KLS Vishwanathrao Deshpande Institute of Technology

(Accredited by NAAC with "A" Grade)
(Approved by AICTE, New Delhi, Affiliated to VTU, Belagavi)
(Recognized Under Section 2(f) by UGC, New Delhi)
Udyog Vidya Nagar, Haliyal - 581 329, Dist.: Uttara Kannada
Phone: 08284 - 220861, 220334, 221409, Fax: 08284 - 220813
www.klsvdit.edu.in | principal@klsvdit.edu.in | hodece@klsvdit.edu.in

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

University / Model Question Paper
Scheme & Solution

Faculty Name	:	Prof. Shree Gowri S S
Course Name	:	Network Security
Course Code	:	18EC821
Year of Question Paper	:	June / July 2023
Date of Submission	:	03/04/2024

Faculty Member

HoD

Dean (Acad.)

CBCS SCHEME

USN | | | | | | | | | | 18EC821

Eighth Semester B.E. Degree Examination, June/July 2023
Network Security

Time: 3 hrs. Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Module-1

1 a. Illustrate the use of 4 chief principles necessary for providing security. (10 Marks)
b. The sole aim of the attacker is to maximize financial gain by attacking computer systems. Identify the attack and further elaborate the different varieties of same. (10 Marks)

OR

2 a. What is an active attack? Explain in detail how active attacks are classified. (10 Marks)
b. With real time examples, discuss phishing and pharming. (10 Marks)

Module-2

3 a. The web is faced with different types of security threats. Compare the threats on the web. (10 Marks)
b. Illustrate with diagram the step by step operation of SSL record protocol. Explain each step briefly. (10 Marks)

OR

4 a. Discuss the different alert codes supported by Transport Layer Security (TLS). (10 Marks)
b. With a neat diagram, explain Secure Shell (SSH) protocol stack. (10 Marks)

Module-3

5 a. Discuss applications of IP Sec. (05 Marks)
b. List and explain IP sec documents. (05 Marks)
c. Explain Transport and Tunnel modes. (10 Marks)

OR

6 a. Discuss the purpose of Padding and Anti-Replay service. (10 Marks)
b. Illustrate the working of basic combinations of security associations. (10 Marks)

Module-4

7 a. Explain 3 classes of intruders with examples, discuss intruder patterns of behavior. (10 Marks)
b. With a neat diagram, illustrate the profiles of intruder and authorized users. Also discuss approaches to intrusion detection. (10 Marks)

OR

8 a. Describe the overall taxonomy of software threats (Terminology of Malicious program). (10 Marks)

b. Explain the anti-virus approaches and also in detail discuss the generations of anti-virus software. (10 Marks)

Module-5

9 a. Explain the four general techniques that the fire wall use to control access. (06 Marks)

b. Discuss the capabilities which one within the scope of a firewall. (05 Marks)

c. With a neat diagram, describe the working of packet filtering fire wall. (10 Marks)

OR

10 a. Discuss the characteristics of Bastion Host. (10 Marks)

b. Explain Host based and personal firewalls. (06 Marks)

c. Explain the different purposes for which internal fire wall can be used. (04 Marks)

* * * * *

Module – 1

1a. Illustrate the use of 4 chief principles necessary for providing Security — 10 Marks.

Sol:- The 4 chief principles necessary for providing Security are

1) Confidentiality

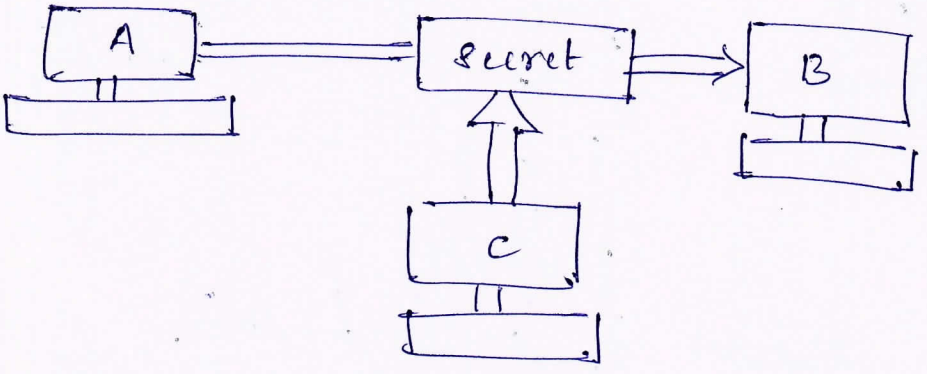


fig: Loss of confidentiality

The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person able to access a message.

