and operating effectiveness of entity-level and security controls.

Figure 4.6 : Organizational Roles and Responsibilities and Security Audits

- Providing adequate resources and budget for the effective implementation of the security system in place

This is the most crucial point of consideration that must be taken into the decision-making process. In essence, this means that various resources must be made available to the information security department. Often it is seen that security implementation program fails due to a lack of financial resources as well as due to other resources and the constraints applied to the resource. For example, not releasing the auditors for carrying out security audits in the organization. The figure 4.7 depicts the roles and responsibilities of the organizations towards the implementation of the information security requirements.

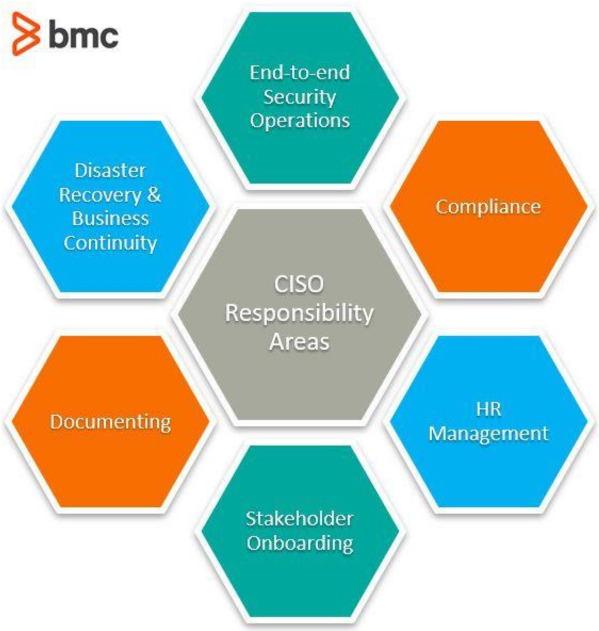

bmc
End-to-end Security Operations
Disaster Recovery & Business Continuity
Compliance
CISO Responsibility Areas
Documenting
HR Management
Stakeholder Onboarding

Figure 4.7 : Roles and responsibilities of the organizations

- Creating a documented structure for the information security requirements

Implementing a system in an organization depends on the well-established documented structure of an organization. In essence, this means that a system must be developed by the CISO and which is mandated by the Executive management must be converted into a document form. The mere fact that the documented structure exists sets the direction where the organization wants to move or go with respect to the security requirements.

The following are the contents of the documented information security system:

- **The security policy**

The security policy sets the direction of the organization in terms of the various measures that are required to be taken. *This security policy is approved by the Executive Management.* It is a signed document by the Chief of the organization. It is also reviewed periodically and is modified in accordance with the market dynamics.

- **The quality manual**

The quality manual is a document that provides a detailed macro-level outline of the various functional aspects of the security system in the organization. It is also reviewed periodically and is changed in accordance with the changes in the security documentation

- **The processes**

The process is the fluid that drives the security functions of the organizations. In general, the following are some of the processes for the security implementation

        - Process for conducting a security audit
        - Processes for incident reporting
        - Processes for database security handling
        - Processes for password implementation
        - Processes for training internal auditors

- The procedures

  The procedures are step-by-step instructions for executing the processes. The procedures provide detailed instructions along with the responsibilities of the resources who will execute them.
- The checklist

  The checklist is the controlling mechanism for verifying the compliance of the security requirements of the implemented security system.
- The guidelines

  The guidelines are the assisting documents that are used by the stakeholders in carrying out security-related tasks such as incident reporting, the conduct of audits, and the like.
- The forms and templates

These are the standards that will enable the CISO to implement a security management system.

- Carrying out mock drills

This is one of the responsibilities which an organization must undertake wherein it is requested to carry out mock drills. This will enable the organization to understand the ground reality situations.

- Review of security audits

This is another important function of an organization wherein the executive management must review the security audits findings.

4.5 Auditors' Responsibility in Security Audits

We have been discussing the various roles and responsibilities of the organizations towards the implementation of the security management system. However, one crucial aspect of security management systems is the role of the auditors.

Worth mentioning is the fact that it is the auditors who ensure the degree of compliance of the information security components in the organizations.

Worth mentioning is the fact that *auditors are of various types.* This means that depending upon the function the auditors are classified. However, we have internal auditors and External Auditors.

- The internal auditors are the members of the organizations who have been trained to carry out auditing tasks.
- The external auditors are the auditors who are trained to carry out third-party audits and they are responsible for leading the team to certify that the organization is meeting the requirements of certifying bodies such as ISO 27001.
- Apart from this basic classification, we have auditors who are experts in their field of operations. This includes aspects such as database auditors, cyberspace auditors, and the like.

The figures given below depict the roles and responsibilities depending on the type of auditors that are there in the organizations.

Let us now discuss some of the roles and responsibilities of the various types of auditors.

External auditors

The following points enumerate the roles and responsibilities of external auditors.

- The external audits are conducted by the lead assessor. He is responsible for developing the audit plan, developing the scope of the audit, and the other aspects necessary for carrying out the audit.
- The audits are required to be conducted within a fixed time frame. Generally, the audit lasts for 3 days
- The scope of the external audit is at the macro level of the organization. Hence the auditors are required to study security-related documentation structure
- Further, the main role and responsibility of external auditors are to carry out our related activities within the scope of the audit process. In other words, the auditors are required not to venture out of their defined scope though they are permitted to objectively evaluate the data generated by the system *even if it means that they are going out of the scope of the audit process.* Let us take an example. Suppose an auditor is required to carry out an audit of product development databases. This may

involve objectively verifying the data from the HR database also *even though this is not under the scope of the auditor*.

- The auditors are responsible for documenting the non-conformities in accordance with the defined processes and procedures as well as clearly mentioning the clause of the standard which is failing to meet the criterion
- The lead assessor must prepare a report of the findings and share it with the senior management of the organization (Figure 4.8)

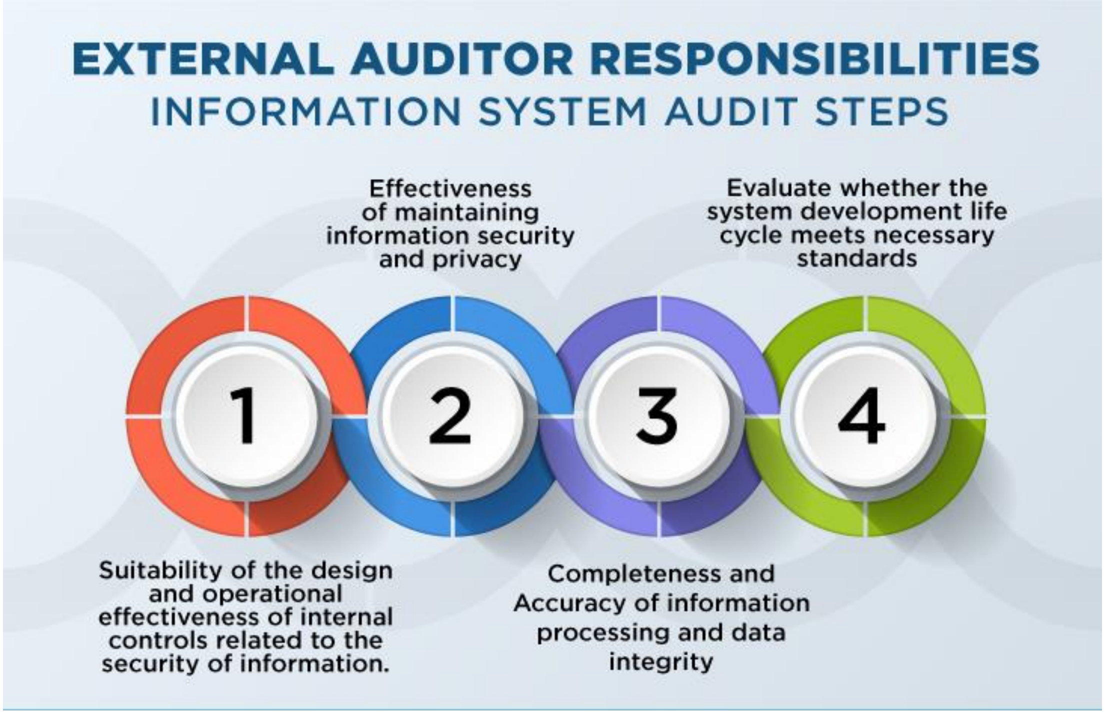

EXTERNAL AUDITOR RESPONSIBILITIES
INFORMATION SYSTEM AUDIT STEPS
Effectiveness of maintaining information security and privacy
Evaluate whether the system development life cycle meets necessary standards
1
2
3
4
Suitability of the design and operational effectiveness of internal controls related to the security of information.
Completeness and Accuracy of information processing and data integrity

Figure 4.8 : External auditors responsibilities

The internal auditor

As mentioned above the internal auditors are the members of the organization who are entrusted with the task of ensuring and verifying compliance with the implemented security management process.

The following points highlight some of the roles and responsibilities of internal auditors.

- The internal auditors need to exercise conduct the audit as per the internal quality audit plan prepared by CISO.
- The auditors are required to ensure that the findings are documented against the established procedures and the clauses.
- The auditors are required to be trained and re-trained depending on the changes implemented by CISO from time to and also depending on the market dynamics.

- The internal auditors are required to upkeep the technical knowledge so as to determine the loops that exist in the implemented system.
- The internal auditors are required to objectively evaluate the compliance.
- They are required to adopt ethical practices and standards in the execution of tasks.
- The auditors are required to conduct regular meetings amongst themselves and discuss the new and innovative security measures which can be implemented in the organization.
- The auditors are required to be vigilant at all times and must be capable enough to handle various incidents which can pose information security risks (Figure 4.9).

REPORT
Internal Auditor (IA)
[in-ˈtər-nᵊl ˈȯ-də-tər]
A trained professional employed by companies to provide independent and objective evaluations of financial and operational business activities, including corporate governance.

Figure 4.9 : Internal auditor

Security Auditor Job Description:

Job Summary: The Security Auditor is in charge of evaluating the information security procedures in place at the company and making sure they are in compliance with all applicable laws and standards. This position entails carrying out security audits, spotting weaknesses, and suggesting fixes to improve the organization's security posture.

Primary Accountabilities:

Perform audits on security:

Conduct thorough and frequent audits of the company's networks, information systems, and procedures to find gaps and vulnerabilities in security.

Analyze how well the current security procedures and controls are working.

Evaluation of Compliance:

Evaluate whether the company complies with all applicable laws, industry standards, and internal security regulations, including ISO 27001, GDPR, HIPAA, and others.

Create and preserve thorough reports that outline the state of compliance and potential improvement areas.

Analyzing Risk:

Determine possible security threats and evaluate the organization's exposure to them.

Create plans for mitigating risks and suggest improvements to security.

Review of Policies and Procedures:

Examine and assess whether the organization's security policies, practices, and standards are sufficient.

Make updates and enhancement suggestions to guarantee that policies are up to date and functional.

Reaction to an Incident:

Take part in the examination of security breaches and incidents.

Make suggestions for enhancing incident response protocols and averting upcoming mishaps.

Record-keeping and Reporting:

Prepare audit reports, record audit results, and deliver findings to management.

Monitor and document the application of suggested security precautions and remedial steps.

Awareness of Security:

Participate in the creation and execution of employee security awareness training programs.

Encourage a secure atmosphere inside the company.

Working together:

Collaborate closely with IT, legal, compliance, and other pertinent departments to guarantee a unified security strategy.

Teams should receive direction and assistance on security best practices and compliance needs.

Qualifications:

Learning:

a bachelor's degree in cybersecurity, information technology, computer science, or a similar discipline.

Professional certificates are widely sought after, including Certified Ethical Hacker (CEH), Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), and others.

Experience

a track record of success in security auditing or related roles.

thorough understanding of information security procedures, technology, and principles.

knowledge of security frameworks and standards (e.g., PCI DSS, NIST, ISO 27001).

Proficiency:

strong ability to analyze and solve problems.

Proficient in recognizing and recording security vulnerabilities and paying close attention to details. strong communication skills, both in writing and speaking. the capacity to function both alone and together.

Chief Information Security officer (CISO)

As mentioned the CISO is the key personnel for implementing a security management system in an organization. The CISO is also an auditor hence it has a very special role to play

The following points enumerate the roles and responsibilities of the CISO

- The CISO is responsible for developing the audit strategy of the organization
- The CISO is responsible for ensuring that the internal auditors are trained and that they are capable enough to conduct the audits
- The CISO is also responsible for developing the internal audit plan, and the functional audit plan and ensuring that it is conducted in accordance with the plan.
- The CISO is also responsible for studying the various reports, logs, and other findings arising out of operational processes which are potential threats and risks to the organizations
- The CISO is also responsible for the constant upgrading of knowledge and the industry standards which are being followed by other competitors (Figure 4.10).

