Course Title	:	**Computer Security**
Semester	:	**Fifth**
Branch	:	**BSc Computer Science**
Created By	:	**Department of Computer Science** **St. Mary's College of Commerce and Management Studies, Thuruthiply**

CS5CRT17: Computer Security (Core)

Unit I

Introduction-Principles of Security- Need for Security- Threats- Attacks

Unit II

Cryptography :Cipher Methods: Caesar cipher -One time pad – Mono alphabetic Cipher - Play fair cipher-Poly alphabetic cipher -Vigenère – Cipher, Transposition ciphers – Cryptographic Algorithms: Symmetric & Asymmetric- Cryptographic tools: PKI- Digital Signatures-Stenography

Unit III

System Security: Intrusion Detection and Prevention Systems, Why IDPS? Types of IDPS, Password Management, Countermeasures

Unit IV

Network Security: Electronic Mail Security, Pretty Good Privacy, S/MIME, IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload.

Unit V

Web Security: Web Security considerations- Secure Socket Layer -Transport layer Security-Secure Electronic transaction, Firewalls-Packet filters- Application Level Gateway-Circuit Level Gateway.

Book of Study:

1. Michael E. Whitman, Herbert J. Mattord, 'Principles of Information Security' Fourth Edition
2. William Stallings, 'Cryptography and Network Security – Principles and Practices',Fourth Edition,2006,Pearson Education.

Reference :

1. Behrouz A. Forouzan, Dedeep Mukhopadhyay 'Cryptography & Network Security', Second Edition,Tata McGraw Hill, New Delhi, 2010.
2. Atul Kahate, 'Cryptography and Network Security', Second Edition, Tata McGraw Hill

MODULE 1

Computer Security

Computer Security is the process of detecting and preventing any unauthorized use of your lap top/computer. Computer security is security applied to computing devices such as computers and smart phones, as well as computer networks such as private and public networks, including the whole Internet

Computer facilities have been physically protected for three reasons:

- **To prevent theft of or damage to the hardware**
- **To prevent theft of or damage to the information**
- **To prevent disruption of service**

In general, security is "the quality or state of being secure—to be free from danger." In other words, protection against adversaries—from those who would do harm, intentionally or otherwise—is the objective.

A successful organization should have the following multiple layers of security in place to protect its operations:

Physical security: To protect physical items, objects, or areas from unauthorized access and misuse

Personnel security: To protect the individual or group of individuals who are authorized to access the organization and its operations

Operations security: To protect the details of a particular operation or series of activities

Communications security: To protect communications media, technology, and content

Network security: To protect networking components, connections, and contents

Information security: To protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. It is achieved via the application of policy, education

Principles of Security

These are the different computer security principles.

Availability

Availability enables authorized users—persons or computer systems—to access information without interference or obstruction and to receive it in the required format.

Accuracy

Information has **accuracy** when it is free from mistakes or errors and it has the value that the end user expects. If information has been intentionally or unintentionally modified, it is no longer accurate.

Authenticity

Authenticity of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is in the same state in which it was created, placed, stored, or transferred.

Confidentiality

Information has confidentiality when it is protected from disclosure or exposure to unauthorized individuals or systems. Confidentiality ensures that *only* those with the rights and privileges to access information are able to do so. When unauthorized individuals or systems can view information, confidentiality is breached. To protect the confidentiality of information, you can use a number of measures, including the following:

- Information classification
- Secure document storage
- Application of general security policies
- Education of information custodians and end users

Integrity

Information has integrity when it is whole, complete, and uncorrupted.

Utility

The utility of information is the quality or state of having value for some purpose or end. Information has value when it can serve a purpose. If information is available, but is not in a format meaningful to the end user, it is not useful.

Possession

The possession of information is the quality or state of ownership or control. Information is said to be in one's possession if one obtains it, independent of format or other characteristics. While a breach of confidentiality always results in a breach of possession, a breach of possession does not always result in a breach of confidentiality.

Need for Security

The network needs security against attackers and hackers. Network Security includes two basic securities. The first is the security of data information i.e. to protect the information from unauthorized access and loss. And the second is computer security i.e. to protect data and to thwart hackers. Here network security not only means security in a single network rather in any network or network of networks.

To protect the secret information users on the net only. No other person should see or access it.

1. To protect the information from unwanted editing, accidently or intentionally by unauthorized users.

2. To protect the information from loss and make it to be delivered to its destination properly.
3. To manage for acknowledgement of message received by any node in order to protect from denial by sender in specific situations. For example let a customer orders to purchase a few shares XYZ to the broader and denies for the order after two days as the rates go down.
4. To restrict a user to send some message to another user with name of a third one. For example a user X for his own interest makes a message containing some favorable instructions and sends it to user Y in such a manner that Y accepts the message as coming from Z, the manager of the organization.
5. To protect the message from unwanted delay in the transmission lines/route in order to deliver it to required destination in time, in case of urgency.
6. To protect the data from wandering the data packets or information packets in the network for infinitely long time and thus increasing congestion in the line in case destination machine fails to capture it because of some internal faults.

Business Needs

Information security performs four important functions for an organization:

1. Protecting the organization's ability to function.
2. Enabling the safe operation of applications running on the organization's IT systems
3. Protecting the data the organization collects and uses.
4. Safeguarding the organization's technology assets

Threats

A threat, in the context of computer security, refers to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more.

Different types of threats are

- Hackers
- Viruses
- Spyware
- Adware
- Phishing
- Worms
- Spam
- Botnets

- **Hacking**

Computer hacking refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's original objective

- **Website Hacking:** Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
- **Network Hacking:** Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.
- **Email Hacking:** It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.
- **Ethical Hacking:** Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.
- **Password Hacking:** This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- **Computer Hacking:** This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

- **Viruses *(Virtual Information Resource Under Seize)***

A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions.

- **Spyware**

Spyware is software that is installed on a computing device without the end user's knowledge. Any software can be classified as spyware if it is downloaded without the user's authorization.

- **Adware**

Adware is any software application in which advertising banners are displayed while a program is running. The ads are delivered through pop-up windows or bars that appear on the program's user interface.

- **Phishing**

Phishing is a method of trying to gather personal information using deceptive emails and websites.

Eg: Acquiring the details Such as credit card numbers, personal identification and account usernames and passwords.

- **Worms**

A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers

- **Spam**

Spam refers to the use of electronic messaging systems to send out unrequested or unwanted messages in bulk.

- **Botnets**

A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. To send spam.

Computer Attacks

An attempt to gain unauthorized access to information resource or services, or to cause harm or damage to information systems.

Computer Attacks mainly classified into two

An attempt to gain unauthorized access to information resource or services, or to cause harm or damage to information systems.

Computer Attacks mainly classified into two

- **Passive:** Attackers gain access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact.
- **Active:** Attackers not only gain unauthorized access but also modify data, either deleting, encrypting or otherwise harming it.

We distinguish network attacks from several other types of attacks:

- **Endpoint attacks**—gaining unauthorized access to user devices, servers or other endpoints, typically compromising them by infecting them with malware.
- **Malware attacks**—infecting IT resources with malware, allowing attackers to compromise systems, steal data and do damage. These also include ransom ware attacks.
- **Vulnerabilities, exploits and attacks**—exploiting vulnerabilities in software used in the organization, to gain unauthorized access, compromise or sabotage systems.
- **Advanced persistent threats**—these are complex multilayered threats, which include network attacks but also other attack types.

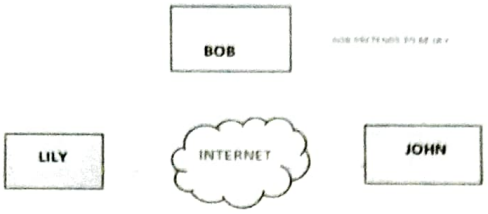
Active and Passive attacks in Information Security

Active attacks: An Active attack attempts to alter system resources or effect their

operations. Active attack involves some modification of the data stream or creation of false statement. Types of active attacks are as following:

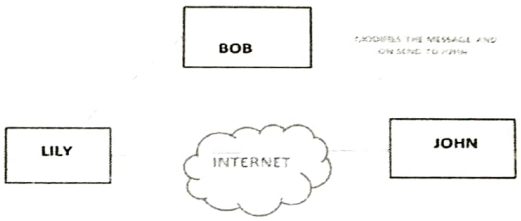
1. **Masquerade**

Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other form of active attacks.



2. **Modification of messages**

It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. For example, a message meaning 'Allow JOHN to read confidential file X' is modified as 'Allow Smith to read confidential file X'.

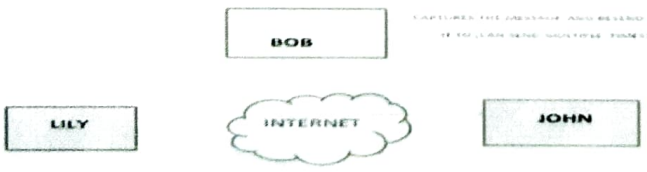


3. **Repudiation**

This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message. For example, customer ask his Bank –To transfer an amount to someone' and later on the sender(customer) deny that he had made such a request. This is repudiation.