With respect to above figure. The user of computer A sends a message to the user of computer B. Another user C gets access to this message, which is not desired & therefore, defeats the purpose of confidentiality. This type of attack is called interception.

2) Authentication.

Authentication mechanisms helps establish the proof of identities. The authentication process ensures the origin of an electronic message or document is correctly identified.

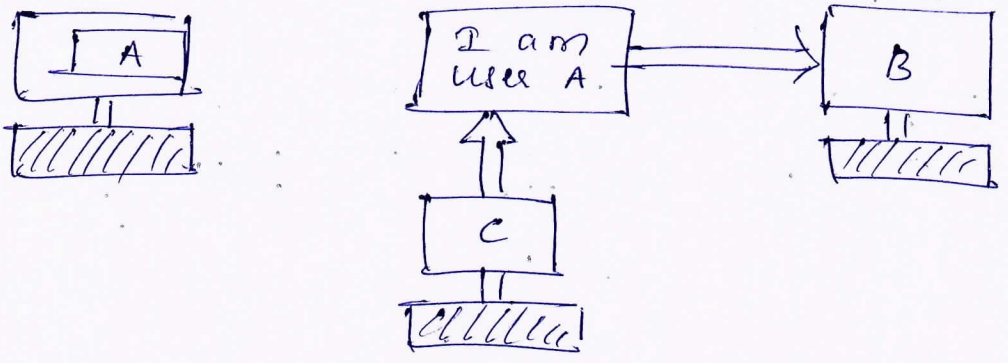


fig: Absence of authentication.

With respect to above figure user C sends an electronic document over the Internet to user B. However the trouble is that user C had posed as user A when she sent this document to user B. How would user B know that the message has come from user C, who is posing as user A. User C is posing as user A, sending a fund transfer request to bank B. The bank might happily transfer the funds from A's account to C's account. This type of attack is called as fabrication.

3) Integrity

When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost

4) Non-repudiation:

There are situations where a user send a message, and later on refuses that she had sent that message For instance, user A could send a funds transfer request as per A's instructions, A could claim that she never sent the fund transfer instruction to the bank. Then A repudiates, or denies her funds transfer instruction. This principle of non-repudiation defeats such possibilities of denying something.

16. The sole aim of the attackers is to maximize financial gain by attacking computer systems. Identify the attacks and further elaborate the different varieties of same..

Sol:- when the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost. Example:- Suppose if you write a cheque for $100 to pay for the goods bought from the US. However when you see your next account statement, you are startled to see that the cheque resulted in a payment of $1000. This is the case for loss of message integrity. Conceptually it is shown in fig