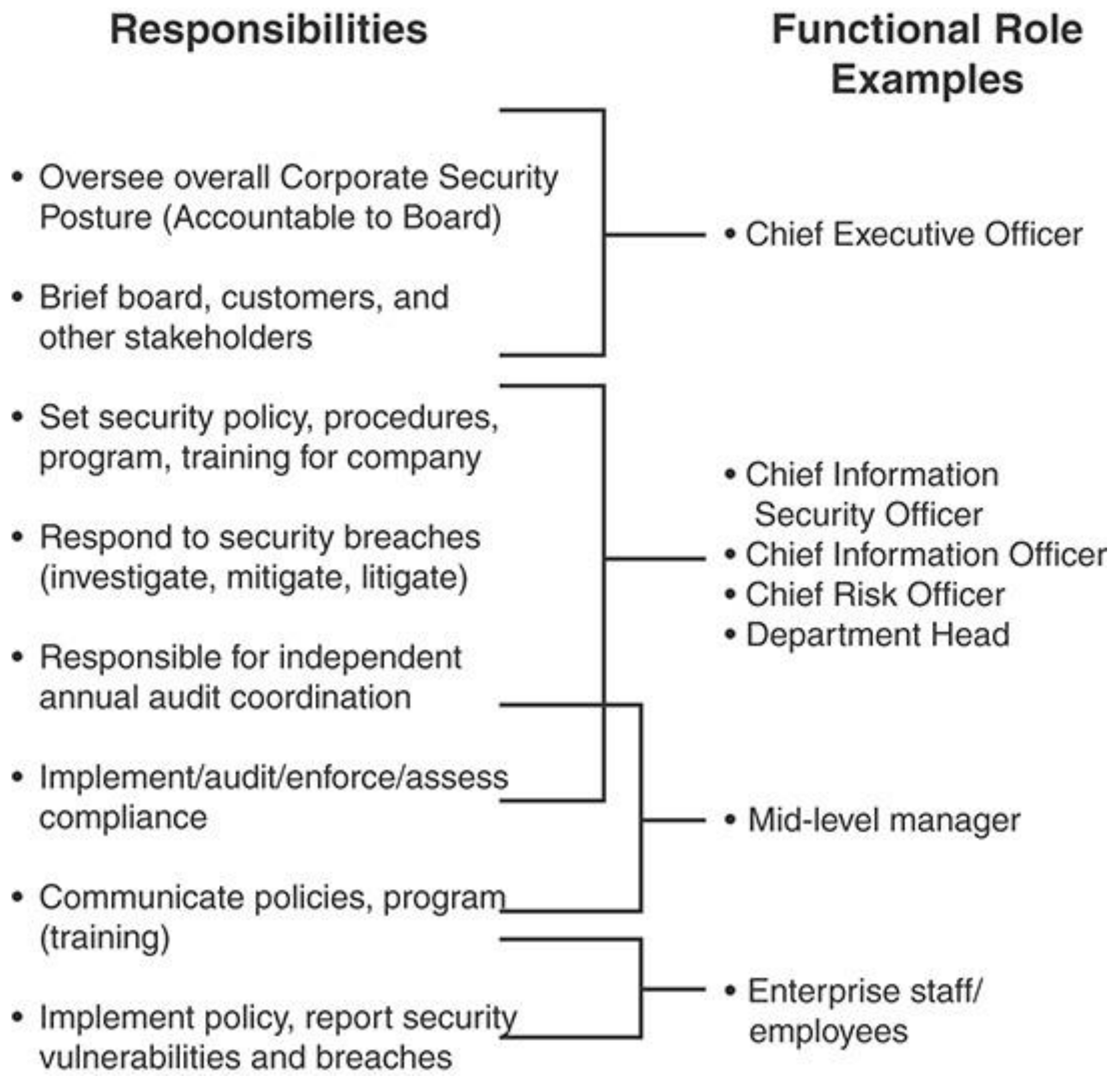

Responsibilities
Functional Role Examples
• Oversee overall Corporate Security Posture (Accountable to Board)
• Brief board, customers, and other stakeholders
• Set security policy, procedures, program, training for company
• Respond to security breaches (investigate, mitigate, litigate)
• Responsible for independent annual audit coordination
• Implement/audit/enforce/assess compliance
• Communicate policies, program (training)
• Implement policy, report security vulnerabilities and breaches
• Chief Executive Officer
• Chief Information Security Officer
• Chief Information Officer
• Chief Risk Officer
• Department Head
• Mid-level manager
• Enterprise staff/ employees

Figure 4.10 : Roles and responsibilities of Chief Information Security officer (CISO)

- **Knowledge Check 1**

  Fill in the Blanks.

  1 The full form of ISMS is _____________.

  2 The security policy deals with _____________.

  3 A Security audit must be a __________ audit.

  4 A security audit deals with ________ and ___________.

  5 Auditors are required to be _____________ in security audits.

- **Outcome-Based Activity 1**

Prepare an Excel sheet by taking an example of the university/institute where you are studying. Identify the components of the system which are required to be protected from the perspective of information security and the type of security that needs to be deployed on them.

4.6 Types of Security Audits

From the above discussions, we have covered the various aspects of the information security system. Let us discuss another important aspect that needs to be taken up in this unit.

The discussion pertains to the types of security audits. Worth mentioning is the fact that security audits are classified according to the purpose and the functioning of the business units. This means that an organization may have a functional security audit or it may technical security audit or it may have software related security audits.

The figures given below depict the various types of security audits which are normally conducted in an organization.

Functional security audit

These are the audits that are conducted on a particular function that is being executed in the business processes. This audit needs to be conducted very carefully *due to the fact that it cannot be detected easily and it does harm the organization* profoundly leading to financial loss and other forms of losses. An example of a functional audit is the Railway reservation system catered by IRCTC during the last 6 years or so. It was found that a hacker had developed software that would capture the server and at the backend, it provided reservations to people who have paid huge amounts of money to get the confirmed reservation whereas the genuine persons were deprived when the system was thrown open to the people at 8:00 am in the morning. This was revealed during functional audits (Figure 4.11 & 4.12).

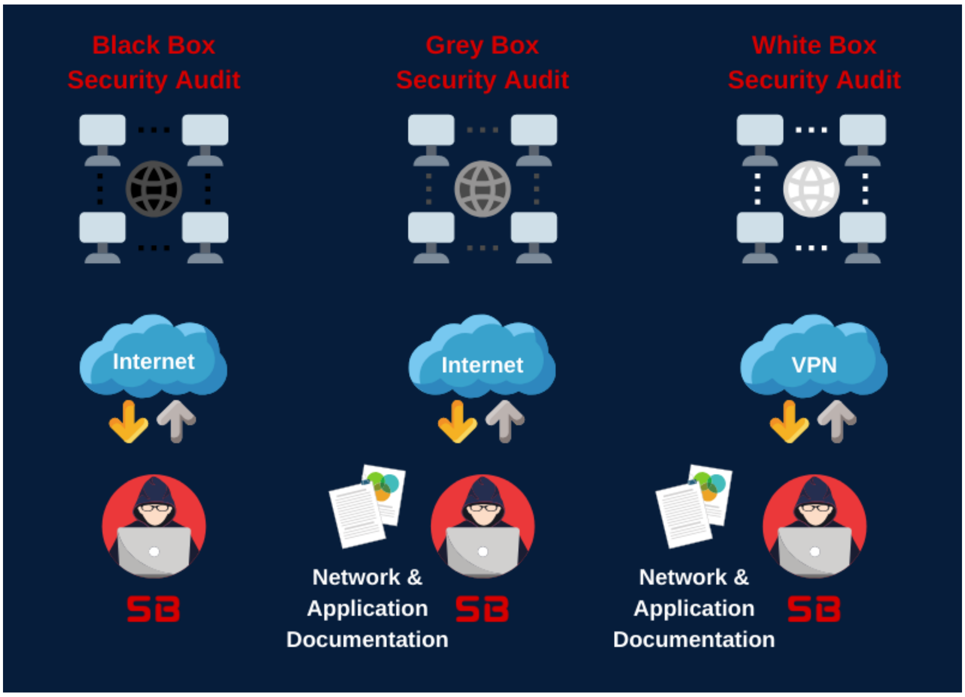


Figure 4.11 : Functional security audit

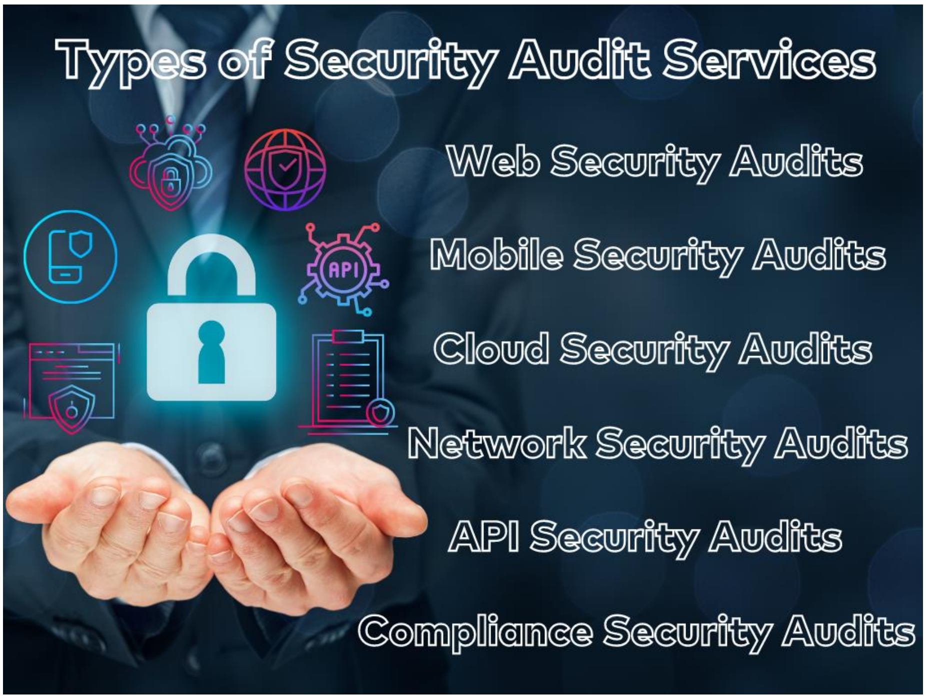


Figure 4.12 : Functional security audit

API security Audits

These are the audits that are conducted on the APIs that application programming interfaces. These are the set of specific data which is needed to be passed from one interface to another interface through a gateway.

The audit is conducted at the gateway to determine whether the correct data is being passed or not.

- **Knowledge Check 2**

  State True or False

  1. Information Security audits are confined to databases only (True / False)
  2. Security audits are to be carried out by trained auditors only (True / False)
  3. There is no role of the organization in the conduct of information security only (True / False)
  4. The data and the information is the same (True / False)
  5. Information security policy is a must for every organization (True / False)

- **Outcome-Based Activity 2**

Prepare an example of a company for which the information security audit is due. You are required to prepare an audit plan for the company clearly highlighting the important components of the audit process.

4.7 Summary

- The commercial world of today is highly dependent on information and data.
- This is due to the fact that Information Technology is highly driving business processes.
- These business processes are generating a large amount of data and information.
- This information or the data is needed to be protected or secured.
- If this information remains unprotected or secured it is susceptible to being exploited by competitors.
- The competitors may use the information to serve their own interests.
- Hence organizations today are putting extra effort to ensure that the information is protected and remains secured.
- However, in the information technology domain, nothing is secured and hackers are always looking out for means mechanisms to exploit the loopholes in the security system.
- For example, the hackers recently exploited the security system of All India Institute of Medical Sciences by taking control of the patient records and freezing the

computing system. They threatened to destroy the information unless a ransom is paid to them. In other words, the patient records contained information that was exploited due to loopholes in the prevention process of the patient records.

- There have been several instances such as fraudulent monetary transactions and stealing confidential information and the like.
- Hence the role of the organization becomes all the more profound.
- They need to identify, develop and implement a sound and secure information system which will protect the data of the customers from being exploited such as money being siphoned off to unintended users and the like.
- The organizations must develop security policies, conduct security audits and regularly update the security procedures.
- One of the means and mechanisms for this is to conduct regular security audits.
- For this, a pool of individuals must be trained to conduct these security audits.
- Every security audit must be planned and executed in a manner as per the plan.
- Depending on the purpose there are various types of security audits.
- There is a first-party audit wherein the organization conducts the audit through its own trained internal audits.
- There is a second-party audit wherein the organization verifies and validates the system based on the commitments made by the vendors.
- There is a third-party audit wherein the audit is conducted by an external agency.

4.8 Self-Assessment Questions

- What is information and information Security? Explain with examples.
- What is the need for auditing information systems? Explain with examples.
- What is the role of an organization in implementing information security? Explain with examples.
- What is the role of auditors in the conduct of information security audits? Explain briefly.
- What are the various types of security audits? Explain briefly.

4.9 References

- Vroom, C., & Von Solms, R. (2004). Towards information security behavioral compliance. Computers & Security, 23(3), 191-198.
- Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. Managerial Auditing Journal.
- Suduc, A. M., Bîzoi, M., & Filip, F. G. (2010). Audit for information systems security. Informatica Economica, 14(1), 43.
- Yen, J. C., Lim, J. H., Wang, T., & Hsu, C. (2018). The impact of audit firms' characteristics on audit fees following information security breaches. Journal of Accounting and Public Policy, 37(6), 489-507.
- Tipton, H. F., & Krause, M. (2007). Information security management handbook. CRC press.
- Ryoo, J., Rizvi, S., Aiken, W., & Kissell, J. (2013). Cloud security auditing: challenges and emerging approaches. IEEE Security & Privacy, 12(6), 68-74.
- Hamdan, M. N. M. (2017). The Relationship between Network Security Policies and Audit Evidence Documentation: The Accounting Information Security Culture as a Mediator. International Journal of Business and Management, 12(12), 168-180.
- Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An introduction to information security. NIST special publication, 800(12), 101.
- Popescu, G., Popescu, V. A., & Popescu, C. R. (2007). Information systems security audit. Manager Journal, 6(1), 81-88.

Unit : 5

Approaches to Audits

Learning Outcomes:

- Students will be able to understand the various approaches to conducting security audits.
- Students will be exposed to various technology-based security audits.
- Students will be made aware of vulnerability testing and penetrating processes that are usedin security testing.
- Students will be exposed to issues and challenges in the process of conducting security audits.
- Students will be exposed process of selecting external consultations and the budgetary issuesand challenges involved in the process of selecting external consultants.

Structure

5.1 Introduction

In the previous unit, we covered the various features pertaining to security audits. In particular, we discovered the entire audit process. However, when it comes to the process of conducting audits, we are left with a dilemma. The prime reason for the generation of the dilemma is the fact that the ambit of the security audit is large. This means that there are several aspects that need to be taken care of with respect to the audit span, the domain of the audit the applicability of the audit standards, and the like.

Refer to the figure 5.1. This figure is covering just one aspect of what is being discussed here.