4. **Replay**

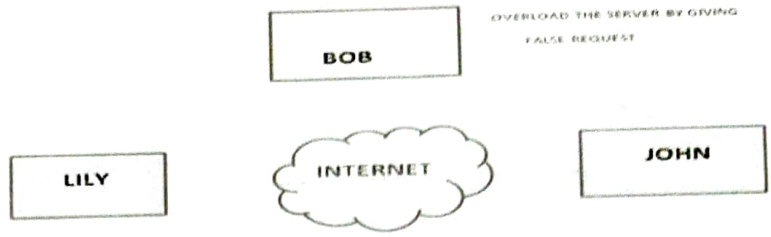
It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.



5. **Denial of Service**

It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular

destination. Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.



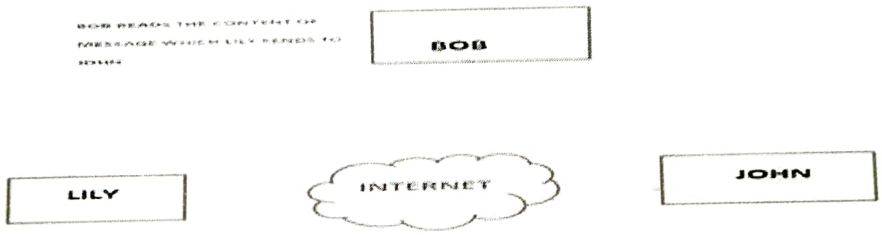
Passive attacks:

A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted.

Types of **Passive attacks are as following:**

1. **The release of message content**

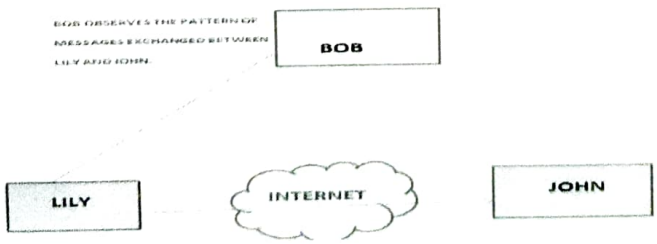
Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



2. **Traffic analysis**

Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.

The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.



* ***Active Attack:*** In computer security, persistent attempt to introduce invalid data into a system, and/or to damage or destroy data already stored in it.

Types of active attacks include:

- Denial of service (DoS)
- Distributed Denial of Service (DDoS)
- Session replay.
- Masquerade.
- Message modification.
- Trojans.

1. **Modification of messages**

   It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. For example, a message meaning –Allow **Repudiation**

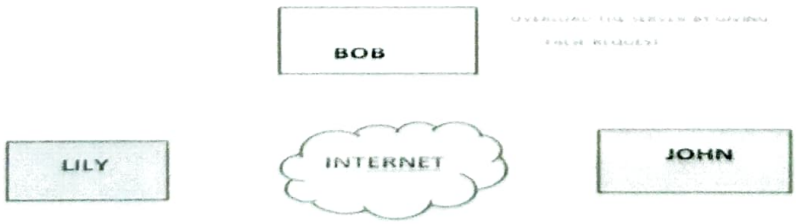
   This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message. For example, customer ask his Bank –To transfer an amount to someone' and later on the sender(customer) deny that he had made such a request. This is repudiation.

2. **Replay**

   It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.

3. **Denial of Service**

   It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruptions of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.



MODULE -II

Cryptography

Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing." Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa.

Three types of cryptographic techniques used in general.

1. Symmetric-key cryptography

2. Hash functions.

3. Public-key cryptography

Symmetric-key Cryptography: Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.

Public-Key Cryptography: This is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and for decryption private key is used.

Hash Functions: No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.

Symmetric Cipher Model

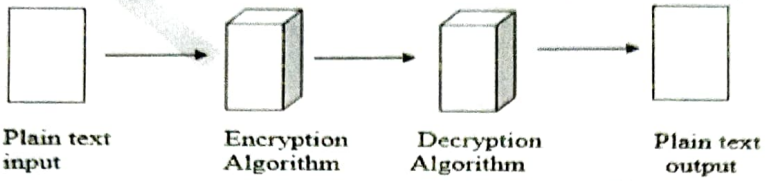
A Symmetric encryption scheme has 5 ingredients.

1. Plaintext: The original message or data that is fed into the algorithm as input.
2. Encryption algorithm: It performs various substitutions and transformations on plaintext.
3. Secret Key: The secret key is also input to the encryption algorithm.

4. Cipher text: This is the scrambled message produced as output.
5. Decryption algorithm: This is essentially the encryption algorithm run in reverse.

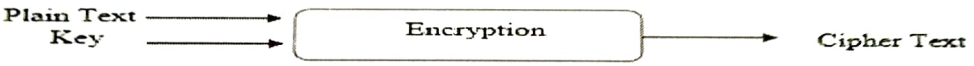
There are two requirements for secure use of conventional encryption.

1. We need strong encryption algorithm
2. Sender and receiver must have obtained copies secret key.



Cipher

Cipher is the way to encrypt data. Plaintext is the original data before being encrypted and the data of the encryption output is called cipher text or cryptogram. The methods which used to encrypt plaintext is called ciphers.



Cipher Methods

Here we are going to discuss about the following types of Ciphers

- **Caesar Cipher**
- **One time pad**
- **Mono Alphabetic Cipher**
- **Play fair Cipher**
- **Poly Alphabetic Cipher**
- **Vigenere Cipher**
- **Transposition Cipher**

Caesar Cipher

Introduction

The Caesar cipher is one of the earliest known and simplest ciphers. It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on.

Eg: Here is a quick example of the encryption and decryption steps involved with the caesar cipher. The text we will encrypt is 'defend the east wall of the castle', with a shift (key) of 1.

Plaintext: defend the east wall of the castle

Cipher text: efgfoe uif fbtu xbmm pg uif dbtumf

It is easy to see how each character in the plaintext is shifted up the alphabet.

Decryption is just as easy, by using an offset of -1.

Plain: abcdefghijklmnopqrstuvwxyz

Cipher: bcdefghijklmnopqrstuvwxyza

One time pad

In this method one key is used for decrypting a single message. Each new message requires a new key of the same length as the new message such a scheme, known as a one-time pad.

Mono Alphabetic Cipher

Mono alphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if 'A' is encrypted as 'D', for any number of occurrence in that plaintext, 'A' will always get encrypted to 'D'.

Eg:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	K	V	Q	F	I	B	J	W	P	E	S	C	X	H	T	M	Y	A	U	O	L	R	G	Z	N

Plain: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D K V Q F I B J W P E S C X H T M Y A U O L R G Z N

Plaintext: I F W E W I S H T O R E P L A C E L E T T E R S
Cipher text: W I R F R W A J U H Y F T S D V F S F U U F Y A

Play Fair Cipher

The best known multiple-letter encryption cipher is the Play fair, which treats diagrams in the plaintext as single units and translates these unit into cipher text diagram.

Play fair Key Matrix

- A 5X5 matrix of letters based on a keyword
- fill in letters of keyword (no duplicates)
- fill rest of matrix with other letters
- Eg. Using the keyword MONARCHY

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	O	S	T
U	V	W	X	Z

Poly alphabetic Cipher

In poly alphabetic substitution each occurrence of a character may have different substitution. The relationship between a characters in the plaintext to a character in the cipher text is one to many.for eg: 'A' could be enciphered as 'D' in the beginning of the text but 'N' at the middle.

Vigenere cipher

One interesting kind of polyalphabetic cipher was designed by Blaise-de-vigenere,a 16th centuary French mathematician. A vigenere cipher uses a different strategy to create the key stream. Then key stream is a repetition of an initial ---- key stream of length M, where we have 1<=M<=26

P=P, P2, P3…

C=C1, C2, C3…

K=K1, K2, K3… Km

Encryption: Ci=Pi+Ki

Decryption: Pi=Ci-Ki

Transposition cipher

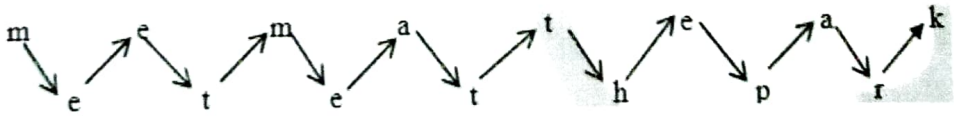
A transposition cipher does not substitute one symbol for another. Instead it changes its location of the symbol. A symbol in the first position of the plaint text message appear in the 10th position of the cipher text. A symbol in the 8th position in the plain text may appear in the first position of the cipher text. In other words the transposition ciphers reorder the symbols.

Keyless transposition cipher

It is a simple transposition cipher. it is a keyless cipher. There are two methods for permutation of characters. in the first method the text is written into a table column by column and then transmitted row by row. In the second method the text is written into the table row by row and then transmitted column by column.

Eg: "A" sends a message to "B"

"meet me at the park"



Here A creates the cipher text "MEMATEAKETETHPR" by sending the first row followed

the second row. B divides the cipher in half. That is first half is the first row and the second half, the second row. Again B reads the result in zigzag.

In second method A writes the same plain text, row by row, in a table of four columns.

m	e	e	t
m	e	a	t
t	h	e	p
a	r	k	

A creates the cipher text "MMTAEEHREAEKTTP" by transmitting the characters column by column. B receives the cipher text and writes the received message column by column and reads it row by row.

Keyed Transposition Cipher

In this method the plain text is dividing into groups of predetermined size, called blocks and then uses a key to permute the characters in each block separately. Eg: "A" needs to send the message "enemy attacks tonight" to "B".