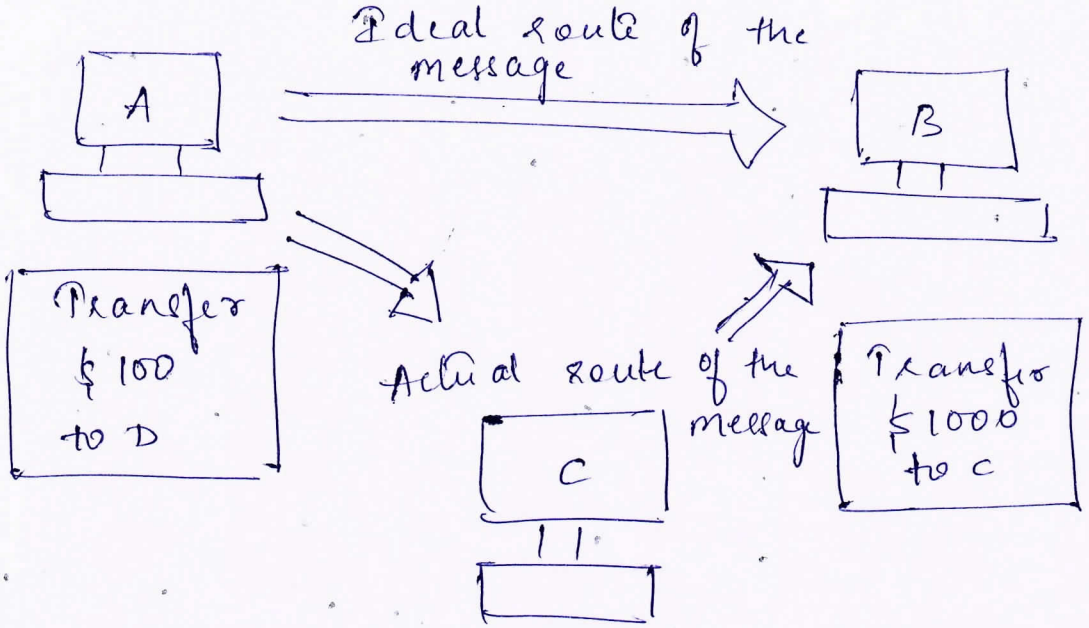


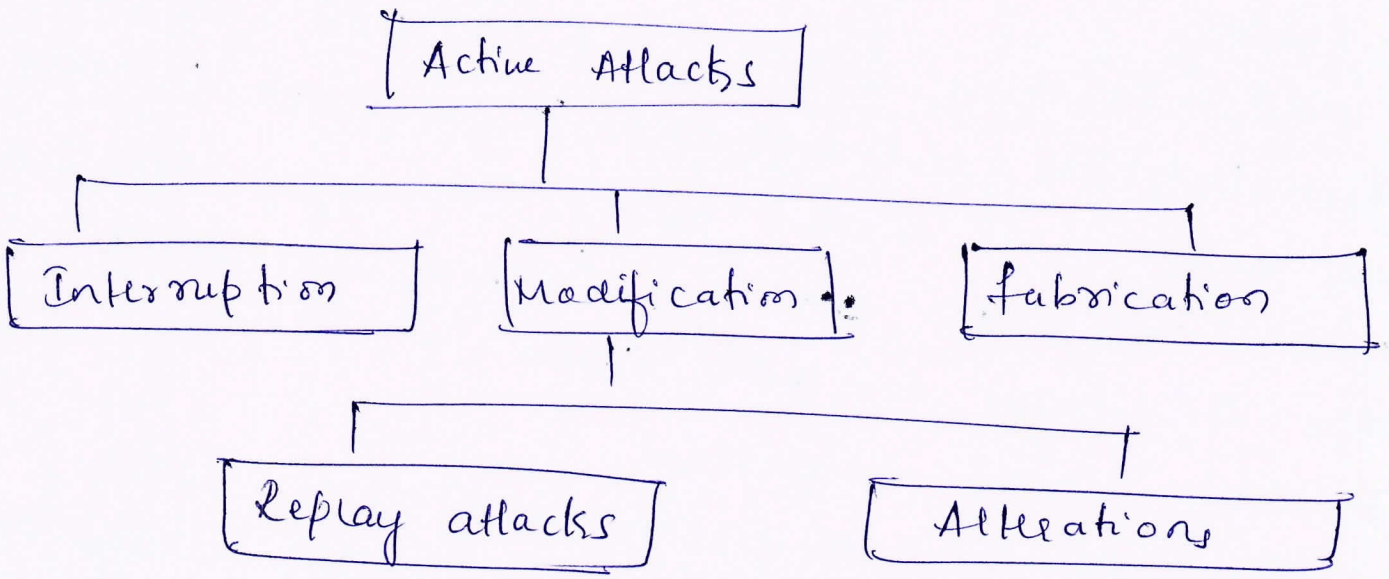
fig: loss of integrity

In the fig, user C tampers with a message originally sent by user A, which is actually destined for user B. User C somehow manages to access it, change its contents, & send the changed message to user B. User B has no way of knowing that the contents of the message were changed after user A had sent it. User A also does not know about this change. This type of attacks is called as modification.

OR

2 a what is an active attack? Explain in detail how active attacks are classified 10 Mar

Sol:- The active attacks are based on modification of the original message in some manner or creation of a ~~ft~~ false message. Active attacks can be detected with some effort & attempts can be made to recover from them. These attacks can be in the form of Interruption, modification and fabrication



Interruption attacks are called as masquerade attacks

Ex:- User C might pose as user A and send a message to user B.

Modification
~~Interruption~~ attacks can be classified into replay attacks and alteration of messages

Replay attacks:- user captures a sequence of events or some data units and resends them.

Alteration of messages involves some change to the original message

3. fabrication causes Denial of Service attacks

Does ~~not~~ attacks make an attempt to prevent legitimate users from accessing some services, which they are eligible for.

26. with real time examples, discuss phishing and pharming. — 10 Marks.