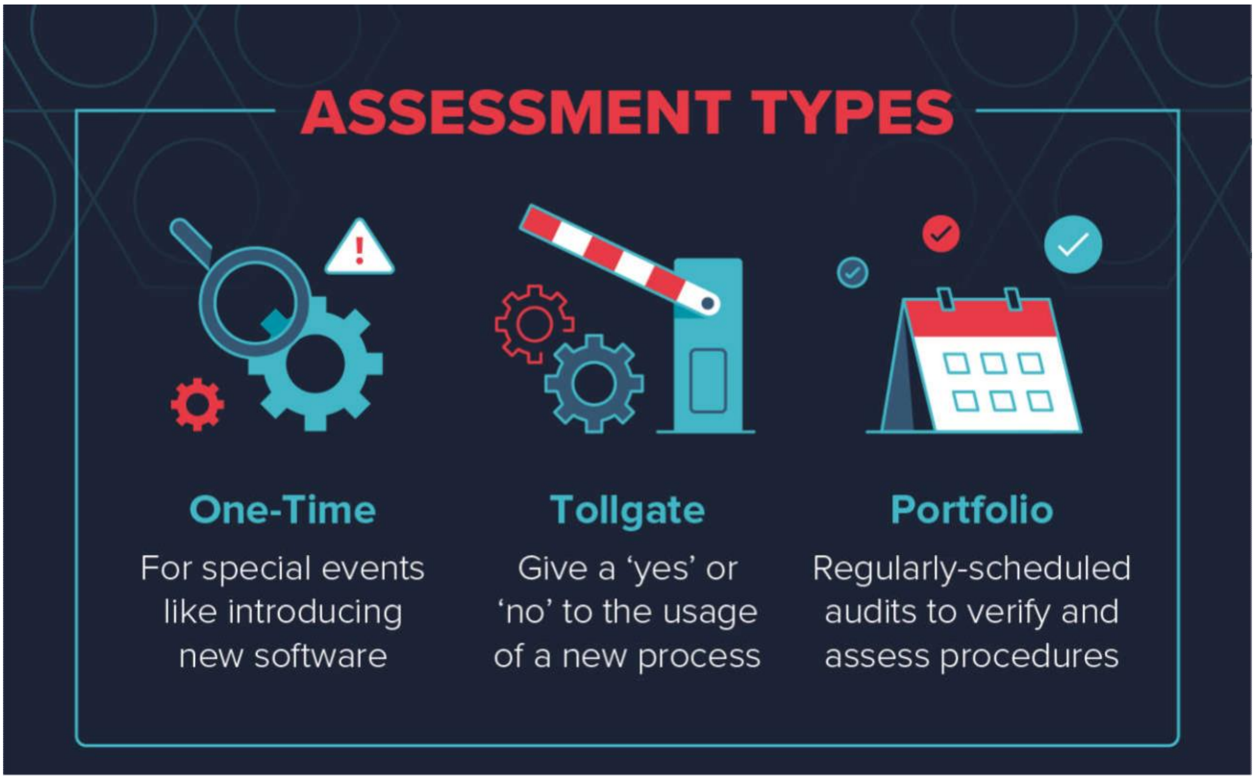

ASSESSMENT TYPES
One-Time
For special events like introducing new software
Tollgate
Give a 'yes' or 'no' to the usage of a new process
Portfolio
Regularly-scheduled audits to verify and assess procedures

Figure 5.1: Assessment Types

From the figure, it is clear that there are various types of audits. Apart from the type of audits, there are other types of audits such as security audits of the network, security audits of devices, and the like.

The figure 5.2 depicts various types of security audits which are needed to be carried out from the perspective of providing security in the organization.

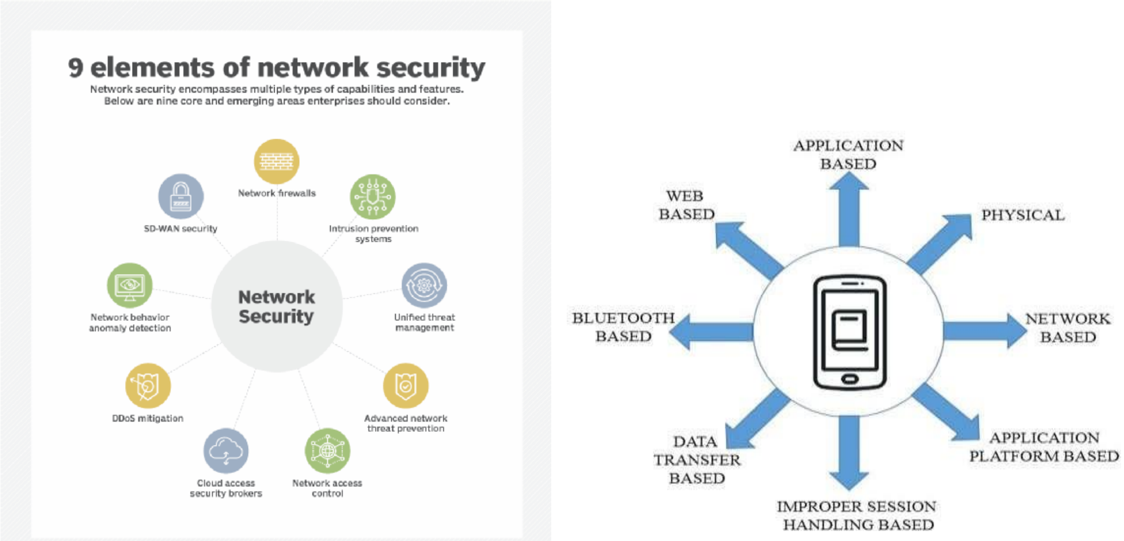

9 elements of network security
Network security encompasses multiple types of capabilities and features.
Below are nine core and emerging areas enterprises should consider.
Network firewalls
SD-WAN security
Intrusion prevention systems
Network Security
Network behavior anomaly detection
Unified threat management
DDoS mitigation
Advanced network threat prevention
Cloud access security brokers
Network access control
APPLICATION BASED
WEB BASED
PHYSICAL
BLUETOOTH BASED
NETWORK BASED
DATA TRANSFER BASED
APPLICATION PLATFORM BASED
IMPROPER SESSION HANDLING BASED

Figure 5.2: Types of security audits

Thus it is evident that when an organization goes in for security audits, one needs to determine the approach to be adopted and this is dependent on the type of audit which is required to be carried out.

Let us take an example of what is being discussed here. Suppose we want to go into network security audit then we must adopt the approach of top-down audit procedures or the methodology while in the case of smartphone security audits of hardware devices we must start with the bottom approach.

Further, it is not only the top-down or bottom-up approach we may have other approaches also. For example, in the case of smartphone devices, we may security audit of the installed apps in the device or we may have a tokenization approach to security audits of payment Apps such as Paytm and the like.

On the other hand, we may conduct audits for replicating worms or adware or any other functional testing.

The next section discusses the various approaches to audits.

5.2 Approaches to Audits

In the previous section, we discussed that security audits need a process-driven approach. In thissection, we discuss some of the approaches to performing security audits.

A security audit needs is a vital component of any organization. Hence we need a systematicapproach to executing security audits.

The following points enumerate the points of consideration that need to be taken care of while defining or determining the approach to be taken.

The business domain and the quantum of the business processes which are being executed in the organization

This is the most important step in the process of determining the approach to be adopted. This essentially boils down to the fact that the business domain of the organization and the business processes which are responsible for achieving business objectives are key drivers for determiningthe approach to be adopted for carrying out audits.

Let us take an example of what is being discussed here. Suppose that a business unit like Paytm or the recent banking examples such as neo banks. These are the business units which are dealingin the finance domain which is where transactions are related to money. This is a very high-risk domain and as such, it needs an approach wherein the audit process must be effective, and efficient and has undergone each and every process that deals with the transference of money from one party to another party. Hence the audits have to be rigorous and must be evaluated fromvarious perspectives *as hackers are always looking out for grey areas wherein they can conduct illegal activities wherein the money can be siphoned off easily.* On the other hand, if theorganization is into logistics or transportation business then a different approach needs to be carried out for conducting security audits.

The audit approach is dependent on the degree and depth of the risk involved in the business processes

This is also one of the crucial aspects which warrant the decision to be undertaken for the approach to be adopted in the audit process. It is to be mentioned that the business houses which are in the financial domain have the greatest risk factor attached to them and hence the audit approach is to be different from other types of business units that are not in the financial domain.Also, the institutes of repute or of national security are also under great risk and hence need a different approach to security audits. For example, take the recent case of the All India Institute of Medical Sciences server has hacked as it is an institute of repute while there have been several incidents wherein the security of the government offices dealing in national security has been compromised.

The above points highlight the criterion that needs to be undertaken and which will provide the approach to the audit process.

Once the criterion is set, then the following are deciding criteria that need to be undertaken for the approach to the audit process.

The following points enumerate the various approaches which are taken for the conduct of the audit process after the above key points of consideration have been taken into the account. Theseare from the perspectives of planning for the conduct of the audit process.

The adoption of the top-down approach

This is the approach which is needed to be adopted when the security audit is required to be conducted from the perspective of the functioning of the entire organization or the business units. It may also be conducted whenever there has been a large-scale security breach. Normally certification agencies or the bodies such as ISO 27001, BS 7792, etc. conduct a top-down approach and it lasts for approximately 4 to 5 days. This is not fixed as it is based on the businessprocesses and the domain in which the business is operating.

On the other hand, this approach is adopted whenever the organization's functioning is stopped altogether due to virus attacks or ransomware. If this is the case then the purpose of the top-downapproach is to determine the degree and the depth of the damage caused as well as to determine the corrective and preventive actions which are needed to be implemented so that these types of attacks are not carried out in the future.

An example of the top-down approach is the adoption of the tactics involved in the process of taking control of the crucial servers of the All India Institute of Medical Sciences by cyber hackers. In such a scenario the entire functioning came to a halt.

In similar parlance, the audit process begins at the main server and cascades down to the minor servers. In other words, the security audit processes are executed in a waterfall-like structure wherein the linkages to the subsequent layers are evaluated so as to determine the crucial grey areas which can be exploited.

The bottom-up approach

The bottom-up approach is the opposite approach to the top-down approach. In this type of audit approach, the process commences at the grass root level and moves upwards to the main level. Again the main purpose of this type of approach is to walk down the linked components so that they can be evaluated with respect to the security breaches.

An example of the bottom-up approach is the process of audit which starts with a simple laptop and determines the security loopholes in the laptop and then proceeds to the network whereinthis laptop is linked until it reaches the point wherein security issues do not possess much of the threat.

The staged approach

In the staged approach of the audit process, the stages are defined based on the priorities arising out of the risk score. Based on the high risk-to-risk profile scores the stages are defined and the security audits are conducted accordingly.

An example of the staged approach is the conduct of security audits for a bank having branches across the country. Here the staged approach may be in the form of a regional branch followed by the main branch followed by the head office. In other words, the stages are defined in theform of the region from main to head office.

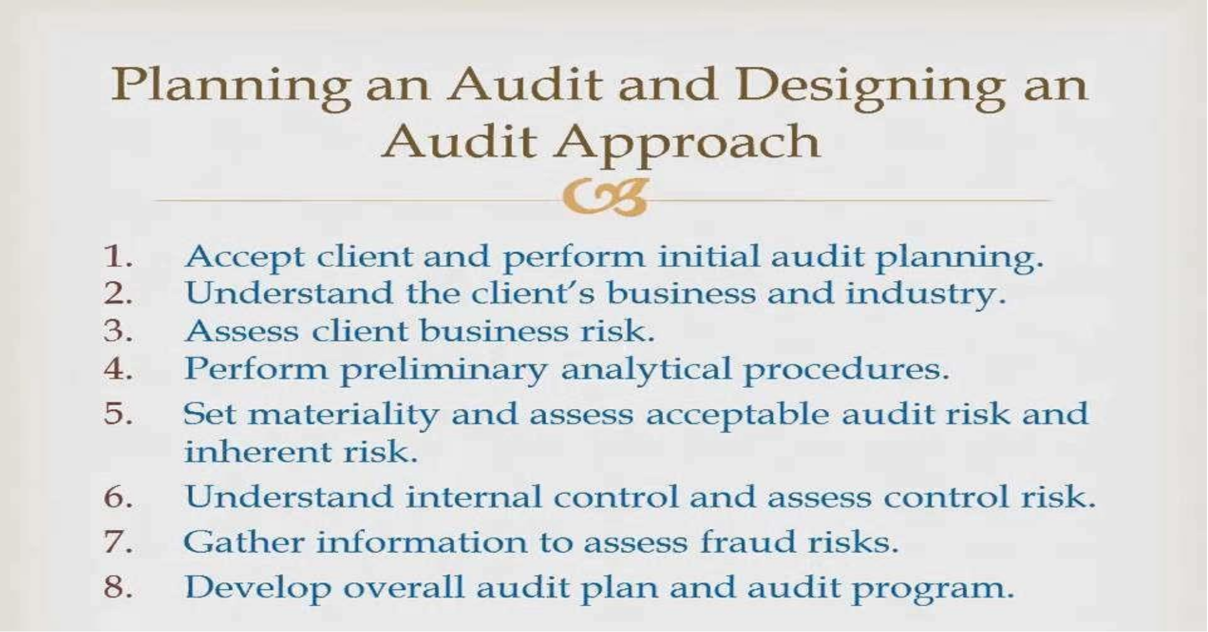
The phase-wise approach

The phase-wise approach is the form of the security audit process wherein the phases are defined in a manner that meets the business objectives of the audit process. For example, phase 1 may include the northern region security audits of banks, while phase two may include the security audits of the western region.

Worth mentioning is the fact that the phase and the stage-wise approach are dependent on many factors such as business operations, the priority of the branches, and the like.

The figure 5.3 depicts the visual pertaining to *one aspect of the audit processes.*

Figure 5.3: Planning an Audit and Designing an Audit Approach

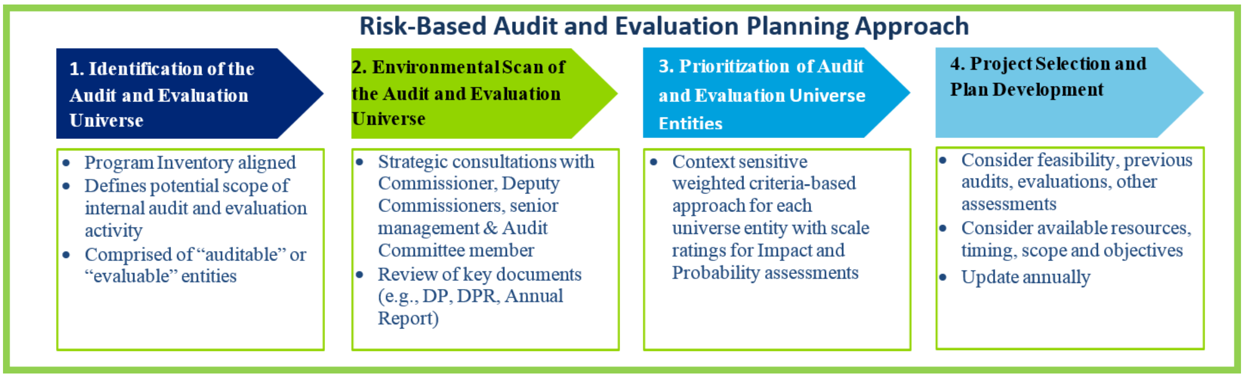


Planning an Audit and Designing an Audit Approach

1. Accept client and perform initial audit planning.
2. Understand the client's business and industry.
3. Assess client business risk.
4. Perform preliminary analytical procedures.
5. Set materiality and assess acceptable audit risk and inherent risk.
6. Understand internal control and assess control risk.
7. Gather information to assess fraud risks.
8. Develop overall audit plan and audit program.

The above figure depicts one of the approaches which is adopted for conducting the security audit process.