Step1: divide the text into groups of 5 characters,

Step2: add a bogus character at the end to make the last group the same size as the others.

E n e m y a t t a c k s t o n i g h t z

For encryption the following keys are used

Encryption ↓

3	1	4	5	2
1	2	3	4	5

↑ Decryption

Third character in the plain text becomes 1; first character becomes 2 and so on.

E E M Y N T A A C T T K O N S H I T Z G

Cryptography algorithm

Set of mathematical function and rules that takes plaintext and a key as a input and product cipher text as output. Cryptography is a process which is associated with scrambling plaintext into cipher text (a process called encryption), then back again (known as decryption).

Types Of Cryptography There are several ways to classify the cryptography algorithms. The most common types are:

- Secret Key Cryptography this is also called as Symmetric Key Cryptography
- Public Key Cryptography this is also called as Asymmetric Key Cryptography

Symmetric Cryptography:

In the symmetric key encryption, same key is used for both encryption and decryption process. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encrypt them. The symmetric key encryption takes place in two modes either as the block ciphers or as the stream ciphers. In the block cipher mode the whole data is divided into number of blocks. These data is based on the block length and the key is provided for encryption. In the case of the stream ciphers the data is divided as small as single bits and randomized then the encryption takes place. Symmetric key cryptosystems are much faster than the asymmetric key cryptosystems. The performance evaluation is taken place for the following symmetric key encryption techniques such as The DES Algorithm, Triple DES algorithm, the AES algorithm and Blowfish algorithm.

Data Encryption Standard

DES is a symmetric key algorithm which was developed by IBM in 1977.It uses block size 64 bit , key size 56 bits.. DES always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm. DES used 16 rounds of transposition and substitution to encrypt each group of 8 (64 bit) plaintext letters and output from each round is one by one. The number of rounds is exponentially proportional to the amount of time and fined a key using a brute-force attack. Therefore the number of rounds increases then the security of the algorithm increases exponentially. DES was clearly no longer invulnerable to the attacks.

Triple DES

Triple DES is same as the DES operation. It uses three 64-bit keys and overall key length of 192 bits. We simply type in the entire 192-bit (24 character) key rather than entering each of the invidiously three keys. The procedure for encryption is exactly the same as DES, but this process is repeated three times. It is encrypted with the first key then decrypted with the second key, and finally encrypted again with the third key. This procedure for decrypting something is the same as the procedure for encryption, except it is accept same as reverse process.

Advanced Encryption Standard

Rijndael was selected as the AES in Oct-2000 Designed by Vincent Rijmen and Joan Daemen in Belgium. AES is a symmetric block cipher that can Block size 128 bit, Cipher keys 128,192 and 256 bits. Basically, encryption algorithms are divided into three major categories – transposition, substitution, and transposition – substitution technique. AES

algorithm uses a round function that is compared of four different byte-oriented transformations such as Sub byte, Shift row, Mix column, Add round key. Number of rounds to be used depend on the length of key e.g. 10 round for 128 bit key, 12 rounds for 192-bit key and 14 rounds for 256 bit keys.

Blowfish Algorithm

Blowfish algorithm is the important type of the symmetric key encryption that has a 64 bit block size and a variable key length from 32 bits to 448 bits in general . It is based on 16 round fiestel cipher network that uses the large key size. The key size is larger as it is difficult to break the code in the blowfish algorithm. Additionally it is exposed to all the attacks apart from the weak key class attack.

Asymmetric Cryptography

Asymmetric key encryption is the technique, in which the different keys are for the encryption and the decryption process. One key is public (published) and second is kept private. They are also called as the public key encryption. If the lock/encryption key is first published then the system enables private communication from the public to the unlocking key's user [5]. If the unlock/decryption key is the one published then the system serves as a signature verifier of documents locked by the owner of the private key. Public key methods are important because they can be used for transmitting encryption keys or other data securely even when the both the users have no opportunity to agree on a secret key in private Algorithm. The keys used in public key encryption algorithms are usually much longer that improves the security of the data being transmitted. For the following algorithms the performance factors are evaluate.

RSA:

Rivest- Shamir- Adleman is the most commonly used public key encryption algorithm. It can be able to be used for both encryption and digital signatures. The security of RSA is generally considered to factoring. RSA computation occurs with integers modules n = p * q, for select two random secret primes p, q. To encrypt a message m, public key use a public key exponent e. so cipher text c = me (mod n) computes the multiplicative reverse d = e -1 (mod (p1) * (q-1)) (we require that e is selected suitably for it to exist) and obtains cd = m e * d = m (mod n). The problem for the attacker is that computing the reverse d of e is assumed to be no easier than factorizing n. The key size should be greater than 1024 bits for a reasonable level of security. Keys of size, say, 2048 bits that provides.

Diffie-Hellman Algorithm

It is that public key encryption algorithm, using discrete logarithms in a finite field .Two

parties allow to exchange a secret key over an insecure medium without any prior secrets. Diffie Hellman (DH) is a widely used key exchange algorithm. In many cryptographically protocols, two parties wish to begin communicating. Diffie-Hellman protocols are exchange keys and allow the construction of common secret key over an unconfident contact channel. This problem is based on related to discrete logarithms; its name is Diffie-Hellman problem. This problem is hard, as compare to the discrete logarithm problem.

Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. As the digital equivalent of a handwritten signature or stamped seal, a digital signature offers far more inherent security, and it is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence of origin, identity and status of an electronic document, transaction or message and can acknowledge informed consent by the signer.

What Is Steganography?

Steganography is the practice of hiding a secret message inside of (or even on top of) something that is not secret. That something can be just about anything you want. These days, many examples of steganography involve embedding a secret piece of text inside of a picture. Or hiding a secret message or script inside of a Word or Excel document. The purpose of steganography is to conceal and deceive. It is a form of covert communication and can involve the use of any medium to hide messages. It's not a form of cryptography, because it doesn't involve scrambling data or using a key. Instead, it is a form of data hiding and can be executed in clever ways.

MODULE - III

Intrusion Detection System (IDS)

An intrusion detection system (IDS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations.

An IDS works by monitoring system activity through examining vulnerabilities in the system, the integrity of files and conducting an analysis of patterns based on already known attacks. It also automatically monitors the Internet to search for any of the latest threats which could result in a future attack.

Classification of Intrusion Detection System:

IDS is basically classified into 2 types:

1. Network Intrusion Detection System (NIDS)

Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.

2. Host Intrusion Detection System (HIDS)

Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.

Intrusion Detection Systems

Intrusion:

An intrusion is defined as the unauthorized use, misuse, or abuse of computer systems by either authorized users or external perpetrators.

Types of Intrusions:

- **External attacks**

Attempted break-ins, denial of service attacks, etc.

- **Internal attacks**

Masquerading as some other user Misuse of privileges, malicious attacks

- **Clandestine users:** exploiting bugs in privileged programs

Types of intruders:

- **Masquerader:** pretend to be someone one is not An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.
- Misfeasor: authentic user doing unauthorized actions A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges. Clandestine user: done secretively, especially because illicit An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

Why Use an IDPS?

- Prevent problem behaviors by increasing the perceived risk of discovery and punishment
- Detect attacks and other security violations.
- Detect and deal with preambles to attacks.
- Document existing threat to an organization.

  Act as quality control for security design and administration, especially of large and complex enterprises.
- Provide useful information about intrusions that take place.

IDPS Terminology

- Alarm or alert: indication that attack is happening.
- Evasion: attacker change the format and/or timing of activities to avoid being detected.
- False attack stimulus: event triggers alarm – no real attack.

- False negative: failure of IDPS to react to attack.
- False positive: alarm activates in the absence of an actual attack.
- Noise: alarms events that are accurate but do not pose threats.
- Site policy: rules & configuration guidelines governing the implementation& operation IDPS.
- Site policy awareness: ability to dynamically modify config in response to environmental activity.
- True attack stimulus: event that triggers alarms in event of real attack.
- Tuning: adjusting an IDPS.
- Confidence value: measure IDPS ability correctly detect & identify type of attacks.
- Alarm filtering: Classification of IDPS alerts.
- Alarm clustering and compaction: grouping almost identical alarms happening at close to the same time.

Types of IDS

- Network based
- Focused on protection network information assets
- Wireless
- Network behavior analysis
- Host-based Focused on protection server of host's information assets

Network-based:

- Perform packet sniffing and analyze network traffic to identify and stop suspicious activity. They are typically deployed inline. Like a network firewall. They receive packets, analyze them, decide whether they should be permitted, and allow acceptable packets to pass through.
- Allow some attacks, such as network service worms, e-mail. Borne worms and viruses with easily recognizable characteristics (e.g., subject, attachment filename), to be detected on networks before they reach their intended targets (e.g., e-mail servers, Web servers).
- Most products use a combination of attack signatures and analysis of network and application protocols.
- Network-based products might be able to detect and stop some unknown threats through application protocol analysis.
- Some products allow administrators to create and deploy attack signatures for many

major new malware threats in a matter of minutes. Although poorly written signature triggers false positives that block benign activity, a custom signature can block a new malware threat hours before antivirus signatures become available.

- However, network-based products are generally not capable of stopping malicious mobile code or Trojan horses.

Advantages of NIDPSs

- Good network design and placement of NIDPS can enable organization to use a few devices to monitor large network.
- NIDPSs are usually passive and can be deployed into existing networks with little disruption to normal network operations.
- NIDPSs not usually susceptible to direct attack and may not be detectable by attackers.