Sol:- Phishing

In ~~packet~~ phishing, attackers set up fake web sites, which look like real web sites. It is simple to create web pages as it involves simple technologies such as HTML, Javascript, CSS etc. Learning and using these technologies is quite simple

Phishing works as follows.

The attacker decides to create own web sites, The attacker sends an email to legitimate customers of the bank. The email appears to come from the bank. for ensuring this, the attacker exploits the email system to suggest that the sender of the email is some banks official

This fake email warns the user that there has been some sort of attack on citibanks computer sys - em and that the bank wants to issue new passwords to all its customers or verify their existing PINs etc

Pharming (DNS Spoofing)

This attack was earlier known as DNS spoofing or DNS poisoning is called as Pharming attacks with DNS, people can identify web sites with human readable names and computers can continue to treat them as IP addresses

Ex:- DNS spoofing attack works as follows

- Suppose that there is a merchant, whose site's domain name is www.bob.com and the IP address is 100.10.10.20 Therefore, the DNS entry for Bob in all the DNS server is maintained as follows : www.bob.com 100.10.10.20
- The attacker manages to hack and replace the IP address of Bob with his own in the DNS server maintained by the ISP of a user. Therefore the DNS server maintained by the ISP of Alice now has the following entry : www.bob.com 100.20.20.20

Thus the contents of the hypothetical DNS table maintained by the ISP would be changed.

When Alice wants to communicate with Bob's site, her web browser queries the DNS server maintained by her ISP for Bob's IP address, providing it the domain name. Alice gets the replaced IP address, which is 100.20.20.20

Module - 2

3 a. The web is faced with different types of security threats. compare the threats on web -10 Marks

Sol:-

	Threats	Consequences	Countermeasures
Integrity	1) Modification of user data 2) Trojan horse browser 3) Modification of Memory 4) Modification of message traffic in transit	1) loss of information 2) compromise of machine 3) Vulnerability to all other threats	Cryptographic checksums
Confidentiality	1) Eavesdropping on net 2) Theft of info from server 3) Theft of data from client 4) Info about n/w configuration	1) loss of information 2) loss of privacy	Encryption, web proxies
Denial of Service	1) Killing of user threats 2) flooding machine with bogus requests 3) filling up disks or memory	1) Disruptive 2) Annoying 3) Prevent user from getting work done	Difficult to prevent
Authentication	1) Impersonation of legitimate users 2) Data forgery	1) Misrepresentation of user 2) Belief that false information is valid	Cryptographic techniques

3b: Illustrate with diagram the step by step operation of SSL record protocol. Explain each step briefly — 10 marks.

Sol:- SSL Record protocol provides two services for SSL connections

1) confidentiality: The Handshake protocol defines a shared secret key that is used for conventional encryption of SSL payloads

2) Message Integrity: The Handshake protocol also defines a shared secret key that is used to perform a message authentication code (MAC)

Step-by-step operation of SSL Record

1) first step:- fragmentation:- Each upper layers message is fragmented into blocks of 2^{14} bytes or less

2) Second step:- Compression:- Compression is optionally applied. It must be lossless and may not increase the content length by more than 1024 bytes

3) Next step:- Message authentication code over the compressed data.

4) fourth step:- compressed message plus the MAC are encrypted using symmetric encryption. Encryption may not increase the content length by more than 1024 bytes, so the total length may not exceed $2^{14} + 2048$.

Head of the Department
Dept. of Electronics & Communication Engg.
KLS V.D.I.T. HALIYAL (U.K.)