Refer to the figure 5.4. The figure depicts another approach to the security audit process



Risk-Based Audit and Evaluation Planning Approach

1. Identification of the Audit and Evaluation Universe
- Program Inventory aligned
- Defines potential scope of internal audit and evaluation activity
- Comprised of "auditable" or "evaluable" entities

2. Environmental Scan of the Audit and Evaluation Universe
- Strategic consultations with Commissioner, Deputy Commissioners, senior management & Audit Committee member
- Review of key documents (e.g., DP, DPR, Annual Report)

3. Prioritization of Audit and Evaluation Universe Entities
- Context sensitive weighted criteria-based approach for each universe entity with scale ratings for Impact and Probability assessments

4. Project Selection and Plan Development
- Consider feasibility, previous audits, evaluations, other assessments
- Consider available resources, timing, scope and objectives
- Update annually

Figure 5.4: Risk-Based Audit and Evaluation Planning Approach

From the figure, it is seen that the approach adopted is based on a risk assessment which is the vulnerability of the system. In other words, the focus of the audit process is to determine the vulnerable points in the information security management system that pose a risk and hence are susceptible to exploitation by hackers.

Apart from the above approaches, there are other approaches that are generally adopted. The following points enumerate the approaches which are generally adopted.

A parallel approach to the audit process

This is the approach that is adopted in case the business units have several offices of units across the geographical location and the security management system works on concurrent systems. For example, if the user in the New Delhi office is raising an invoice and simultaneously another user in the Chennai office is also raising the invoice for the same client then whether the system behaves in a risk-free manner or not meaning that the system is vulnerable or not. Another example of the parallel approach to the audit process includes the withdrawal of money simultaneously at the same time and noting whether the records are updated simultaneously or not.

The serial approach of the audit process

This is the approach that is adopted when the output of one system forms and input to another system and the audit process validates that this is actually happening. An example of thisapproach is the withdrawal of money from the ATM machine wherein now the feature has been introduced in the ATM machines wherein the money is not retracted back if it is not taken or is left over. Earlier the provision for retraction was an inbuilt feature of ATM machines and this was exploited. Hence the serial concept was introduced wherein there is no provision for retraction in machines.

5.3 Technology based audits, Vulnerability Scanning, and Penetrating Testing

In the previous section, we discussed the various approaches to audits. In this section, we discusstechnology-based audits.

In simple parlance, the term technology-based audits refer to the usage of tools to determine the preparedness of the organization in terms of the software and hardware usage and deployment for executing the business processes. The data generated by this hardware and software is used asobjective evidence and accordingly, corrective and preventive actions are taken.

Let us take an example to illustrate the concept of technology-based audits. Suppose an e-commerce business unit such as Flipkart. The entire business of Flipkart is executed on the internet. For this purpose, the Flipkart business comprises several servers stored at distributed locations for security reasons as well as operational reasons. Also, the entire website which is what we observe in the browser, along with other associated files are stored on the servers. Further, there are routers, hubs, and switching pairs for providing the network. Thus, the security audit will make examine the logs of these devices and based on the documented system will examine the data and determine the grey areas which are susceptible to security risks.

This is not possible to carry out the audit of these devices and software manually including the orders placed by the customers. Hence technology-based tools are deployed for studying the dataobjective data from these operational processes.

For example, Opmanager is a complete technology-based tool that is used for monitoring network traffic that is assessing the behavior of users *who with intention try to slow down the network by running several processes simultaneously.*

The following is the list of some of the ways wherein security can be comprised when the business is running on the internet.

Data center management

For a business unit running over the internet, data center management is the crucial component of the information security system. Hence it needs to be ensured that it is protected at *any cost.*

Mobile application

Nowadays mobile is an essential component of business operations as users are always carrying it around. Hence, security issues can arise if adequate security measures are not provided in mobile applications. Technology-based audits ensure that the security concepts are well in place in the case of mobile-based applications.

Multi-site and remote operation

Nowadays due to security and operational issues software deployment is carried out at several distributed places. Hence security can arise at any location and at any remote place and hence there is a need for implementing strong security measures in place.

Firewall analyzer

A firewall is a protection device for the router and hence it is also susceptible to security breaches.

Vulnerability testing and penetration testing

We have discussed the basic concepts of technology-based tools. However, there are two concepts that are used in technology-based tools. These are vulnerability testing and penetration testing.

Let us try to understand these approaches.

Vulnerability testing is carried out to determine the flaws in the system. In other words, it is used to assess the weak points in the implemented system meaning that these are vulnerable pointsthat can be exploited.

Let us take an example of vulnerable points. Suppose that a user does not log out of the particular application as a habit. This becomes a vulnerable spot as a hacker may exploit the entry point through which he can do harm either from the port or from the firewall from the server *or from any other points such as networks, routers, sockets, and the like.*

On the hand, penetration testing is done to determine the vulnerabilities in the software system, malicious content, and flaws in the system. It is part of an ethical testing process.

Difference between vulnerability testing and penetration testing

Table: Difference between Vulnerability Testing and Penetration Testing

S.No.	Penetration Testing	Vulnerability Assessments
1.	This is meant for critical real-time systems.	This is meant for non-critical systems.
2.	This is ideal for physical environments and network architecture.	This is ideal for lab environments.
3.	It is non-intrusive, with documentation and environmental review and analysis.	Comprehensive analysis and thorough review of the target system and its environment.
4.	It cleans up the system and gives a final report.	Its attempts to mitigate or eliminate the potential vulnerabilities of valuable resources.
5.	It gathers targeted information and/or inspects the system.	It allocates quantifiable value and significance to the available resources.
6.	It tests sensitive data collection.	It discovers the potential threats to each resource.
7.	It determines the scope of an attack.	It makes a directory of assets and resources in a given system.
8.	The main focus is to discover unknown and exploitable weaknesses in normal business processes.	The main focus is to list known software vulnerabilities that could be exploited.
9.	It is a simulated cyberattack carried out by experienced ethical hackers in a well-defined and controlled environment.	It is an automated assessment performed with the help of automated tools.
10	This is a goal-oriented procedure that should be carried out in a controlled manner.	This cost-effective assessment method is often considered safe to perform.
11	It only identifies exploitable security vulnerabilities.	It identifies, categorizes and quantifies security vulnerabilities

From the above table, it is evident that the scope of both the testing is different. In the case of penetration testing, the scope is related to real-time critical applications while in the case of vulnerability testing it is not confined to mission-critical applications.

Refer to another figure 5.5:

This figure points out the similarities and differences between penetration testing and vulnerability assessment.

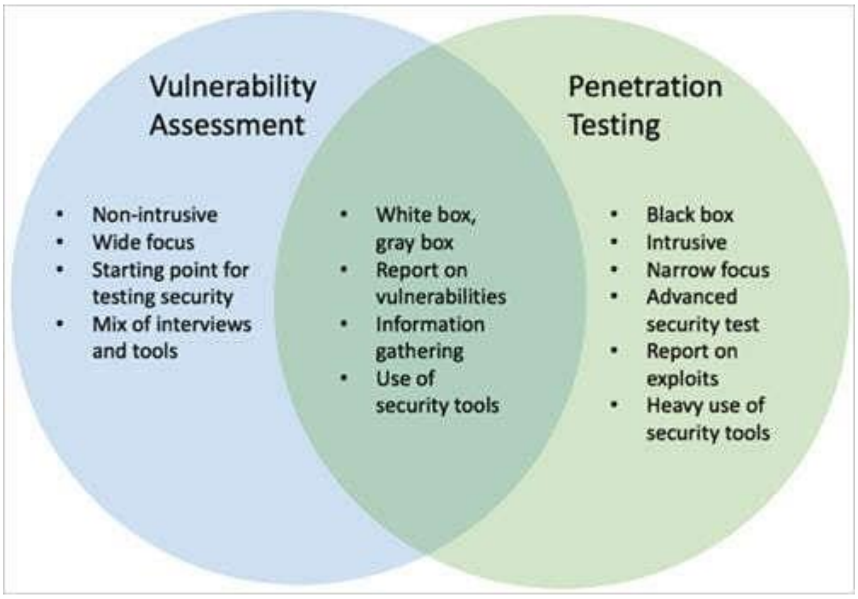


Figure 5.5: Differences Between Penetration Testing and Vulnerability Assessment

5.4 Resistance to security audits

In the previous sections, we discussed technology-based audits. However, implementing an information management system in an organization is always resisted. In other words, it is not aneasy task to implement an information security system in a business unit on account of the following factors which are enumerated in the points given below.

It is human nature to resist changes

Every change is bound to meet resistance. This is a fact that every business unit is aware of. Also, it is human nature to resist changes. However, it is also well known that the business units which have adopted changes have moved to the path of progress whereas the business units which have failed to adopt the changes have been forced to maintain a low profile. Only those organizations survive which are open to accepting changes.

A security audit is viewed as a fault-finding exercise

This is the main reason for the resistance to security audits in business units. The result of security audits is the highlighting of the grey areas in the system. This grey area is *perceived* or is viewed as a weakness of an individual *and if it is exposed and some penal action will be taken against an individual.* Thus, the audit process is resisted in many forms such as suppressing the data generated by the processes, giving evasive replies, and not cooperating with the auditors andother forms of evasive techniques.

Let us take an example of what is being discussed here. Suppose that during a security audit the session log file of the database shows some activities of an individual for which he has no access permissions. Now when this is being pointed out to the concerned individual, he or she will go into the defensive mode and will give evasive responses to the auditors or to the authorities. In other words, he or she is resisting the audit process as it is viewed as something which is negative or adverse.

- **A security audit brings in transparency and it is human nature to oppose transparency** Forming no system in business units to some form of well-established system brings inopposition from the stakeholders *as every system is seen as a constraint that limits theoperational areas and challenges the authority. Thus it is resisted.*

Let us take an example of what is being discussed here. Suppose that a biometric attendance system is installed in an organization. This will be resisted in the sense that the *luxury* of coming late, jotting down the wrong arrival time and leaving time and the like is curtailed *as the actual time is recorded in the system.* Also, proxy attendance will not work anymore in the organization.Every movement is now transparent.

A security audit is viewed as a time-wasting activity and thus it is resisted

The mature organizations wherein the processes are well-established stakeholders see this as a time waste of activity as they have been using it for a considerable length of time. On the other hand, the organizations which are immature blame the management for not releasing the funds for other development activities which they consider a necessity. Hence security audits are resisted.

A security audit is viewed as a measure to pull up the employees regarding their performance.

This is the most important reason for the resistance to the security audit. The prime reason is the fact that through audits the stakeholders feel that they are exposed and some punitive actions willbe taken against them. For example, it is through security audits the movement is tracked and if there is there are abnormal variations that may be genuine or intentional the boss may pull up theindividual for being late or for wasting time.

A security audit is viewed as a measure to encroach upon the authority and the responsibility of the stakeholders.

This is another important reason which is why the security audit is opposed. An audit brings out factual information and the stakeholders feel threatened by their lapses when they fail to do work as per the procedures due to constraints imposed by the management. Thus, whereas the management wants to bypass the procedures, the auditors want to evaluate the implementation ofthe information security management system as per the procedures hence the gap remains. This gap is viewed as a time-wasting activity for which there is no solution. Hence responsibility and authority are challenged

5.5 Phases in security audits, security audit engagement costs, and other aspects

We have been discussing the issues of information security audits. However, as mentioned conducting a security audit is a systematic process that needs planning budget allocation, and several other aspects depending on the security model which is implemented in the organization. For example, the ISO 27001 information model or the BS 7792 security model, or the COBIT information security model.

In this section, we will discuss the phases of the security audits.

Worth mentioning is the fact that there are two major considerations in the course of conducting security audits. In other words, there are two types of security audits.

Internal security audit

The internal security audit is conducted by the members of the organization who have undergonespecialized training in the audit process. They are trained on the various aspects of the audit process such as developing the report and recording nonconformities with respect to the processes and procedures involved in the information security management processes.

The main purpose of the internal audit is to ensure that the processes are being followed and that there is continuity in the system.

The findings that are recorded in the internal audits form an input to the external audit process

External security audit or the certification audit.

This is the audit that is concerned with the certification process of the organization. In generalthe information security model such as ISO 27001 (Figure 5.6).

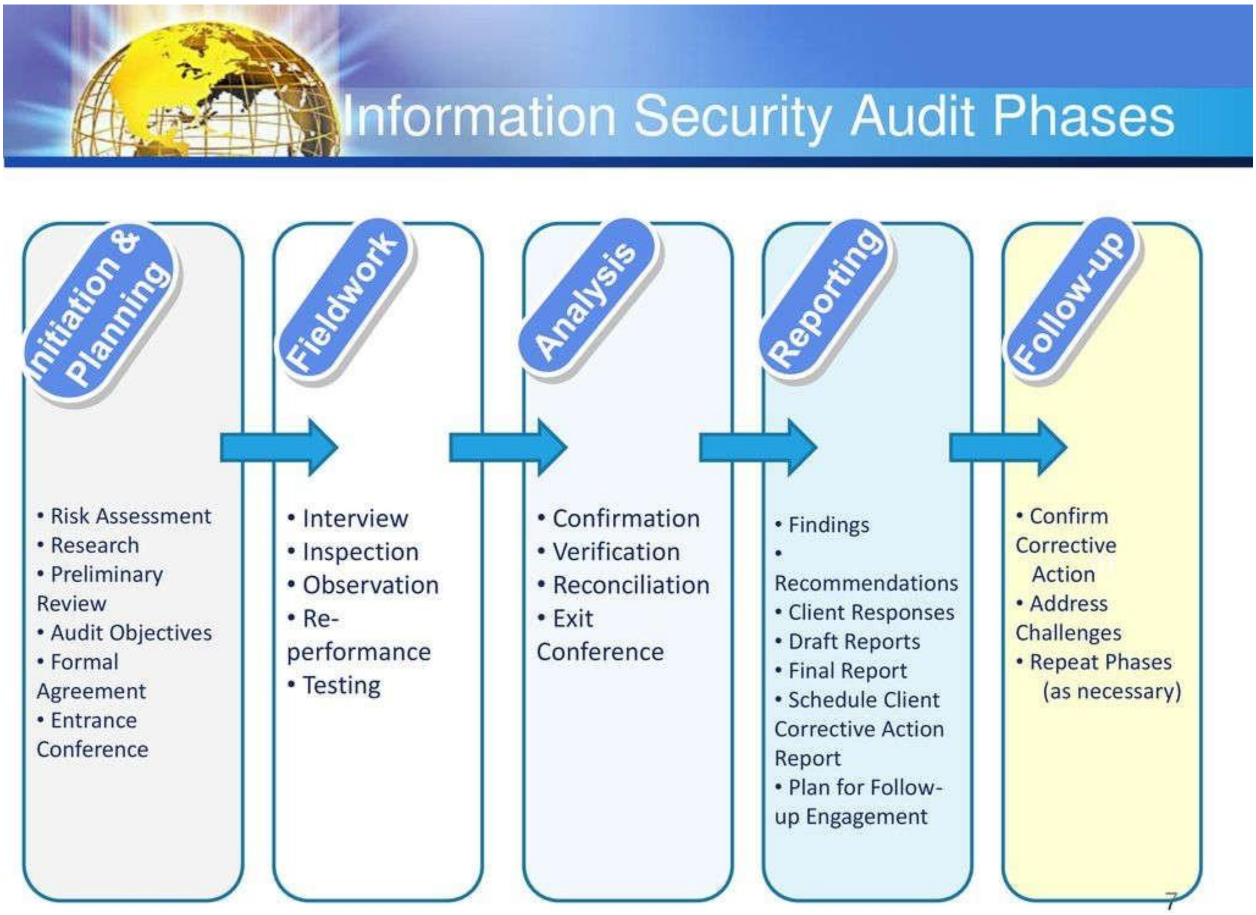


Figure 5.6: Information Security Audit Phases

5.6 Budgeting for Security audits

As mentioned in the previous sections, an information security management system is the need of the hour as businesses have moved online. Moving to online business has many advantages however, security concerns also have gained traction. This necessitates the need for the allocating budget to implement an information security management system.