Disadvantages of NIDPSs

- Can become overwhelmed by network volume and fail to recognize attacks.
- Require access to all traffic to be monitored.
- Cannot analyze encrypted packets.
- Cannot reliably ascertain if attack was successful or not.
- Some forms of attack are not easily discerned by NIDPSs, specifically those involving fragmented packets.

Host-based IDPS

- Resides on a particular computer or server and monitors activity only on that system
- Benchmark and monitor the status of key system files and detect when intruder creates, modifies, or deletes files
- Most HIDPSs work on the principle of configuration or change management
- Advantage over NIDPS: can usually be installed so that it can access information encrypted when traveling over network

Advantages of HIDPSs

- Can detect local events on host systems and detect attacks that may elude a networkbased IDPS.
- Functions on host system, where encrypted traffic will have been decrypted and is available for processing.
- Not affected by use of switched network protocols.
- Can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs.

Disadvantages of HIDPSs

- Pose more management issues
- Vulnerable both to direct attacks and attacks against host operating system
- Does not detect multi-host scanning, nor scanning of non-host network devices
- Susceptible to some denial-of-service attacks
- Can use large amounts of disk space
- Can inflict a performance overhead on its host systems

Wireless NIDPS

- Monitors and analyzes wireless network traffic
- Looks for potential problems with the wireless protocols (layers 2 and 3)
- Cannot evaluate & diagnose issue with higher level layers
- Issues associated with implementation
- Physical security
- Sensor range
- Access point and wireless switch locations
- Wired network connections
- Cost

Can detect conditions in addition to traditional types of IDSPS

- Unauthorized WLAN and WLAN devices
- Poorly secured WLAN devices
- Unusual usage patterns
- The use of wireless network scanners
- DoS attacks and condition
- Man-in-middle attacks

Unable to detect

- Passive wireless protocol attacks
- Susceptible to evasion techniques
- Susceptible to logical and physical attacks on wireless access point

Password Management

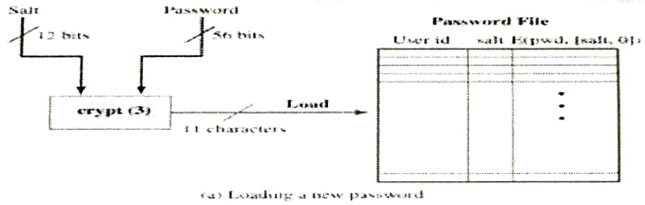
- **Password Protection:** The front line of defense against intruders is the password system. Virtually all multiuser systems require that a user provide not only a name or identifier (ID) but also a password. The password serves to authenticate the ID of the individual logging on to the system.

In turn, the ID provides security in the following ways:

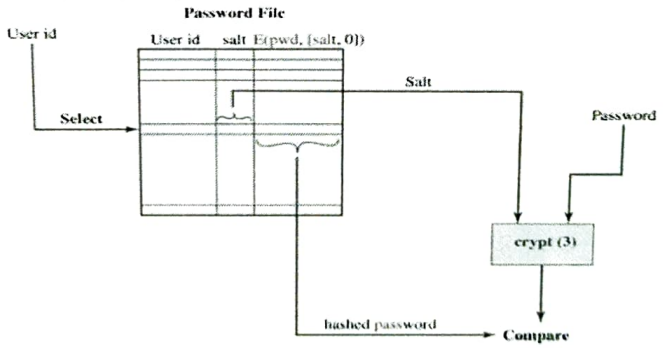
- The ID determines whether the user is authorized to gain access to a system.
- The ID determines the privileges accorded to the user.

The Vulnerability of Passwords:

- Let us consider a scheme that is widely used on UNIX:
- Each user selects a password up to eight characters.
- This is converted into a 56-bit value (key input to an encryption routine).
- The encryption routine is based on DES. The DES algorithm is modified using a 12-bit.
- This value is related to the time at which the password is assigned to the user.
- The modified DES algorithm is exercised with a data input consisting of a 64-bit block of zeros.
- The output of the algorithm then serves as input for a second encryption. □ This process is repeated for a total of 25 encryptions.
- The resulting 64-bit output is then translated into an 11-character sequence.
- The hashed password is then stored, together with a plaintext copy of the salt, in the password file.



(a) Loading a new password



(b) Verifying a password

Security countermeasures

Security countermeasures are the controls used to protect the confidentiality, integrity, and availability of data and information systems.

- Virus
- Pretty Good Privacy (PGP)
- Secure Multipurpose Internet Mail Extensions (S/MIME)
- Privacy Enhanced Mail (PEM)

- Secure Shell (SSH)
- Secure Electronic Transmission (SET)
- Terminal Access Controller Access Control System (TACACS)
- Kerberos
- SSL
- Transport Layer Security (TLS)
- Windows Sockets (SOCKS)
- Secure RPC (S/RPC)
- IPsec
- Point-to-point Tunneling Protocol (PPTP)
- Challenge Handshake Authentication Protocol (CHAP)
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Packet Filters
- Network Address Translation (NAT)
- Secure Coding

MODULE IV

Network Security

E-Mail Security

Email security describes different techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss or compromise. Email is often used to spread malware, spam and phishing attacks. Attackers use deceptive messages to entice recipients to part with sensitive information, open attachments or click on hyperlinks that install malware on the victim's device. Email is also a common entry point for attackers looking to gain a foothold in an enterprise network and obtain valuable company data.

Email encryption involves encrypting, or disguising, the content of email messages to protect potentially sensitive information from being read by anyone other than intended recipients. Email encryption often includes authentication.

Email Security Tools

A secure email gateway, deployed either on-premises or in the cloud, should offer multilayered protection from unwanted, malicious and BEC email; granular visibility; and business continuity for organizations of all sizes. These controls enable security teams to have confidence that they can secure users from email threats and maintain email communications in the event of an outage.

An email encryption solution reduces the risks associated with regulatory violations, data loss and corporate policy violations while enabling essential business communications. The solution should work for any organization that needs to protect sensitive data, while still making it readily available to affiliates, business partners and users—on both desktops and mobile devices. An email encryption solution is especially important for organizations required to follow compliance regulations, like GDPR, HIPAA or SOX, or abide by security standards like PCI-DSS.

Pretty Good Privacy (PGP)

Pretty Good Privacy or PGP is a popular program used to encrypt and decrypt email over the Internet, as well as authenticate messages with digital signatures and encrypted stored files.

Previously available as freeware and now only available as a low-cost commercial version, PGP was once the most widely used privacy-ensuring program by individuals and is also used by many corporations. It was developed by *Phil R. Zimmermann* in 1991 and has

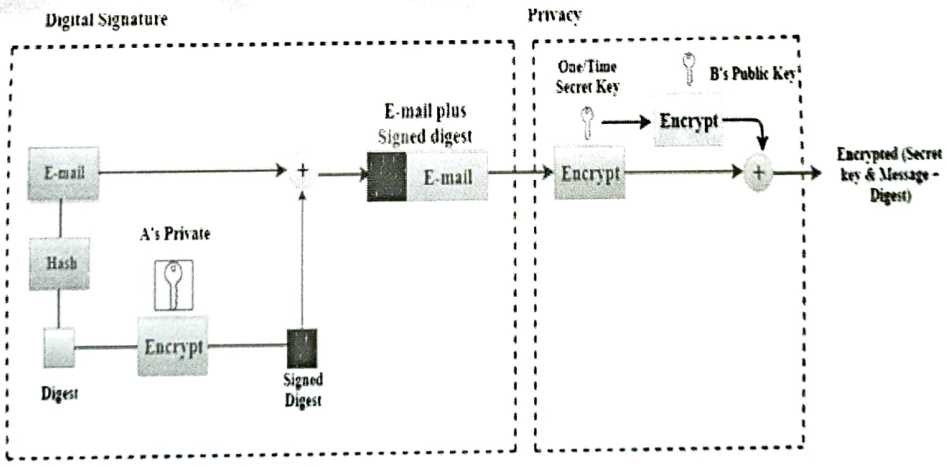
become a de facto standard for email security.

PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.

PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.

PGP at Sender Site

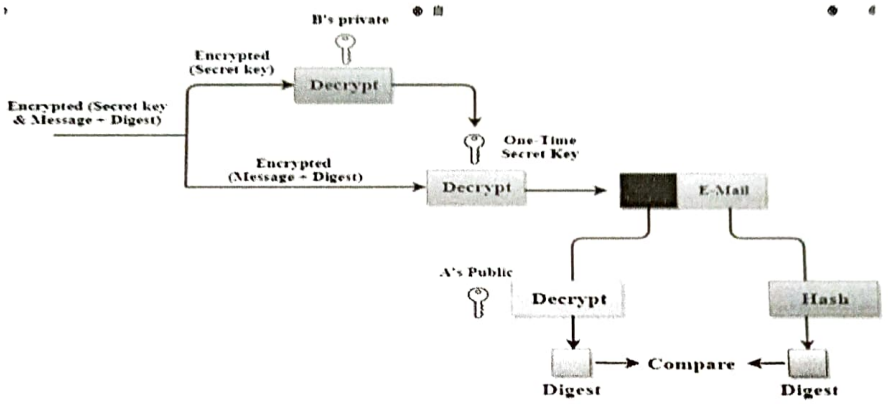
- The e-mail message is hashed by using a hashing function to create a digest.
- The digest is then encrypted to form a signed digest by using the sender's private key, and then signed digest is added to the original email message.
- The original message and signed digest are encrypted by using a one-time secret key created by the sender.
- The secret key is encrypted by using a receiver's public key.
- Both the encrypted secret key and the encrypted combination of message and digest are sent together.



PGP at the Receiver site

- The receiver receives the combination of encrypted secret key and message digest is received.
- The encrypted secret key is decrypted by using the sender's private key to get the one-time secret key.

- The secret key is then used to decrypt the combination of message and digest.
- The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest.
- Both the digests are compared if both of them are equal means that all the aspects of security are preserved.



Disadvantages of PGP Encryption

- **The Administration is difficult:** The different versions of PGP complicate the administration.
- **Compatibility issues:** Both the sender and the receiver must have compatible versions of PGP. For example, if you encrypt an email by using PGP with one of the encryption technique, the receiver has a different version of PGP which cannot read the data.
- **Complexity:** PGP is a complex technique. Other security schemes use symmetric encryption that uses one key or asymmetric encryption that uses two different keys. PGP uses a hybrid approach that implements symmetric encryption with two keys. PGP is more complex, and it is less familiar than the traditional symmetric or asymmetric methods.
- **No Recovery:** Computer administrators face the problems of losing their passwords. In such situations, an administrator should use a special program to retrieve passwords. For example, a technician has physical access to a PC which can be used to retrieve a password. However, PGP does not offer such a special program for recovery; encryption methods are very strong so, it does not retrieve the forgotten passwords results in lost messages or lost files.

Secure/Multipurpose Internet Mail Extension (S/MIME)

Secure MIME (S/MIME) is an Internet standard for digitally signing MIME-based email data and its public key encryption. It was initially developed by RSA Security, Inc. and is based on the company's public key encryption mechanism. Most email services and software use S/MIME to secure email communication.

S/MIME enables email security features by providing encryption, authentication, message integrity and other related services. It ensures that an email message is sent by a legitimate sender and provides encryption for incoming and outgoing messages.

S/MIME Functionality

In terms of general functionality, S/MIME is very similar to PGP. Both offer the ability to sign and/or encrypt messages. In this subsection, we briefly summarize S/MIME capability. We then look in more detail at this capability by examining message formats and message preparation.

1. Functions

S/MIME provides the following functions:

- **Enveloped data:** This consists of encrypted content of any type and encrypted-content encryption keys for one or more recipients.
- **Signed data**: A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer. The content plus signature are then encoded using base 64 encoding. A signed data message can only be viewed by a recipient with S/MIME capability.
- **Clear-signed data:** As with signed data, a digital signature of the content is formed. However, in this case, only the digital signature is encoded using base 64. As a result, recipients without S/MIME capability can view the message content, although they cannot verify the signature.
- **Signed and enveloped data:** Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted.

2. Cryptographic Algorithms

- hash functions: SHA-1 & MD5
- digital signatures: DSS & RSA

- session key encryption: ElGamal & RSA
- message encryption: Triple-DES, RC2/40 and others

S/MIME uses the following terminology, taken from RFC 2119 to specify the requirement level:

Must: The definition is an absolute requirement of the specification. An implementation must include this feature or function to be in conformance with the specification.

Should: There may exist valid reasons in particular circumstances to ignore this feature or function, but it is recommended that an implementation include the feature or function.

IP Security Overview

Internet Protocol security (IPSec) is a framework of open standards for protecting communications over Internet Protocol (IP) networks through the use of cryptographic security services. IPSec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.

Need for IP Sec

In Computer Emergency Response Team (CERT)'s 2001 annual report it listed 52,000 security incidents in which most serious types of attacks included IP spoofing, in which intruders create packets with false IP addresses and exploit applications that use authentication based on IP and various forms of eavesdropping and packet sniffing, in which attackers read transmitted information, including logon information and database contents. In response to these issues, the IAB included authentication and encryption as necessary security features in the next-generation IP i.e. IPv6.

Applications of IP Sec

IPSec provides the capability to secure communications across a LAN, across private and public wide area networks (WAN's), and across the Internet.

- Secure branch office connectivity over the Internet: A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks,

saving costs and network management overhead.

• Secure remote access over the Internet: An end user whose system is equipped with IP security protocols can make a local call to an Internet service provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for travelling employees and telecommuters.

• Establishing extranet and intranet connectivity with partners: IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

• Enhancing electronic commerce security: Even though some Web and electronic commerce applications have built-in security protocols, the use of IPsec enhances that security.

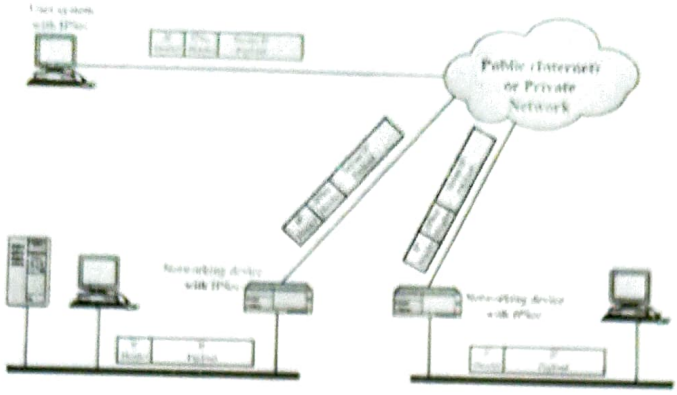
The principal feature of IPsec enabling it to support varied applications is that it can encrypt and/or authenticate all traffic at IP level. Thus, all distributed applications, including remote logon, client/server, e-mail, file transfer, Web access, and so on, can be secured.

Benefits of IPsec

The benefits of IPsec are listed below:

- IPsec in a firewall/router provides strong security to all traffic crossing the perimeter
- IPsec in a firewall is resistant to bypass.
- IPsec is below transport layer (TCP,UDP), hence transparent to applications
- IPsec can be transparent to end users
- IPsec can provide security for individual users if needed (useful for offsite workers and setting up a secure virtual sub network for sensitive applications)

IPsec Scenario

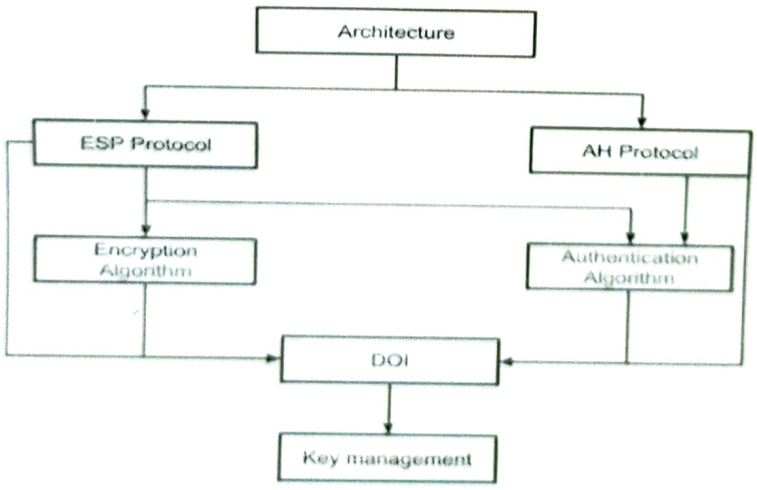


IPSec Architecture

IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture include protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

- Confidentiality
- Authentication
- Integrity

IP Security Architecture:



1. **Architecture:**

   Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms and security requirements of IP Security technology.

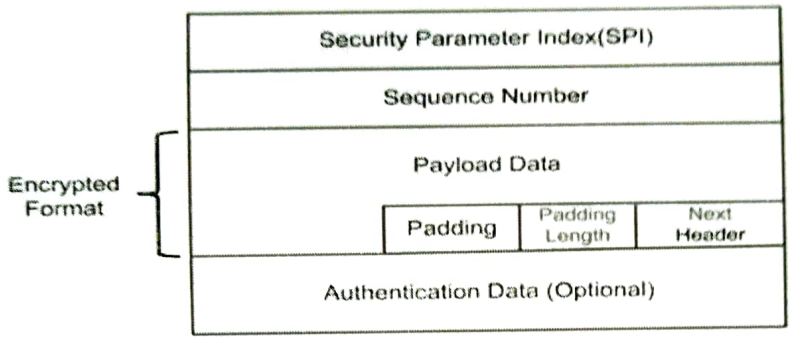
2. **ESP Protocol:**

ESP (Encapsulation Security Payload) provide the confidentiality service.

Encapsulation Security Payload is implemented in either two ways:

- ESP with optional Authentication.
- ESP with Authentication.

Packet Format:



- **Security Parameter Index (SPI):**

This parameter is used in Security Association. It is used to give a unique number to the connection build between Client and Server.

- **Sequence Number:**

Unique Sequence number are allotted to every packet so that at the receiver side packets can be arranged properly.

- **Payload Data:**

Payload data means the actual data or the actual message. The Payload data is in encrypted format to achieve confidentiality.

- **Padding:**

Extra bits or space added to the original message in order to ensure confidentiality.

Padding length is the size of the added bits or space in the original message.

- **Next Header:**

Next header means the next payload or next actual data.