However, as mentioned in the previous units and previous sections, implementation of information security management is complex and complicated as it involves several interfaces, as well as the span of security management system, is very large for even a small business unit such as the kirana store.

The following points highlight the budget allocation needed for implementing information security management systems in the business units

Allocating budget for implementing security concerns for the human resources

This is the most important consideration for which the business units must allocate the budget. The amount of the budget allocated for this category includes the aspects such as the confidentiality of the tasks performed by human beings, the number of people performing the confidential and security tasks, and they also the business domain in which the organization the business into it.

Let us take an example of what is being discussed in this context. Suppose that an IT company that is into software development needs to have a budget allocation for this category. For example, the server room is a very essential component for any organization hence there are special devices that need to be installed from a security point of view. This includes aspects such as bio-metric access to the server room, close circuit Tv cameras, voice recording features, and other forms of security devices at multi-level security checkpoints.

This is done to allow or permit only authorized persons in the server room. On the other hand, if an organization such asa strong room of a government treasury there the degree and depth of the security must be very high due to the sensitivity of the nature of the business processes being executed. Hence separate budget for installing hardware devices, allocation of budget for manual frisking, allocation of budget for patrolling by armed security guards, and the like. Thus, the budget allocation must be quite high.

Budget allocation for technological advancements implementation

A separate budget must be allocated for the implementation of technological advancements in the organization. This is necessary on account of the fact that *every system when it goes into production starts to be outdated.* In other words, the security lapses or the grey areas of the system begin to surface *and it is these grey areas that are susceptible to being exploited.* These grey areas are taken care of in the new or the technological updates *and these require finances in other words a separate budget for implementing technological advancements.*

Let us take the example of Microsoft vista as the operating system. Organizations at that time implemented Microsoft vista as the operating system on their machines. However, Microsoft vista over a period of time started showing drawbacks or limitations, and soon enough it was replaced with a new and improvised version of Windows XP which replaced Microsoft vista.

Hence the budget for technological advancement as security implementations must be taken care of.

Budget for training on security issues and implementation processes

Information security is today a very important component in the survival of business units. Also, as technology advances, the implemented system needs to be viewed in terms of the vulnerability it can expose which if implemented can lead to a potential loss. Hence, the security in-charges must be trained on a regular basis with respect to the new trends or security mishaps that are happening across the world and which can be seamlessly integrated into the already implementedsystem. To achieve this a separate budget must be allocated.

Budget for implementing security devices on the premises of the organization

The security of the organization is dependent on the physical security of the organization. And, it is these physical securities do need hardware devices to implement information security in the organization. For example, the entire boundary wall of the premises must be under electronic surveillance and this is achieved by means of installing security devices. These devices incur costs hence a budget for implementing them as a part of the system.

Refer to the figure 5.7. This figure demonstrates some of the security points which required budget allocation for security implementation.

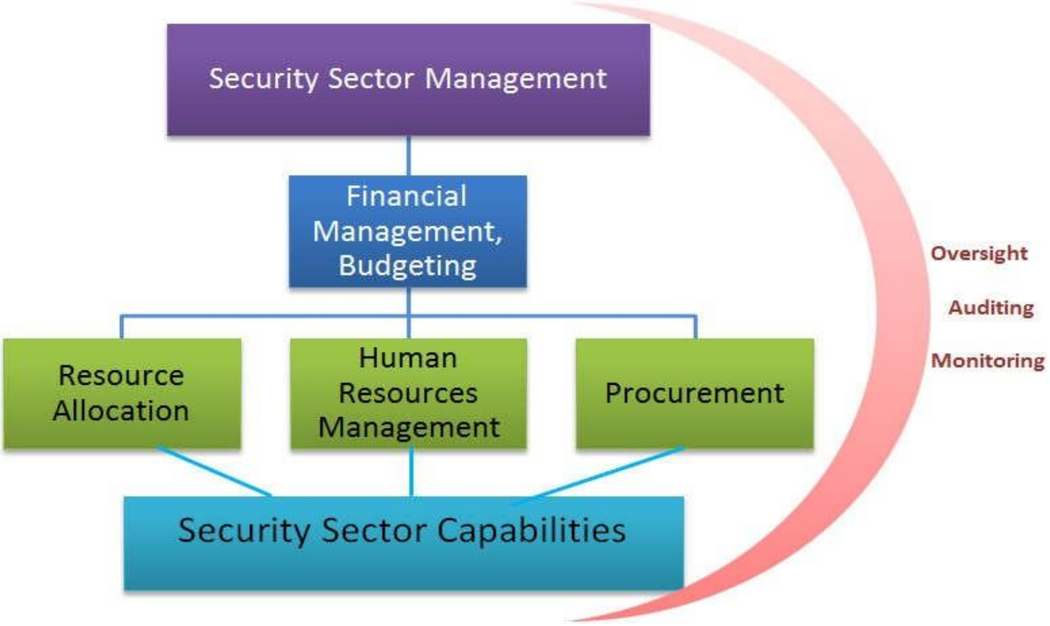

Security Sector Management
Financial Management, Budgeting
Resource Allocation
Human Resources Management
Procurement
Security Sector Capabilities
Oversight
Auditing
Monitoring

Figure 5.7: Budget for implementing security devices on the premises in the organization

Worth mentioning is the fact that the points discussed depends on the degree, depth, and type ofthe business processes being executed in the organization.

- **Knowledge Check 1**

  Fill in the Blanks.

  1. The Security audits are confined to ______,______, and ______.

  2. The External agency is used to _______ the security-related processes as per the standard.

  3. The security audits must be based on __________.

  4. __________ scanning is used to determine the gaps in existing processes.

  5. Whenever a change is introduced it is always____________.

Outcome-Based Activity 1

Prepare an excel report which will depict the various components of the information security management system. Based on the components identified document the risks associated with these components.

5.7 Selecting external security consultants

In the previous sections, we have discussed the various issue pertaining to the security audit process. However, as mentioned in several processes, the structure of the security audit is very large and it is impossible to understand the various avenues in the business organization from wherein the security breach can occur. In other words, an internal security audit is not sufficient to prevent the system from being manipulated by persons outside the organization that is taking undue advantage which would lead to business failure.

All this boils down to the process of taking the help of external consultants or bodies who are experienced in implementing an information security system in the business unit.

The following points depict the reason why an external consultant is the need of the hour for organizations going for information security and implementation

- The prime reason for hiring an external consultant is the fact that an external agent provides more objective shortcomings and vulnerable points in the system *which cannot be identified and anticipated by the internal auditors.*
- The external auditors are exposed to various types of organizations and hence they are able to provide better options and solutions to the business units with respect to risk susceptible points and the like
- The external auditors are trained on world-class information security models such as ISO 27001 or BS 7792 models. These models are developed on the best practices which are adopted by leading organizations with respect to information security implementation issues and challenges.
- The external auditors are exposed to technological advancements and hence they are able to carry out and guide the organizations with respect to implementing security models

Having understood the importance of external consultants let us now discuss the points needed for selecting external consultants.

The following are some of the key points which are needed for the selection of external auditors.

The type of business processes that are executed by the organization

This is the most important point of consideration for selecting an external agency for a security audit. For example, if the business unit is in the financial domain then there is no point in selecting an external agency that has a reputation in the IT domain security audits.

The domain of the external agency

This is another important aspect that needs to be taken into consideration for security audits. This means that the external consultants must have domain knowledge of the various processesin which the business unit is operating.

The cost consideration

This is another important factor which is involved in the process of selecting an external information security consultant. The business unit takes into consideration the budget which is allocated for information security implementation processes based on the business unit's vision and business objectives.

The reputation of the external consultants

This is another important point of consideration that needs to be taken care of. The reputation of the external consultant takes into consideration various aspects such as the type of services provided, the quality of the services provided, and the degree and depth of the risk assessment features to be provided to the business unit.

Refer to the figure 5.8 which depicts some of the key points which are needed for selecting an external consultant.

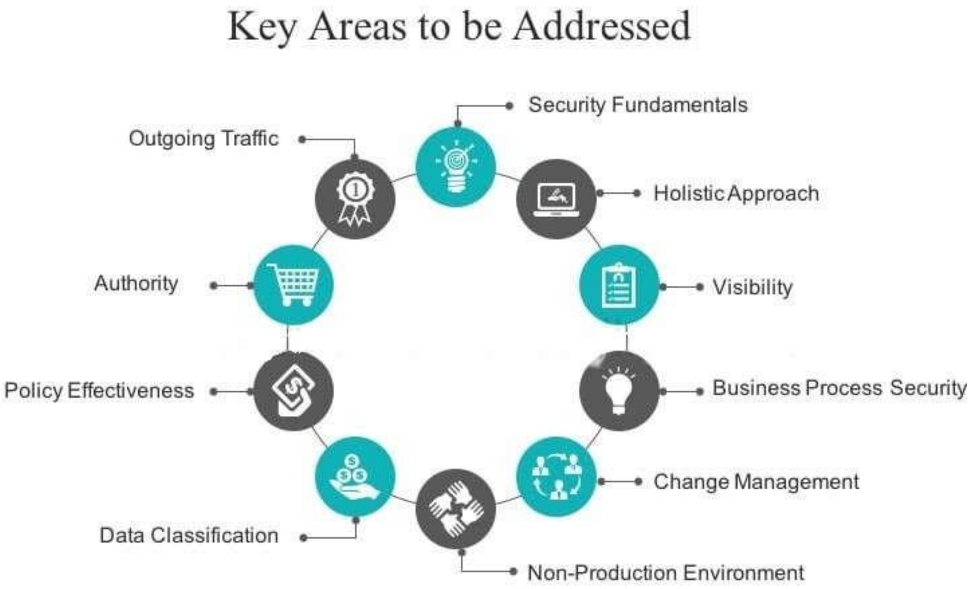


Figure 5.8: Key Areas to be Addressed

From the above figure, it is evident that the external consultant must be capable enough to address the issues such as security fundamentals which are needed for implementation in the organization, the ability and the capability of the external security agency for implementing change management based on the market dynamics and the security requirements based on technology and the like. Thus the organization must be aware that these are the key points and it is on these key points that the external agency is selected.

In addition to these, there are other essential points that must be kept in mind. They are enumerated below.

Recognizing that the organization or the business unit is the target

This is the key point for selecting the external agency. An external agency that makes an organization aware of the target areas based on the market dynamics and the global technology environment and how they were able to manage the risks involved. *it should not be the focus of the external security agency to provide bare minimum services to the business unit instead of highlighting the risk areas and the potential financial losses to the business organization.* This vital point should be addressed during the course of negotiations and finalization of the award of the contract to the external body. *If at any point it is a sense that the external agency is merely taking the business unit for a ride then the proposal should be dropped immediately andalternatives should be explored.*

Failure to inform the business units of the threats to the business sustainability

This is another important aspect that needs to be taken into consideration while selecting an external consultant. The core function for which the business unit is looking for availing the services of the external agency is the fact that the external agency must determine the potential threats and the risks involved in the functioning of the core processes of the organization. In the case of security audits the main or the prime function of the external agency is not only to highlight the risks to the business units but also to provide solutions and recommendations that the business units are able to implement quickly *so as to prevent financial losses.*

The need to stay on top of cybersecurity

This is the most important point of consideration that needs to be taken for selecting a security external agency. The cyber-world is dynamic and hence new areas of risk are emerging everyday wherein security can be breached. Also, the hackers are also trying the use technological advancements to suit their own nefarious purposes of extracting money from the business units. Thus, business units must assess the technological advancements of the external agency when selecting them for implementation of an information security framework and also in the process of extending the contract or otherwise in case of incident handling.

Treating cyber security like an IT issue instead of a financial issue

This is the most important and crucial factor that needs to be undertaken for selecting the external agency. Every risk has cost considerations and hence this must be highlighted by the body. Thus an external agency that is focused on treating information security as an IT issue instead of projecting it as a financial loss must be taken seriously and the business unit must address this concern to the external agency to take it seriously.

5.8 Key success factors for security audits

We have been discussing the various aspects of information security audits. However, information security audits are never complete and it cannot be said that the security audit is a success. The prime reason is the fact that there are various aspects that are attached to the security audits meaning that the audit process must necessarily take into account a 360^0 approach to the audit scope. However, there are certain key points of consideration for calling the security audit a success.

Some of these points are enumerated below:

The key to the success of any initiative of the organization is dependent on the active, visible, and continuous support to the information security management

This is the biggest success factor for the success or failure of a security management system. In other words, the executive management or the top management must demonstrate active visible support. Further, the support must be visible at vantage points so that it sends the message across the organization. Taking an example of an organization Infosys. In this company, the active support of the executive management was clearly visible at all times. For example, the CEO and the Chairman of the company always wore their access cards at all times on campus, and also the vehicle in which they were traveling was also searched for security reasons. Their laptops and desktops were regularly scanned for potential threats and risks. And, sometimes they were required to pay fine as a lapse on their part when they failed to meet the security requirements of the company.

Thus the security audits can be called a success only when the auditors are shown this objective evidence in the context of visible support for security implementation. They need to see and verify objectively the data generated by the executive management towards security requirements.

The existence of a security policy for the organization and the need to verify the degree and the depth of the implementation of the security policy across the organization

This is again one of the key points for determining the success or the failure of security audits. The auditors must verify and validate that the security policy is recent and that it is owned by theCEO. There must objective evidence to prove that the policy is reviewed from time to time and that changes suggested by the auditors are incorporated into the security policy.

Adherence to the audit scope and the audit plan

This is another success factor for the security audit. Often it happens that the audit process itself deviates from the audit scope and the audit plan due to the paucity of time and other crucial factors such as client visits or traveling by key persons. In most cases during the audit process, it is observed that the auditors fail to extract objective evidence from the key stakeholders, and thisresults in partial success or failure of the audit process.

The availability of the documented system of information security management

The auditors must necessarily thoroughly examine the documented structure of the information security management system. In the absence of this core activity, the audit process will be awaste of time.