- **Authentication Data**

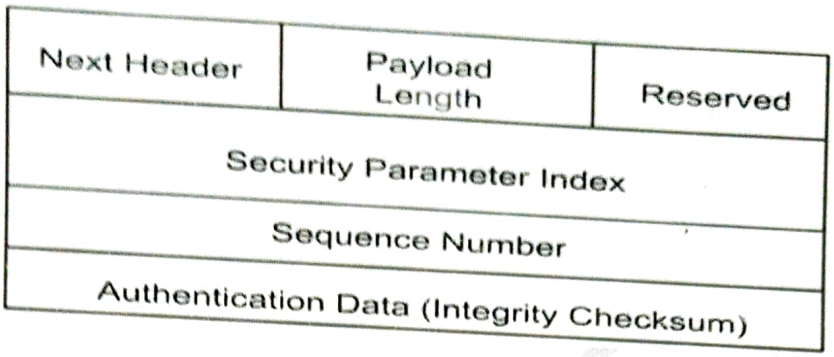
This field is optional in ESP protocol packet format.

3. **Encryption algorithm:**

Encryption algorithm is the document that describes various encryption algorithm used for Encapsulation Security Payload.

4. **AH Protocol:**

AH (Authentication Header) Protocol provides both Authentication and Integrity service. Authentication Header is implemented in one way only: Authentication along with Integrity.

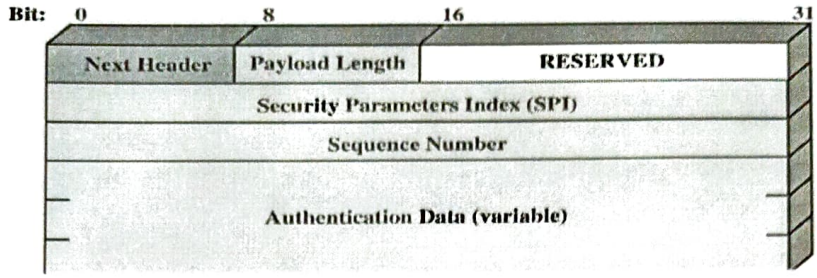


Authentication Header covers the packet format and general issue related to the use of AH for packet authentication and integrity.

5. **Authentication Algorithm:**
   Authentication Algorithm contains the set of the documents that describe authentication algorithm used for AH and for the authentication option of ESP.
6. **DOI (Domain of Interpretation):**
   DOI is the identifier which support both AH and ESP protocols. It contains values needed for documentation related to each other.
7. **Key Management:**
   Key Management contains the document that describes how the keys are exchanged between sender and receiver.

Authentication Header

The Authentication Header provides support for data integrity and authentication of IP packets. The data integrity feature ensures that undetected modification to a packet's content in transit is not possible. The authentication feature enables an end system or network device to authenticate the user or application and filter traffic accordingly; it also prevents the address spoofing attacks observed in today's Internet. The AH also guards against the replay attack. Authentication is based on the use of a message authentication code (MAC), hence the two parties must share a secret key. The Authentication Header consists of the following fields:

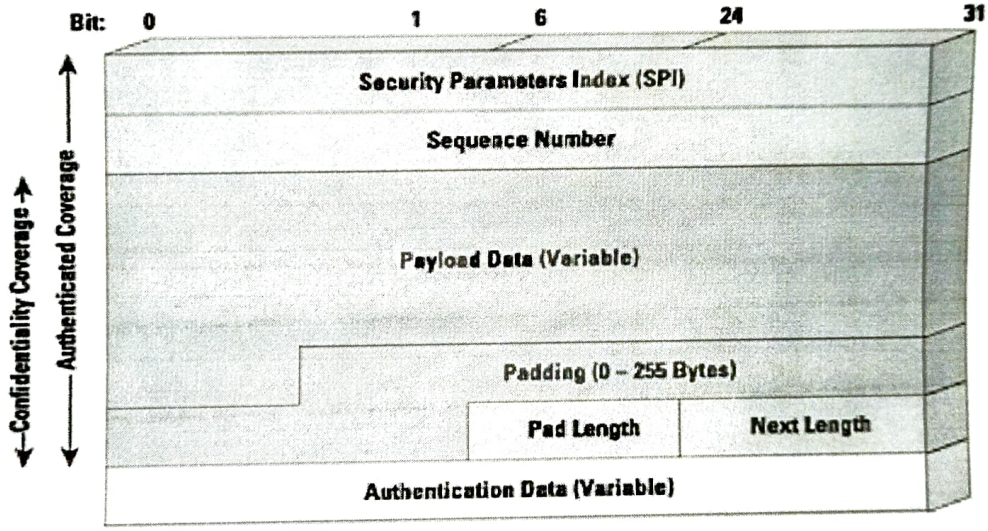


Encapsulating Security Payload

The Encapsulating Security Payload provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality. As an optional feature, ESP can also provide an authentication service.

ESP Format

The following figure shows the format of an ESP packet. It contains the following fields:



Unit V

Web Security

What is website security?

Website security is any action or application taken to ensure website data is not exposed to cybercriminals or to prevent exploitation of websites in any way.

Website security protects your website from:

DDoS attacks **(Distributed Denial-Of-Service)**.These attacks can slow or crash your site entirely, making it inaccessible to visitors.

Malware. Short for —malicious software,I malware is a very common threat used to steal sensitive customer data, distribute spam, and allow cybercriminals to access your site, and more.

Blacklisting. Your site may be removed from search engine results and flagged with a warning that turns visitors away if search engines find malware.

Vulnerability exploits. Cybercriminals can access a site and data stored on it by exploiting weak areas in a site, like an outdated plugin.

Defacement. This attack replaces your website's content with a cybercriminal's malicious content.

Website security protects your visitors from:

Stolen data. From email addresses to payment information, cybercriminals frequently go after visitor or customer data stored on a site.

Phishing schemes. Phishing doesn't just happen in email – some attacks take the form of web pages that look legitimate but are designed to trick the user into providing sensitive information.

Session hijacking. Some cyber-attacks can take over a user's session and force them to take unwanted actions on a site.

Malicious redirects. Certain attacks can redirect visitors from the site they intended to visit to a malicious website.

SEO Spam (Search Engine Optimization). Unusual links, pages, and comments can be put on a site to confuse your visitors and drive traffic to malicious websites

Web security Threats

Table 16.1 A Comparison of Threats on the Web

	Threats	Consequences	Countermeasures
Integrity	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerability to all other threats	Cryptographic checksums
Confidentiality	• Eavesdropping on the net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server	• Loss of information • Loss of privacy	Encryption, Web proxies
Denial of Service	• Killing of user threads • Flooding machine with bogus requests • Filling up disk or memory • Isolating machine by DNS attacks	• Disruptive • Annoying • Prevent user from getting work done	Difficult to prevent
Authentication	• Impersonation of legitimate users • Data forgery	• Misrepresentation of user • Belief that false information is valid	Cryptographic techniques

SSL (Secure Socket Layer)

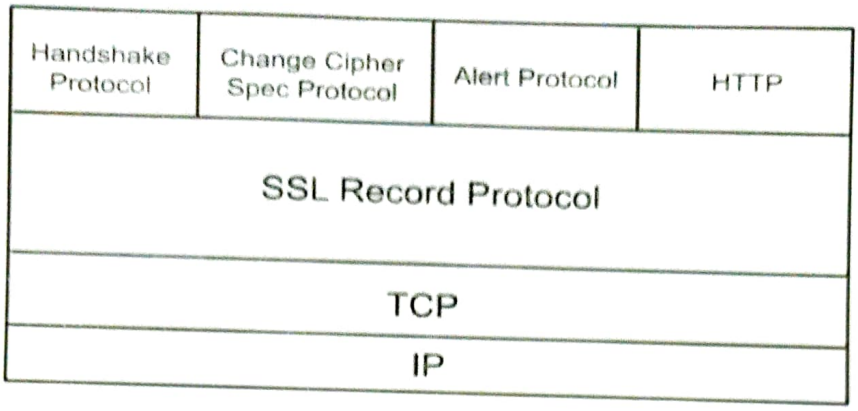
SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol. It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications.

Secure Socket Layer (SSL) provide security to the data that is transferred between web browser and server. SSL encrypt the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

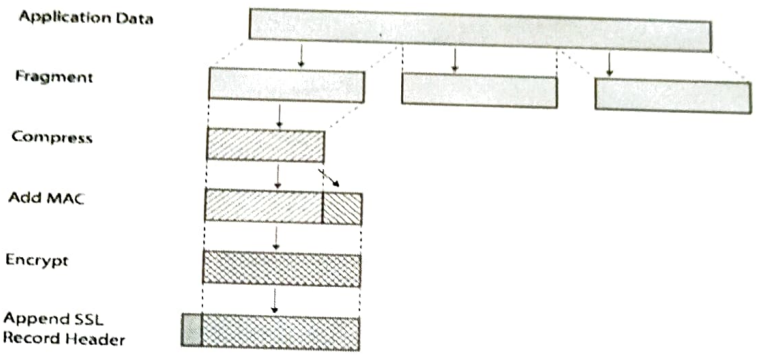
- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

SSL Architecture



SSL Record Protocol

SSL Record Protocol Operation



SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

3 higher layer protocols are defined as part of SSL

Handshake Protocol:

Handshake Protocol is used to establish sessions. This protocol allows client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

- Phase-1: In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purpose.
- Phase-2: Server send his certificate and Server-key-exchange. Server end the phase-2 by sending Server-hello-end packet.
- Phase-3: In this phase Client reply to the server by sending his certificate and

Client-exchange-key.

- Phase-4: In Phase-4 Change-cipher suite occurred and after this Handshake Protocol ends.

Change-cipher Protocol:

This protocol uses SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in pending state. After handshake protocol the Pending state is converted into Current state.

Alert Protocol:

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.

Transport Layer Security (TLS)

Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called Secure Service Layer (SSL).

There are several benefits of TLS

Encryption:

TLS/SSL can help to secure transmitted data using encryption.

Interoperability:

TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.

Algorithm flexibility:

TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.

Ease of Use:

Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

What does TLS do?

There are three main components to what the TL protocol accomplishes: Encryption, Authentication, and Integrity.

- **Encryption:** hides the data being transferred from third parties.
- **Authentication:** ensures that the parties exchanging information are who they claim to be.
- **Integrity:** verifies that the data has not been forged or tampered with.

Two important TLS concepts are the TLS session and the TLS connection, which are defined in the specification as follows:

- Connection: A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For TLS, such connections are peer to-peer relationships.
- Session: A TLS session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections.

TLS Protocols

1. **Record Protocol**: The SSL Record Protocol provides two services for SSL connections.

- Confidentiality: The Handshake Protocol defines a shared secret key that is used for symmetric encryption of SSL payloads.
- Message integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

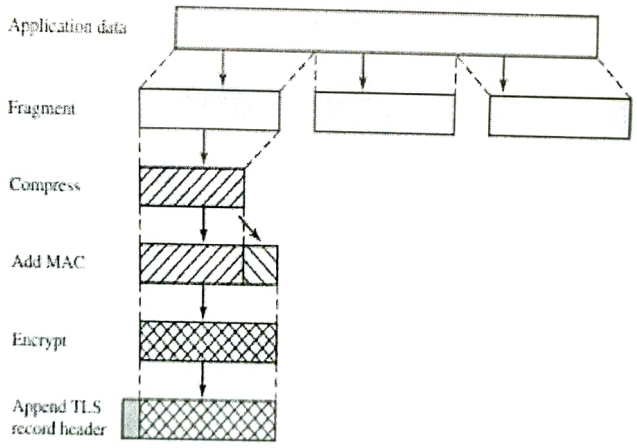


Figure 22.5 **TLS Record Protocol Operation**

2. **Change Cipher Spec Protocol**

The Change Cipher Spec Protocol is one of the four TLS-specific protocols that use the TLS Record Protocol, and it is the simplest. This protocol consists of a single message, which consists of a single byte with the value 1. The sole purpose of this message is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.

3. Alert Protocol

The Alert Protocol is used to convey TLS-related alerts to the peer entity. As with other applications that use TLS, alert messages are compressed and encrypted, as specified by the current state.

Handshake Protocol The most complex part of TLS is the Handshake Protocol. This protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in a TLS record. The Handshake Protocol is used before any application data are transmitted.

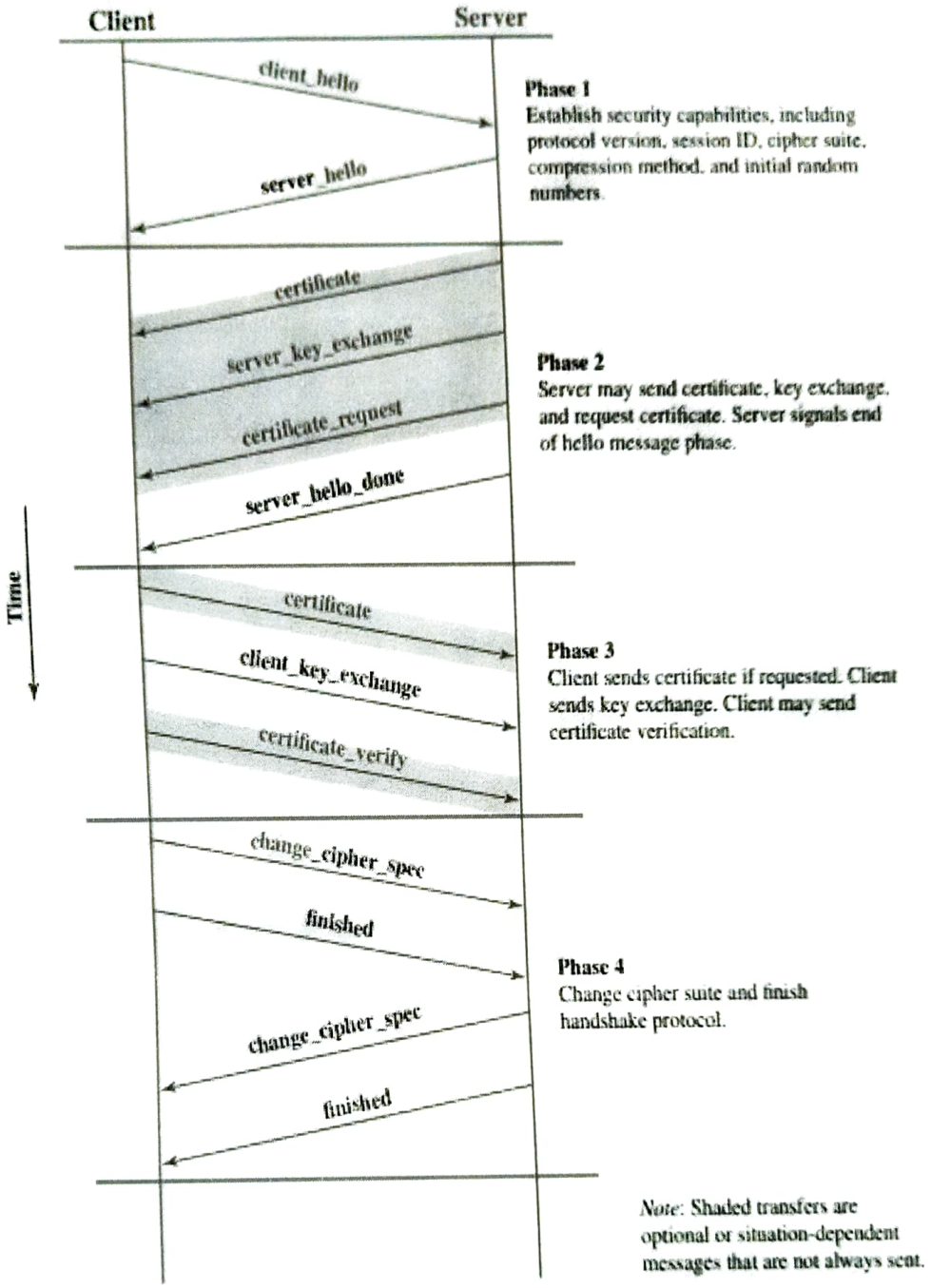


Figure 22.6 **Handshake Protocol Action**

SSL and TLS

- The TLS Record Format is the same as that of the SSL Record Format
- Fields in the header have the same meanings. The one difference is in version values.
- For the current version of TLS, the Major Version is 3 and the Minor Version is 1

Secure Electronic Transaction

SET is an open encryption and security specification designed to protect credit card transactions on the Internet. SET is not itself a payment system. Rather it is a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network, such as the Internet, in a secure fashion.

SET provides three services:

- provides a secure communications channel among all parties involved in a transaction
- Provides trust by the use of X.509v3 digital certificates
- Ensures privacy because the information is only available to parties in a transaction when and where necessary.

Key Features of SET

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication

SET Participants Cardholder:

A cardholder is an authorized holder of a payment card (e.g., MasterCard, Visa) that has been issued by an issuer.

Merchant:

A merchant is a person or organization that has goods or services to sell to the

Cardholder.

Issuer: This is a financial institution, such as a bank, that provides the cardholder with the payment card.

- **Acquirer:**

This is a financial institution that establishes an account with a merchant and processes payment card authorizations and payments.

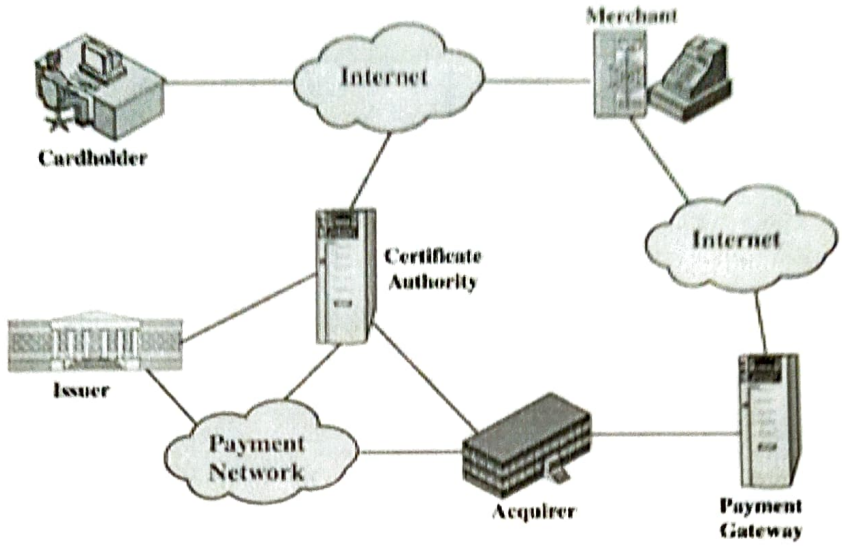
Payment gateway:

This is a function operated by the acquirer or a designated third party that processes merchant payment messages.