Hence the auditors must do a preliminary base work of the documentation process before conducting the audit. This ensures that the auditors are aware of the processes and the security system that exists in the organization.

The experience of the auditors

This is also one of the key success factors of the security audit process. The presence of trained auditors who are technically strong generates a lot of value addition to the audit process. Hence this becomes a key factor for the success of the audit process.

- **The technical skills including the risk assessment skill and capability of the auditors**

This is perhaps the most important key success factor of the audit process. The auditors mustpossess sufficient technical knowledge and skills to estimate the risk involved and the potentialdamages that may accrue to the organization when the risk happens. Thus making the executive management of the organization aware of the potential pitfalls and prompting them to takecorrective and preventive actions would term the audit process a success.

The figure 5.9 depicts some of the other factors which are responsible for the success ofthe audit process.

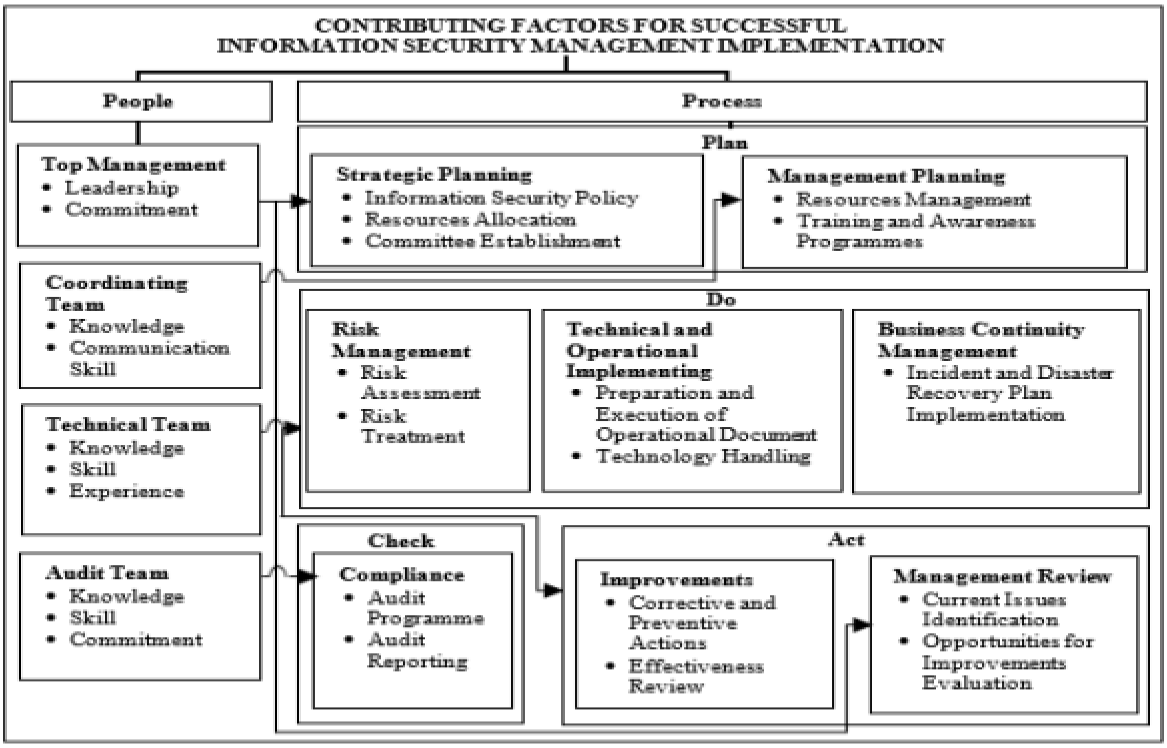

CONTRIBUTING FACTORS FOR SUCCESSFUL
INFORMATION SECURITY MANAGEMENT IMPLEMENTATION
People
Process
Top Management
• Leadership
• Commitment
Coordinating Team
• Knowledge
• Communication Skill
Technical Team
• Knowledge
• Skill
• Experience
Audit Team
• Knowledge
• Skill
• Commitment
Plan
Strategic Planning
• Information Security Policy
• Resources Allocation
• Committee Establishment
Management Planning
• Resources Management
• Training and Awareness Programmes
Do
Risk Management
• Risk Assessment
• Risk Treatment
Technical and Operational Implementing
• Preparation and Execution of Operational Document
• Technology Handling
Business Continuity Management
• Incident and Disaster Recovery Plan Implementation
Check
Compliance
• Audit Programme
• Audit Reporting
Act
Improvements
• Corrective and Preventive Actions
• Effectiveness Review
Management Review
• Current Issues Identification
• Opportunities for Improvements Evaluation

Figure 5.9: International Journal of Innovation Information Security

- **Knowledge**
  Check 2State

True or False.

1. The top-down approach is better than the bottom-up approach in the case of securityaudits (True / False)
2. Technology-based security audits are more effective than manual-based security audits(True / False)
3. The cost of a security audit is the deciding factor for the success of a security audit (True
   / False)
4. The security audit must always be conducted by an external agency (True / False)
5. Penetrating and vulnerability testing is the same (True / False)

Outcome-Based Activity 2

By taking an example of an IT company that is into product development prepare a report for the various points of consideration that are required to be taken for conducting an external security audit in the organization.

5.9 Summary

- The information security management system is needed to undergo regular and periodic audits.
- This is required as every information security management system *decays* after a period of time thereby exposing the system to be susceptible to hackers to exploit the gaps in the implemented security system.
- Conducting security audits is a proactive process wherein the status of the security management system is determined to assess the efficacy of the implemented system.
- Thus audits help the organization to determine the needed steps so that necessary corrective actions can be taken to minimize the loss occurring due to leakage of information.
- Vulnerability and penetrating testing are the two technology-based auditing approaches.
- These methods let the user know the vulnerable key points in the information management system which are vulnerable that is which can be exploited by hackers.

Advanced knowledgeor key points enable organizations to take appropriate actions to bridge the gap.

- In general conducting security, audits is bound to meet resistance from various stakeholders.
- This is due to the fact that it is human nature to resist change. Hence whenever there are gapsor loopholes change is needed hence there is bound to be resistance.
- In other words, audits expose the weakness or the weak points in the system and it is thisweak point that is resisted by the stakeholders.
- Audits are conducted as per the plan. However, while conducting audits, there are severalphases. It cannot be conducted in one go.
- This is due to the fact that the security audits scope is very large and the domain is alsonumerous.
- Hence there are phases in the audit process.
- For example, if an organization says software development company. The audit scope may be auditing of the human resource department and the scope may be limited to higher executive persons of NCR region only.
- Other considerations which are needed to be undertaken are the cost considerations and the choice or the selection of an external body for conducting security audits.
- There are several key success factors for security audits.
- The organization must draft these key success factors in order to ensure that the implementedprocess is effective, efficient, and efficacious.

5.10 Self-Assessment Question

1. What is meant by the approaches to security audits? Explain briefly with an example.
2. What are the various phases in security audits? Explain.
3. What are the various points of consideration that are required to be taken into account forselecting an external consultant? Explain with examples.
4. What are the success key factors for security audits? Explain.
5. What is meant by the term budgeting for security audits? Explain.

5.11 References

- Ryoo, J., Rizvi, S., Aiken, W., & Kissell, J. (2013). Cloud security auditing: challenges and emerging approaches. IEEE Security & Privacy, 12(6), 68-74.

- Koval, V., Nazarova, K., Hordopolov, V., Kopotiienko, T., Miniailo, V., & Diachenko, Y. (2019). Audit the state economic security system. Management Theory and Studies for Rural Business and Infrastructure Development, 41(3), 419-430.
- Golyash, I., Sachenko, S., & Rippa, S. (2011, September). Improving the information security audit of the enterprise using XML technologies. In Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced ComputingSystems (Vol. 2, pp. 795-798). IEEE.
- Pereira, T., & Santos, H. (2010, September). A security audit framework to manage Information system security. In International Conference on Global Security, Safety, and Sustainability (pp. 9-18). Springer, Berlin, Heidelberg.
- Goel, J. N., & Mehtre, B. M. (2015). Vulnerability assessment & penetration testing as a cyber defence technology. Procedia Computer Science, 57, 710-715.
- Khera, Y., Kumar, D., & Garg, N. (2019, February). Analysis and Impact of Vulnerability Assessment and Penetration Testing. In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon) (pp. 525-530). IEEE.
- Shakya, S., & Gupta, A. (2017). Concerns on Information System and Security Audit. Journal of Advanced College of Engineering and Management, 3, 127-135.
- Bleikertz, S., Schunter, M., Probst, C. W., Pendarakis, D., & Eriksson, K. (2010, October). Security audits of multi-tier virtual infrastructures in public infrastructure clouds. In Proceedings of the 2010 ACM workshop on Cloud computing security workshop (pp. 93- 102).

Unit : 6

Introduction to Network Security

Learning Objectives

1. To understand Network Security.
2. To understand the Need for security.

Structure:

6.1 Introduction to “Network Security”

Network security means taking steps to keep your network and data safe. Any company or organization dealing with lots of data has ways to defend against cyber threats. Network security includes actions to keep your data and network safe and valuable. It covers software, hardware, actions, guidelines, and setups for network use, access, with overall protection.

A simple case of network security is using a code word chosen by the user. Recently, it's become a major focus in cyber security, and many organizations are looking for people skilled in this area. Network security solutions help protect computer systems from vulnerabilities like users, locations, data, devices, and applications.

6.2 Need for Security

Ensuring the security of our network is crucial to defend against attackers and hackers. Network Security involves two main aspects: safeguarding datainformation to prevent unauthorized access and loss and ensuring computer security to protect data and thwart hackers. Network security isn't limited to a single network but extends to any network or group of networks.

Now, our requirement for network security has evolved into two distinct needs: information security and computer security.

On the internet or within an organization's network, a multitude of vital information is exchanged daily , making it susceptible to misuse by attacker

Information security

Is imperative for various reasons:

1. Safeguarding secret information accessible only to authorized users.
2. Preventing unauthorized editing , whether accidental or intentional.
3. Protecting information from loss and ensuring proper delivery.
4. Managing acknowledgement of received messages to prevent denial by the sender, especially in specific situations like a customer ordering shares and later denying the order due to market fluctuations.
5. Restricting users from sending messages with a third party's name prevents deceptive

practices.

6. Preventing unwanted delays in message transmission for timely delivery, especially in urgent situations.
7. Avoiding data congestion caused by data or information packets wandering indefinitely in the network if the destination machine fails to capture them due to internal faults.

Another integral aspect of network security is computer security, which aims to protect computer systems from damage caused by the network . Viruses and spyware pose significant threats, capable of erasing information or causing hardware problems. Protecting the network from such destructive software deployed by individuals known as hackers is paramount. Computer security from hackers involves:

1. Protection against replicating and capture viruses from impure files.
2. Proper defence against "worms" and bombs.
3. Protection from Trojan Horses, known for their potential danger to computer systems.

Security approaches

- **Firewalls:** Firewalls operate like a protective barrier between a trusted internal network along with external networks that might not be reliable. They control the flow of network traffic entering and leaving, positioned at the network's edge to filter and block any harmful traffic.
- **Intrusion Prevention Systems (IPS): "**Intrusion Prevention Systems (IPS)" monitor the network or system actions for any malicious attempts or breaches of security policies. They can identify and halt unauthorized access or attacks in real time.
- **VPN:** Virtual Private Networks (VPNs) establish a secure online communication pathway, enabling remote users to connect safely to a private network. Encryption is employed to protect data during its journey, ensuring confidentiality.
- **NAC:** Network Access Control (NAC) enforces rules regarding which devices can access the network and under what conditions. It assesses the security status of devices before allowing connection, ensuring compliance with security policies.
- **SIEM: "**Security Information and Event Management (SIEM) "systems collect and analyze log data from various network devices and applications. This aids in recognizing and respond to security incidents, providing a centralized view of security events for monitoring and analysis.

6.3 Policies of security

Program policy

Program policies are like master plans for an organization’s info safety. They lay out the program's purpose, scope, roles, and rules to follow. Also called master or organizational policies ,they're made with input from top managers and aren't tied to a specific technology. They sometimes change because they're meant to stay relevant, even with tech and organizational change.

Issue-specific policy

Issue-specific policies build on general security policies and guide an organization’s team more specifically. Examples are “Network security “, bring-your-own-device (BYOD), social media, or distant work policies. They focus on certain tech area but are regularly broader. For instance, a remote access policy might say offsite access needs an approved company VPN but won't name a specific VPN client .This way , the company can switch vendors without significant update.

System-specific policy

System-specific policies are super detailed IT security rules for a specific system ,like a firewall, web server, or even one computer .Unlike issue-specific policies ,these are more for tech folks maintaining them . NIST says they should have both security goals and operational rules. IT and security teams help make, enforce, and implement them, but top managers make the big decisions and rules.

6.4 Summary

- Network security means taking steps to keep your network and data safe.
- Network security includes actions to keep your data and network safe and valuable. It covers software, hardware, procedures, guidelines, and setups for network use, access, with overall protection.
- A simple case of network security is using a password chosen by the user.
- Network security solutions help protect computer systems from vulnerabilities like users, locations, data, devices, and applications.
- Ensuring the security of our network is crucial to defend against attackers and

hackers.

- Network Security involves two main aspects: safeguarding data information to prevent unauthorized access and loss and ensuring computer security to protect data and thwart hackers.
- Another integral aspect of network security is computer security, which aims to protect computer systems from damage caused by the network.
- Protecting the network from such destructive software deployed by individuals known as hackers is paramount.
- "Firewalls" act like a protective wall between a trusted "Internal network" and "External networks" that might not be reliable.
- "Intrusion Prevention Systems" (IPS) monitor the network or system activities for any malicious attempts or breaches of security policies.
- Virtual Private Networks (VPNs) establish a secure online communication pathway, enabling remote users to connect safely to a private network.
- Network Access Control (NAC) enforces rules regarding which devices can access the network and under what conditions.
- "Security Information and Event Management" (SIEM) systems collect and analyze log data from a variety of network devices and applications.
- Program policies are like master plans for an organization’s info safety.
- Issue-specific policies build on general security policies and guide an organization’s team more specifically.
- System-specific policies are super full IT security rules for a specific system, like a firewall, web server, or even one computer.
- IT and security teams help make, enforce, and implement them, but top managers make the big decisions and rules.

6.5 Keywords

1. **Firewalls: “**Firewalls” act like a protective obstacle between a trusted internal network and external networks that might not be reliable.Theycontroltheflow ofnetworktrafficenteringandleaving,positionedatthenetwork'sedgetofilter and block any harmful traffic.
2. **Intrusion Prevention Systems (IPS): “**Intrusion Prevention Systems” (IPS) monitor the network or system activities for any malicious attempts or breaches of security

policies. They can identifyandhaltunauthorizedaccessorattacksinreal time.