Certification authority (CA):

This is an entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways.

SET Participants



Sequence of events for transactions

1. The customer opens an account.
2. The customer receives a certificate.
3. Merchants have their own certificates.
4. The customer places an order.
5. The merchant is verified.
6. The order and payment are sent.
7. The merchant request payment authorization.
8. The merchant confirm the order.
9. The merchant provides the goods or service.
10. The merchant requests payments.

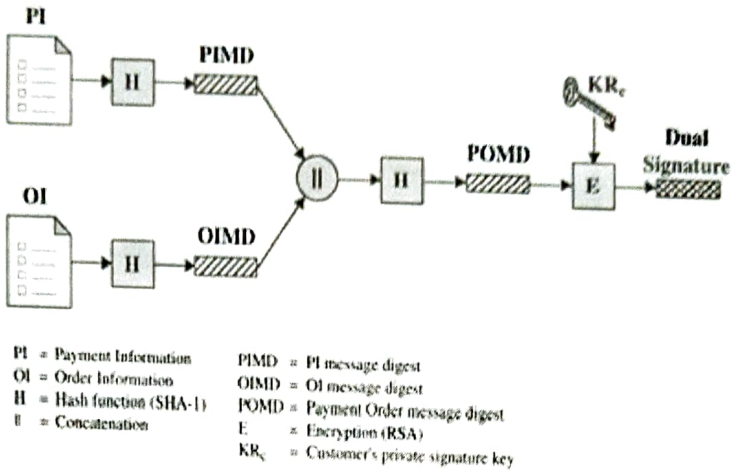
Dual Signature

Before looking at the details of the SET protocol, let us discuss an important innovation introduced in SET: the dual signature. The purpose of the dual signature is to link two messages that are intended for two different recipients. In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank. The merchant does not need to know the customer's credit card number, and the bank does not need to know the details of the customer's order.

The customer is afforded extra protection in terms of privacy by keeping these two

items separate.

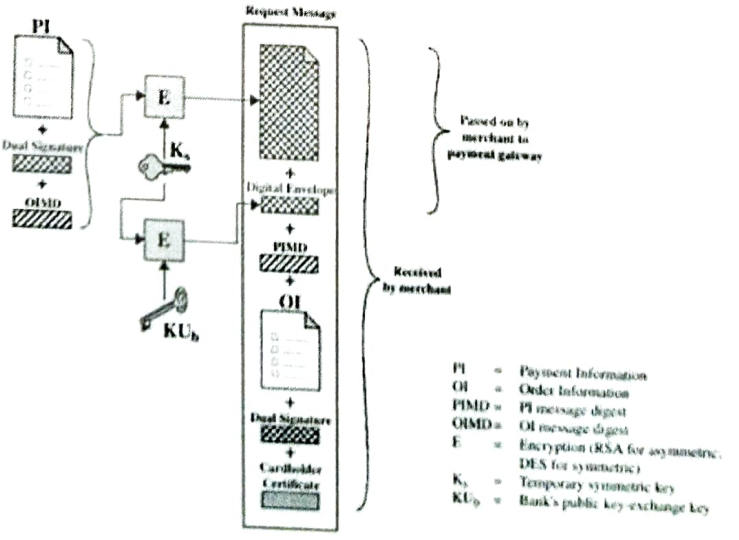
However, the two items must be linked in a way that can be used to resolve disputes if necessary. The link is needed so that the customer can prove that this payment is intended for this order and not for some other goods or service.

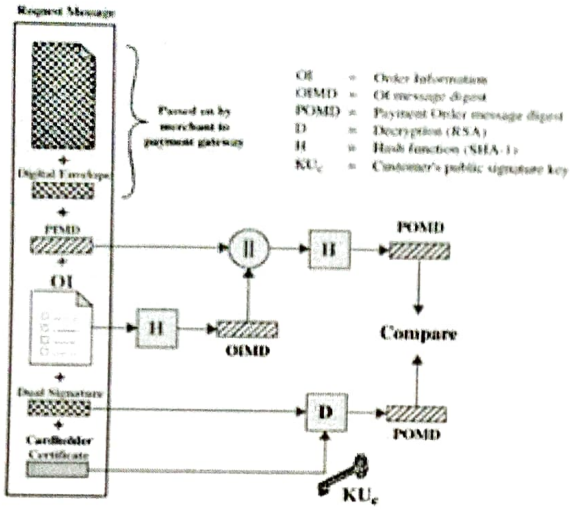


Payment Processing

- **Purchase request**
- **Payment authorization**
- **Payment capture**

Card Holder sends a purchase request





Merchant Verifies Customer Purchase Request

Payment Authorization

During the processing of an order from a cardholder, the merchant authorizes the transaction with the payment gateway. The payment authorization ensures that the transaction was approved by the issuer. This authorization guarantees that the merchant will receive payment.

The payment authorization exchange consists of two messages:

- **Authorization Request and**
- **Authorization response.**

Payment Capture

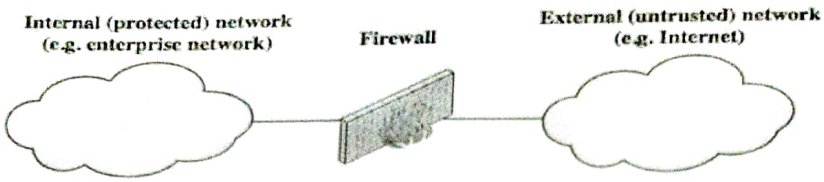
To obtain payment, the merchant engages the payment gateway in a payment capture transaction, consisting of a capture request and a capture response message.

It consists of two things

- **Capture Request**
- **Capture Response**

Firewalls

Firewalls can be an effective means of protecting a local system or network of systems from network based security threats while at the same time affording access to the outside world via wide area networks and the Internet.



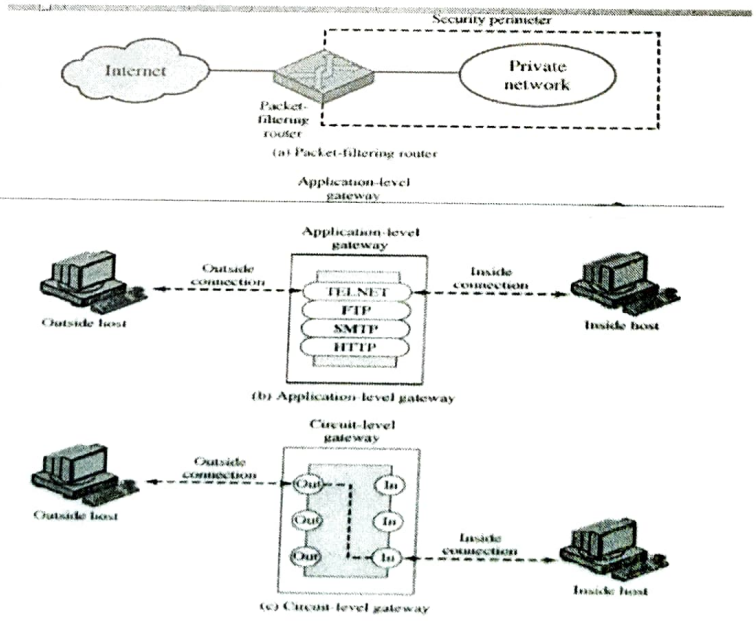
Firewalls have their limitations, including the following:

1. The firewall cannot protect against attacks that bypass the firewall.
2. The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
3. The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.

Types of Firewalls

Figure illustrates the three common types of firewalls:

- **packet filters**
- **application-level gateways**
- **circuit-level gateways.**



Packet-Filtering Router

A packet-filtering router applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. The router is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet

Application-Level Gateway

An application-level gateway, also called a proxy server, acts as a relay of application-level traffic. Application-level gateways tend to be more secure than packet filters. Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application-level gateway need only scrutinize a few allowable applications. In addition, it is easy to log and audit all incoming traffic at the application level.

Circuit-Level Gateway

A third type of firewall is the circuit-level gateway. This can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications. A circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function Consists of determining which connections will be allowed.

MODEL QUESTION PAPER

B.sc Computer Science

COMPUTER SECURITY

Time: 3Hrs **Max Marks: 80**

PART A

Answer *any 10*.Each Carries *2 marks*

1. What is computer security?
2. What do you mean by threats?
3. What is cryptography?
4. What is one time pad?
5. Explain Caesar cipher.
6. What is intrusion?
7. Explain IDPS.

8. Explain network security.
9. Define PKI.
10. Explain about IP.
11. What is gateway?
12. What is web security

PART B

Answer *any 6.* Each Carries *5 marks*

13. Explain the principles of security. 14. What is stenography?
15. What is counter measures? 16. What is Pretty Good Privacy?
17. Explain S/MIME.
18. Explain about Encryption and decryption.
19. Explain Circuit level gateway.
20. Explain about Firewalls.
21. What is E-Mail security?

PART C

Answer *any 2.* Each Carries *15 marks*

22. Explain the different types of cryptography 23. Explain the different types of Threats and Attacks.
24. Draw and explain the IP security architecture and Authentication header.
25. Explain about Application level Gateway and Circuit level Gateway.