- **VPN:** Virtual Private Networks (VPNs) establish a secure online communication pathway, enabling remote users to connect safely to a private network. Encryption is employed to protect data during its journey, ensuring confidentiality.

Self-Assessment Questions

- Define the main purpose of a security policy?
- What are major security policies?
- Do I need to have a security policy?
- How do I create a security policy?
- Why is security essential in the realm of information technology and network systems?
- What are the primary objectives of implementing security measures in a network environment?
- Briefly explain the concept of confidentiality and how it relates to network security.
- How do security policies contribute to the over all protection of network resources and sensitive information?
- Discuss the importance of authentication in ensuring secure access to network resources.
- What are the common security approaches used to safeguard networks, and how do they differ in their methodologies?

6.7 References

- Douglas Stinson, "Cryptography Theory and Practice", 2nd Edition, Chapman & Hall/CRC.
- B.A. Forouzan, "Cryptography & Network Security", Tata McGraw Hill.
- W. Stallings, "Cryptography and Network Security", Pearson Education.
- Kaufman, C., Perlman, R., and Speciner, M., "Network Security, Private Communication in a public world", 2nd ed., Prentice Hall PTR., 2002.

- Cryptography and Network Security; McGraw Hill; Behrouz A. Forouzan.
- Information Security Intelligence Cryptographic Principles and App., Calabrese Thomson.

Unit : 7

Types of Attacks

Learning Objectives:

1. Understand the Types of attacks.
2. Understand the Services.

Structure:

7.1 Types of Attacks

7.2 Services

7.3 Summary

7.4 Keywords

7.5 Self-Assessment Questions

7.6 References

7.1 Types of attacks

Various type of attack target Network security .Let's explore the most common ones:

1. **Malware:** Malware is speedy, malicious software crafted by hackers to disrupt systems, damage networks, and gain unauthorized access for stealing data or individual information. It gets automatically installed through the internet and swiftly infects all connected computers.
2. **Virus:** Also a malicious software, a virus needs user interaction to harm the system. It can't replicate independently and relies on human involvement, often through malicious links like email attachments containing harmful code. Clicking on such links can corrupt files and lead to personal information theft.
3. **Worm:** A standalone computer malware, worms replicate without human intervention, spreading through networks by exploiting system flaws. They don't require a host file and can infiltrate a system through applications, consuming processing power and causing unresponsiveness.
4. **Man-in-the-middle:** A “Man-in-the-middle” attack occurs when a person intercepts and takes away private information or changes it between two gadgets, like a user's device and a server.
5. **(DDoS) Distributed Denial of Service:** DDoS is a complex type of DoS attack where the attacker employs many systems to flood the victim's server with traffic, leading to malfunctions and blocking access. Identifying DDoS threats is tricky because they originate from different infected systems and are frequently employed for blackmail or revenge.

Denial-of-service attacks include:

- Correlation flooding
- Vulnerability attacks
- Bandwidth flood

6. **Phishing:** “Phishing” is a sneaky trick used by hackers. They send fake emails to fool people into giving away personal info like credit card details, online banking info, usernames, and passwords. These emails look legit but have harmful stuff hidden in them.
7. **IP Spoofing:** IP Spoofing is a crafty move by attackers. They change their computer's

ID to pretend they're someone trustworthy. This helps them break into a system without being noticed.

8. **Botnet:** A Botnet is like a hacker's team of infected computers. These computers do what the hacker wants, all working to attack different systems simultaneously. It's like a zombie army controlled by the hacker.
9. **Trojan horse:** A seemingly harmless application that turns malicious when installed, often embedded in games and spreading through social engineering methods like emails. Trojans can give attackers access to sensitive information.
10. **Packet Sniffer:** These tools capture and save transmission packets in a network. Attackers use sniffers to gather sensitive information such as social details, financial data, trade secrets, user IDs, and passwords by intercepting network packets.

7.2 Services

When we discuss network security, the CIA triad emerges as a crucial model guiding information security policies in an organization. CIA stands for “Confidentiality , Integrity, and Availability” —critical objectives for securing a network.

Confidentiality

Confidentiality is about making sure only authorized people can access data. It's the responsibility of users to keep control systems secure, like passwords for computers and physical restrictions like ID cards.

Employees need to be well-trained in information security to avoid accidentally sharing data. It's crucial to limit data sharing and set rules to maintain confidentiality.

Physical restrictions are equally important. Unauthorized access to your building canlead to unauthorized data access. Door codes should never be written down, andstaff should be cautious to ensure no one is watching or recording them enteringcodes. Many organizations require employees to wear ID badges, making it easier toidentify non-employees. ID badges should be worn only at work to prevent criminalsfrom using your details to gain access. Areas with sensitive information may haveextraaccess restrictions, like anadditional door code.

Integrity

Integrity means ensuring data is accurate and up-to-date. An organization's trustworthiness and conscientiousness depend on the integrity of its data. One of the fundamental principles in data protection is keeping data accurate and up-to-date.

Users must fulfill their legal duties to maintain data integrity. Assigning specific roles and responsibilities for data integrity helps ensure everyone takes it seriously.

Availability

Availability ensures authorized personnel can reliably access information. Data mustbestoredin a logical and secure system to be easily accessible. High availabilitysupports efficient business processing and benefits the organization. Every user isresponsible for organising desktop documents for future access. Paper copies should besecurely filed and not leftunattended.

7. 3 Summary

- Various types of attacks target network security.
- Malware is speedy, malicious software crafted by hackers to disrupt systems, damage networks, and gain unauthorized access for stealing data or personal information.
- Malicious software, a virus needs user interaction to harm the system.
- A standalone computer malware, worms replicate without human intervention, spreading through networks by exploiting system flaws.
- Man-in-the-middle attack occur when a person intercepts and takes away private information or changes it between two gadgets, like a user's device and a server.
- DDoS is a complex type of DoS attack where the aggressor employs many systems to flood the victim's server by traffic, leading to malfunctions and blocking access.
- Phishing is a sneaky trick used by hackers. They send fake emails to fool people into giving away personal info like credit card details, online banking info, usernames, and passwords.
- IP Spoofing is a crafty move by attackers. They change their computer's ID to pretend they're someone trustworthy.
- A Botnet is like a hacker's team of infected computers. These computers do what the hacker wants, all working to attack different systems simultaneously.

- A seemingly harmless application that turns malicious when installed, often embedded inside games and spreading through social engineering methods like emails.
- When we discuss network security, the CIA triad emerges as a crucial model guiding information security policies in an organization.
- Secrecy ensures that only authorized individuals or systems can access sensitive or classified information transmitted over the network.
- Encryption techniques like "AES (Advanced Encryption Standard) or DES (Data Encryption Standard)" are employed to thwart this.
- Moving onto Integrity, it ensures data remains unaltered. Data corruption signifies a failure to maintain Integrity.
- Availability emphasizes the network's constant accessibility for users, encompassing systems and data.
- Network administrators ensure availability by maintaining hardware, implementing regular upgrades, establishing fail-over plans, and preventing bottlenecks.

7.4 Keywords

1. **Malware:** Malware is speedy, malicious software crafted by hackers to disrupt systems ,damage networks, and gain unauthorized access for stealing data or private information. It gets automatically installed through the internet and swiftly infect all connected computers.
2. **Worm:** A standalone computer malware, worms replicate without human intervention, spreading through networks by exploiting system flaws. They don't require a host file and can infiltrate a system through applications, consuming processing power and causing unresponsiveness.
3. **Phishing:** Phishing is a sneaky trick used by hackers. They send fake emails tofool people into giving away personal info like credit card details, online bankinginfo, usernames, and passwords. These emails look legit but have harmful stuffhidden in them.
4. **IPSpoofing**: IP Spoofing is a crafty move by attackers. They change their computer's ID to pretend they're someone trustworthy. This helps them break into a system without being noticed.
5. **Confidentiality:** Confidentiality ensures that just authorized individuals or systems

can access sensitive or classified information transmitted above the network. Unauthorized access poses a risk, as attackers may use various tools to capture data.

7.5 Self-AssessmentQuestions

- Breakdown the idea of phishing attacks and how they mess with keeping things confidential.
- How does a man-in-the-middle attack mess with the honesty of data when it's being passed around?
- Define ransomware and discuss how it messes with keeping things secret and available.
- What's SQL injection, and how does it sneak through weak spots to mess with data honesty?
- How can social engineering attacks mess with keeping secret info secret?
- Explain what encryption does to keep data talks down low.
- Why are access control mechanisms essential for keeping data honest?
- How do buffer overflow attacks mess with a system's availability?
- Define "zero-day exploit" and discuss how it throws a wrench in system security.
- How does multi-factor authentication help keep user accounts confidential?

7.6 References

- Douglas Stinson, "Cryptography Theory and Practice", 2nd Edition, Chapman & Hall/CRC.
- B.A. Forouzan, "Cryptography & Network Security", Tata McGraw Hill.
- W. Stallings, "Cryptography and Network Security", Pearson Education.
- Kaufman, C., Perlman, R., and Speciner, M., "Network Security, Private Communication in a Public World", 2nd Edition, Prentice Hall PTR, 2002.
- "Cryptography and Network Security", McGraw Hill, Behrouz A. Forouzan.
- "Information Security Intelligence Cryptographic Principles and App.", Calabrese Thomson.

Unit : 8

Encryption Techniques

Learning Objectives:

1. Tounder stand the Encryption Techniques.
2. Tounder stand Encryption & Decryption.

Structure:

8.1 Encryption Techniques

Encryption is a way to safeguard information by turning it into code that can only be understood by someone with the correct key. It appears chaotic and unreadable if unauthorized individuals try to access encrypted data. When we talk about encryption, it's the process of changing data from a readable form to a scrambled one. This is done to stop anyone from peeking at sensitive data while it's being transmitted. Encryption can be applied to various things like documents, files, messages, or any communication over a network.

PlainText

In simple terms, encrypted communication transforms regular text into code using ciphers or encryption methods. Plaintext is any information that can be read without a decryption key, including binary files. Everything intended to be encrypted or already encrypted is considered plain text. A cryptographic system takes this plaintext, processes it, and produces code known as ciphertext. Algorithms help convert ciphertext back into plain text and vice versa. This process ensures that only the intended recipient can understand the data. Protecting plain text stored in computer files is crucial because unauthorized access can expose the information, leading to potential actions based on that data. To ensure security, the storage medium, the device, its components, and any backups must be secured.

Ciphertext

Ciphertext is the result of using encryption methods, often called ciphers. If someone or something doesn't have the correct cipher, the data appears encrypted and cannot be understood. The cipher is essential for interpreting the data. Algorithms are used to transform regular text into ciphertext and vice versa, involving encryption and decryption processes.

In simpler terms, substitution ciphers replace letters or groups of letters with other letters, preserving the initial sequence. This cryptographic approach involves substitutions rather than revealing the original elements.

Substitution Cipher Technique

In the Substitution Cipher technique, characters are replaced with other characters or symbols, changing their identity but not their position in the string. This method encrypts text by substituting letters or units of text. While basic substitution ciphers became easy for computers to crack, some concepts persist in modern encryption.

Transposition Cipher Technique

In the Transposition Cipher Technique, each character's position shifts to a different position. This encryption method arranges plaintext units predictably, creating a permutation of the plaintext.

One example is the Rail Fence encryption, where the plaintext is written on imaginary "rails" of a fence and then read in a series of rows. This technique follows a scytale-like pattern, an ancient Greek device for constructing transposition ciphers.

The Rail Fence Cipher encrypts by coiling a ribbon around a cylinder, and decoding happens when the ribbon is uncoiled from a cylinder with the same diameter as the encrypting cylinder.

8.2 Encryption & Decryption

Encryption

Encryption is like a secret code for data. It's a way of jumbling up regular information (plaintext) so that only the right people can unscramble it back to its original form.

This jumbled-up version is called ciphertext. The idea is to keep unauthorized folks from understanding the info even if they try to snoop around.

To do this, encryption uses a unique key (think of it as a secret codebreaker) created by a computer algorithm. Even if someone tries to crack the code without the key, it's super hard because it takes a lot of computer smarts and time. Only the person supposed to get the info can easily unscramble it using the key. When data is encrypted, it looks like a bunch of random letters and numbers.

Once data is locked up with encryption, the only way to open and reread it is by using the right key. Encryption is crucial for keeping sensitive info safe when it's sent or stored. There are different types of encryption, like stream ciphers that handle data bit by bit and block ciphers that deal with larger chunks.

Decryption

Decryption is the opposite of encryption. It's the process of turning encrypted databack to its original state. It's like using the secret codebreaker (key) to unlock thejumbled-up info. Decryption needs this unique key or password, and only the rightpersoncan use it to decodethe data.

When infotravels on the internet, there's a risk of sneaky people trying to peek at it.
That's why we use encryption – to stop data from being stolen. Email, text files,pictures, and more can be encrypted to keep them safe. When someone needs todecrypt the info, they usually get a pop-up or window asking for the password. This ensures that only authorized users can access the protected data.

8.3 Cryptographicattacks

A cryptographic attack allows terrible actors to get around the security of a cryptographic system by discovering weaknesses in its code, cipher, cryptographic protocol, or key management scheme. This evasion is also known as "cryptanalysis." So, these attacks focus on cryptographic or cipher systems that hide data so only a few people can see it. There are six main types of these attacks, depending on the cryptographic system and information available to the attacker:

- **Brute force attacks:** In brute force attacks, the person trying to break into a system tests different keys to uncover a coded message. For instance, if the critical size is 8 bits, there are 256 potential keys (2^8). To succeed, the attacker must know the algorithm and test all 256 keys.
- **Ciphertext-only attack:** Ciphertext-only attacks happen when an intruder gets hold of a bunch of coded messages. Even though they can't directly access the original message, they can deduce it from the coded collection. This method is typically less effective than brute force.
- **Chosen plaintext attack:** In chosen plaintext attacks, a cybercriminal handpicks specific data to obtain the corresponding ciphertext, making it more straightforward to figure out the encryption key.**Known plain text attack:** This occurs when the attacker already knows the plain text of some parts of the cipher text through information-gathering techniques.
- **Dual key and algorithm attack:** The attacker tries to recover the key used for encryption or decryption by analysing the cryptographic algorithm.

Active vs Passive Cryptographic Attacks:

Besides these six types,cryptographic attacks can be either passive or active.

- **Passive attacks:** Passive attacks are launched to gain unauthorized access tosensitive data by intercepting or eavesdropping on general communication. Significantly, in passive attacks, the data and communication are not tampered with; they remain intact.
- **Active attacks:** Involve modifying the data or communication. The attacker gains access to the data and tampers with it.

Key Range & Size

- Key range: In cryptography, the key range refers to all the potential values acryptographic key can have. A sufficiently sizable key range is crucial to makeithardforattackerstoguessorbrute-forcethecorrectkey.
- When the key range is more extensive, cryptographic algorithms become more complex, making it more challenging for attackers to carry out various attacks, likebrute-force attempts.
- Key Size: The key Size, usually measured in bits, is a specific numeric valuewithin the key range. It shows the length or complexity of the cryptographickey. In simple terms, a larger key size means a higher level of security. For instance, a 128-bit key offers more possible combinations than a 64-bit key, making it more resilient against cryptographic attacks.

  As computational power advances, cryptographic algorithms often need to boost their key sizes to ensure a consistently high level of security.

8.4 Summary

- Encryption is a way to safeguard information by turning it into code that can only be understood by someone with the correct key.
- When we talk about encryption, it's the process of changing data from a readable form to a scrambled one.
- In simple terms, encrypted communication transforms regular text into code using

ciphers or encryption methods.

- Everything intended to be encrypted or already encrypted is considered plaintext.
- A cryptographic system takes this plaintext, processes it, and produces code known as ciphertext.
- Ciphertext is the result of using encryption methods, often called ciphers.
- In the Substitution Cipher technique, characters are replaced with other characters or symbols, changing their identity but not their position in the string.
- In the Transposition Cipher technique, each character's position shifts to a different position.
- The Rail Fence Cipher encrypts by coiling a ribbon around a cylinder, and decoding happens when the ribbon is uncoiled from a cylinder with the same diameter as the encrypting cylinder.
- Encryption is like a secret code for data. It's a way of jumbling up regular information (plaintext) so that only the right people can unscramble it back to its original form.
- Once data is locked up with encryption, the only way to open and reread it is by using the right key.
- Decryption is the opposite of encryption. It's the process of turning encrypted data back to its original state.
- Decryption needs this unique key or password, and only the right person can use it to decode the data.
- A cryptographic attack allows malicious actors to get around the security of a cryptographic system by discovering weaknesses in its code, cipher, cryptographic protocol, or key management scheme.
- In brute force attacks, the person trying to break into a system tests different keys to uncover a coded message.
- Ciphertext-only attacks happen when an intruder gets hold of a bunch of coded messages.
- Chosen ciphertext attacks involve the attacker trying to link the coded message to the original one, aiming to guess the key and obtain secret details.
- In cryptography, the key range refers to all the potential values a cryptographic key can have.
- When the key range is more extensive, cryptographic algorithms become more complex, making it more challenging for attackers to carry out various attacks, like

brute-force attempts.

- The key size, usually measured in bits, is a specific numeric value within the key range. It shows the length or complexity of the cryptographic key.
- As computational power advances, cryptographic algorithms often need to boost their key sizes to ensure a consistently high level of security.

8.5 Keywords

1. **Ciphertext:** Ciphertext is the result of using encryption methods, often calledciphers. If someone or something doesn't have the correct cipher, the data appears encrypted and cannot be understood. The cipher is essential for interpreting the data.
2. **Encryption:** Encryption is like a secret code for data. It's a way of jumbling upregular information (plaintext) so that only the right people can unscramble it back to its original form. This jumbled-upversion is called ciphertext. The idea is to keep unauthorized folks from understanding the info even if they try to snoop around.
3. **Brute force attacks:** In brute force attacks, the person trying to break into a system tests different keys to uncoveracoded message. For instance, if the Criticalsizeis 8bits, there are 256 potential keys (2^8). To succeed, the attacker must know the algorithm and test all 256 keys.
4. **Ciphertext-onlyattack:** Ciphertext- Only attacks happen when an intruder gets hold of a bunch of coded messages. Even though they can't directly access the original message, they can deduce it from the coded collection. This method is typically less effective than brute force.

8.6 Self-AssessmentQuestions

- What is plaintext in the context of encryption?
- How do substitution techniques contribute to encryption methods?
- Can you provide an example of a substitution cipher and how it works?
- What is the role of transposition techniques in encryption?
- Explain the difference between substitution and transposition techniques in encryption.
- How does encryption ensure secure communication and data protection?
- Define cryptographic attacks and provide examples of common types.

- What is the purpose of key range in encryption algorithms?
- What are the potential vulnerabilities associated with encryption algorithms?
- How do cryptographic keys enhance the security of encrypted data?

8.7 References

- Douglas Stinson, Cryptography: Theory and Practice, 2nd Edition, Chapman & Hall/CRC.
- B.A. Forouzan, Cryptography & Network Security, Tata McGraw Hill.
- W. Stallings, Cryptography and Network Security, Pearson Education.
- Kaufman, C., Perlman, R., and Speciner, M., Network Security: Private Communication in a Public World, 2nd ed., Prentice Hall PTR, 2002.
- Cryptography and Network Security, McGraw Hill, Behrouz A. Forouzan.
- Information Security Intelligence: Cryptographic Principles and Applications, Calabrese Thomson.

Unit : 9

Symmetric & Asymmetric Key Cryptography

Learning Objectives:

1. To understand the Symmetric & Asymmetric Key Cryptography.
2. To underst and Algorithm types & Modes.

Structure:

9.1 Symmetric & Asymmetric Key Cryptography

Symmetric Encryption:

The simplest way to keep information safe is using symmetric encryption. In this method, a single secret key is use to both lock and unlock the data. It's an old but effective technique involving a private key, which can be a number, a word , or a arbitrary bunch of letters. This key mixes with the original message, changing its content in a specific manner. To make this work, in cooperation with the sender and receiver must know the secret key for locking and unlocking the messages .Examples of symmetric encryption methods are “Blowfish “, AES , RC4 , DES , RC5 ,and RC6, with AES-128, AES-192, and “AES-256” commonly used. However, there's a catch–all parties concerned have to share the key before they can unlock the information.

Pros and Cons of “Symmetric Encryption”:

Pros:

- Faster: use a single key for encryption and decryption speeds up the process.
- Identity verification: It employs secret word authentication for verifying the receiver's identity.
- Easy to execute & manage: With only one key for “encryption and decryption” , it's simple to implement as well as manage.

Cons:

- Secure key sharing is challenging, making it difficult to share keys securely.
- Symmetric encryption could be more scalable ,making it unsuitable for various users.

Asymmetric Encryption:

“Asymmetric encryption” , also recognized as public key cryptography, is a relatively recent method compare to symmetric encryption. This technique utilizes two keys for encrypting plain text and exchanging secret keys over the Internet or a network .This prevents malicious individuals from misuse the keys. Notably, anyone possessing the secret key be capable of decrypt the message, prompting using two related keys to improve security. A public key is shared openly for message-senders, while the second private key remains confidential. Messages encrypted by a public key require a private key for decryption, as well as vice versa. With its heightened security, asymmetric encryption is commonly employed in daily communication channels, specially over the Internet. Examples include EIGamal,” RSA “, DSA, Elliptic curve techniques, and PKCS.

Pros and Cons of Asymmetric Encryption:

Pros:

- Dual keys- public and private-eliminate key distribution issues.
- Scalability: With a pair of keys ,communication by multiple parties becomes manageable in big networks.

Cons:

- Performance: “Asymmetric encryption” is slower than symmetric encryption.
- Complexity: Implementing and managing asymmetric encryption is more challenging due to large key sizes.

Algorithm Types & Modes

Symmetric Key Cryptography

Symmetric Key Cryptography involves encrypting and decrypting messages using a shared key between the sender and receiver. While it's a faster and simpler system, securely exchanging the key is the challenge. Notable examples ofsymmetriccritical cryptography systems include “Data Encryption System (DES)” and Advanced Encryption System (AES).

Hash Function

Hash Functions, on the other hand, don't use any key. They calculate a fixed-length hash value based on the plain text ,making it nearly unfeasible to recover the original content. Many operating systems employ hash functions for password encryption.

Asymmetric Key Cryptography

“Asymmetric key cryptography is also called public-key cryptography, there are two keys: a private one for the receiver and a public one for everyone. These keys, linked by math, come in pair. The public key is open to everyone, while the private key is only for the individual who creates it.

Digital Signatures

Moving on to Digital Signatures in Cryptography ,they are compare able to handwritten signatures and serve as electronic verifications of the sender. Digital signatures find everyday use in software distribution and financial transactions, serving three essential purposes : Authentication, proving the sender in cryptography; non-repudiation,ensuringsomeonecan'tdenyvalidity;andIntegrity,maintainingthe quality of the sent and received messages.

Data Encryption Standard (DES):

“Data Encryption Standard” (DES) is vital in safeguarding data by acting as a block cipher with a 56-bit key length. Over time, DES has been a critical playerinensuring data security. However, its popularity has slightly waned due to discovering vulnerabilities through powerful attacks.

DES operates as a block cipher when processing data, working on 64-bitblocks.This means it transforms “64 bits of plaintext” into 64 bits of cipher text. Both encryption and decryption employ the same algorithm and key, and the key has a significant length of 56 bits.

International Data Encryption Algorithm (IDEA):

Created in 1991, the (IDEA) International Data Encryption Algorithm is a type of encryption that keep digital information safe .It uses a 64-bit block size and a 128-bit key length. To transform regular text into a secret ciphertext code, IDEA uses mathematical techniques such as modular arithmetic, bit shifting, and XOR operations. It's good at defending against different attacks,like differential and linear cryptanalysis. One of IDEA's strong points is that it works well in software and hardware applications.

IDEA's speed, low memory requirement, and modest processing power make it suitable for limited-resource applications. Despite being succeeded by newer algorithms like AES, IDEA remains secure andisstillusedinsomelegacysystemsand applications.

Differential & Linear Cryptanalysis:

Cryptanalysis is the procedure of transforming encrypted communications into readable format without access to the actual key. Unlike brute force attacks, cryptanalysis seeks vulnerabilities within a cryptosystem. It involves a concentrated mathematical effort at decryption, utilizing available knowledge on the encryption scheme.

Linear Cryptanalysis:

"Linear cryptanalysis" is a common type of attack against block ciphers. It relies on discover affine approximation to a cipher's action to exploit weaknesses in the encryption process.

Differential Cryptanalysis:

Differential cryptanalysis is a method applicable to Block and Stream ciphers and cryptographic hash functions. It explores how changes in input information affect subsequent differences inside the output. In the framework of block ciphers, it tracks differences across transformations to identify non-random behavior and recoverthe secret key. Cryptanalysis is crucial for breaking cryptographic security systems and accessing encrypted messages, even with an unknown cryptographic key.

9.2 Summary

- The simplest way to keep information safe is using symmetric encryption. In this method, a single secret key is used to both lock and unlock the data.
- To make this work , in cooperate with the sender and receiver must know the secret key for locking and unlocking the communication.
- "Asymmetric encryption", also known as public key cryptography ,is a relatively recent method compared to symmetric encryption.
- Notably, anybody possessing the secret key can decrypt the message, prompting using two related keys to enhance security.
- Messages encrypted by a public key need a private key for decryption, andvice versa.
- Symmetric Key Cryptography involves encrypting and decrypting messages using a shared key among the sender and receiver.
- Hash Functions ,on the other hand ,don't use any key.They calculate a "Fixed-length" hash value base on the plaintext ,making it nearly not possible to recover the original content.
- In "Asymmetric key cryptography" ,also called public-key cryptography, there are two keys: a private one for the receiver and a public one for everyone.
- MovingontoDigitalSignaturesinCryptography,theyarecomparableto handwritten signatures and serve as electronic verifications of the sender.

- Data Encryption Standard (DES) is vital in safeguarding data by acting as a block cipher with a 56-bit key length.
- DESoperatesasablockcipherwhenprocessingdata,workingon64-bit blocks.
- An exciting aspect of DES is its key manipulation process. Despite starting witha 64-bit key, DES discards every 8th bit before getting underway.
- To transform regular text into a secret ciphertext code, IDEA uses mathematical techniques such as modular arithmetic, bit shifting, and XOR operations.
- One of IDEA's strong points is that it works well in software and hardware applications.
- Cryptanalysis is the process of transforming encrypted communications into readable format without access to the actual key.
- Linear cryptanalysis is a common type of attack against block ciphers .It relies on discover affine approximation to a cipher's action to exploit weaknesses in the encryption process.
- Differential cryptanalysis is a method applicable to “Block and stream ciphers and cryptographic hash functions”.
- In the context of block ciphers, it tracks differences across transformations to identify non-random behaviour and recover the secret key.
- Cryptanalysis is crucial for breaking cryptographic securitysystemsandaccessing encrypted messages, even with an unknown cryptographic key.

9.3 Keywords

1. **Hash Functions:** Hash Functions, on the other hand, don't use any key. They calculate a fixed-length hash value stand on the plaintext, building it nearly not possible to recover the original content. Many operating systems employ hash functions for password encryption.
2. **DES:** Data Encryption Standard (DES) is vital in safeguarding data by acting as a block cipher with a 56-bit key length. Over time, DES hasbeenacriticalplayerin ensuring data security. However, its popularity has slightly waned due to discovering vulnerabilities through powerful attacks.
3. **Linear Cryptanalysis:** Linear cryptanalysis is a common type of attack against block ciphers .It relies on discovering affine approximation to a cipher's action to exploit weaknesses in the encryption process.

4. **Differential Cryptanalysis:** Differential cryptanalysis is a method applicable to “Block and stream ciphers and cryptographic hash functions”. It explores how changes in input information affect subsequent differences in the output.

9.4 Self-AssessmentQuestions

- What sets Symmetric and Asymmetric Key Cryptography apart at their core?
- Can you list two standard symmetric key encryption algorithms?
- Elaborate on the idea of block cipher modes in symmetric key cryptography.
- Tell me about DESandits functioning in symmetric key encryption.
- Break down the IDEA algorithm and its importance in cryptography.
- Mention a widely used block cipher mode in symmetric key cryptography and clarify its workings.
- Name two prevalent asymmetric key encryption algorithms.
- Delvein to the security pros and cons of symmetric key cryptography.
- How does management differ in a symmetric key cryptography from symmetric key cryptography?
- Explain the role of cryptographic algorithms in ensuring data integrity in a communication system.

9.5 References

- Douglas Stinson, "Cryptography Theory and Practice", 2nd Edition, Chapman & Hall/CRC.
- B. A. Forouzan,"Cryptography & Network Security",TataMcGrawHill.
- W.Stallings,"Cryptography and Network Security", Pearson Education.
- Kaufman, C., Perlman, R., and Speciner, M., Network Security, Private Communication in a public world, 2nd ed., Prentice Hall PTR., 2002.
- Cryptography and Network Security; McGrawHill; Behrouz A Forouzan.
- Information Security Intelligence Cryptographic Principles and App.Calabrese Thomson