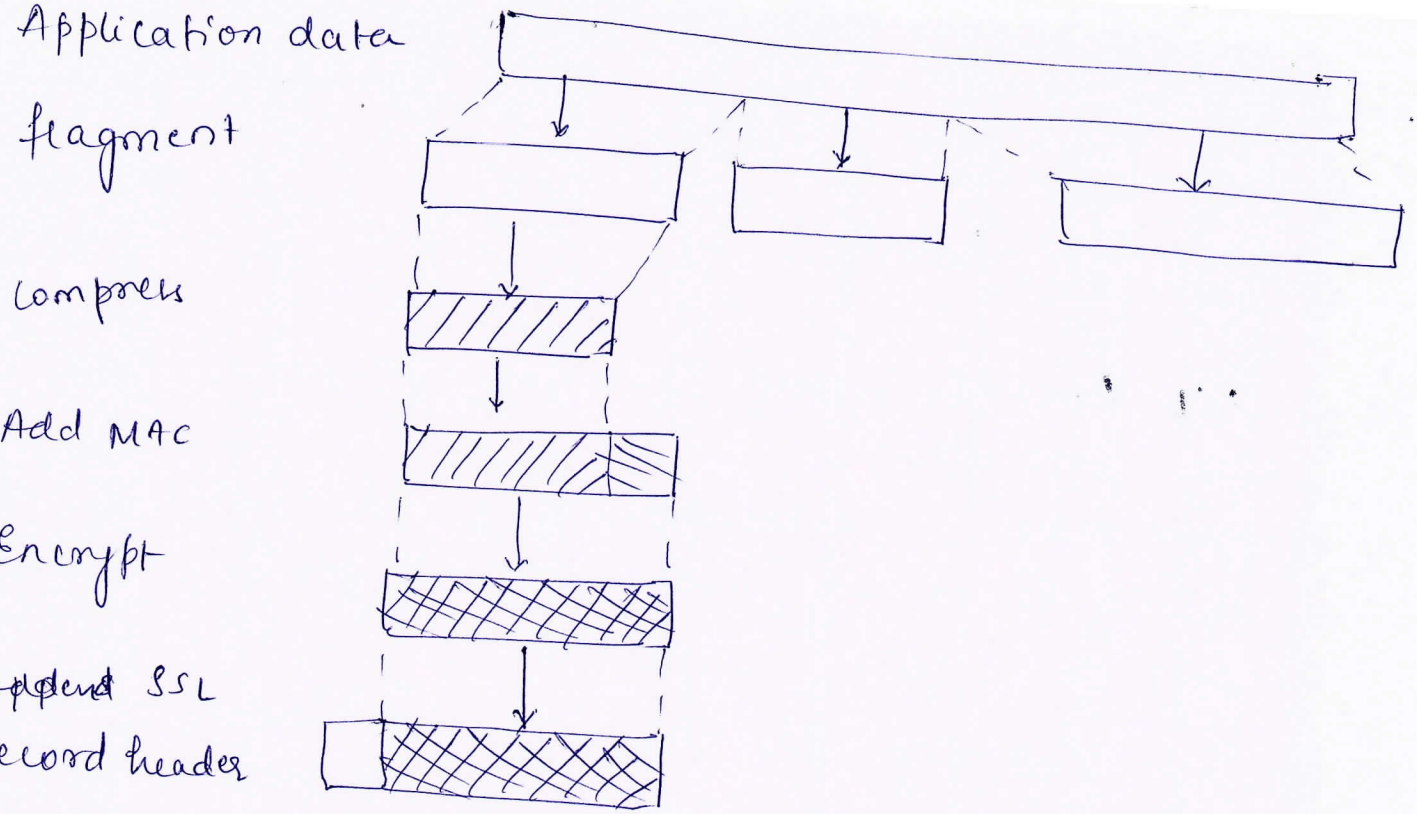


fig: SSL record protocol operations

OR

8a. Discuss the different alert codes supported by Transport layer security (TLS) – 10 Marks

Sol:- The different alert codes supported by TLS are

1) record_overflow:- A TLS record was received with a payload whose length exceeds $2^{14}+2048$ bytes or the ciphertext decrypted to a length of a greater than $2^{14}+1024$ bytes

2) Unknown_ca:- A valid certificate chain or partial chain was received, but the certificate was not accepted because the CA certificate could not be located or could not be matched with a known trusted CA

3) access_denied :- A valid certificate was received, but when access control was applied, the sender decided not to proceed with the negotiation.

4) decode_error : A message could not be decoded because either a field was out of its specified range or the length of the message was incorrect

5) Protocol_version : The protocol version the client attempted to negotiate is recognized but not supported

6) Insufficient_security :- Returned instead of handshake_failure when a negotiation has failed specifically because the server requires ciphers more secure than those supported by client.

7) unsupported_extension :- Sent by clients that receive an extended server hello containing an extension not in the corresponding client hello.

8) internal_error : An internal error unrelated to the peer or the correctness of the protocol makes it impossible to continue.

45. With a neat diagram, explain Secure Shell (SSH) protocol attacks. — 10 Marks

Sol:- SSH is organized as three protocols that typically run on top of TCP

1) Transport layer protocol :- Provides server authentication, data confidentiality, and data integrity with forward secrecy. The Transport layer may optionally provide compression.

2) User Authentication Protocol :- Authenticates the user to the server

3) Connection Protocol: Multiplexes multiple logical communications channels over a single, underlying SSH connection.

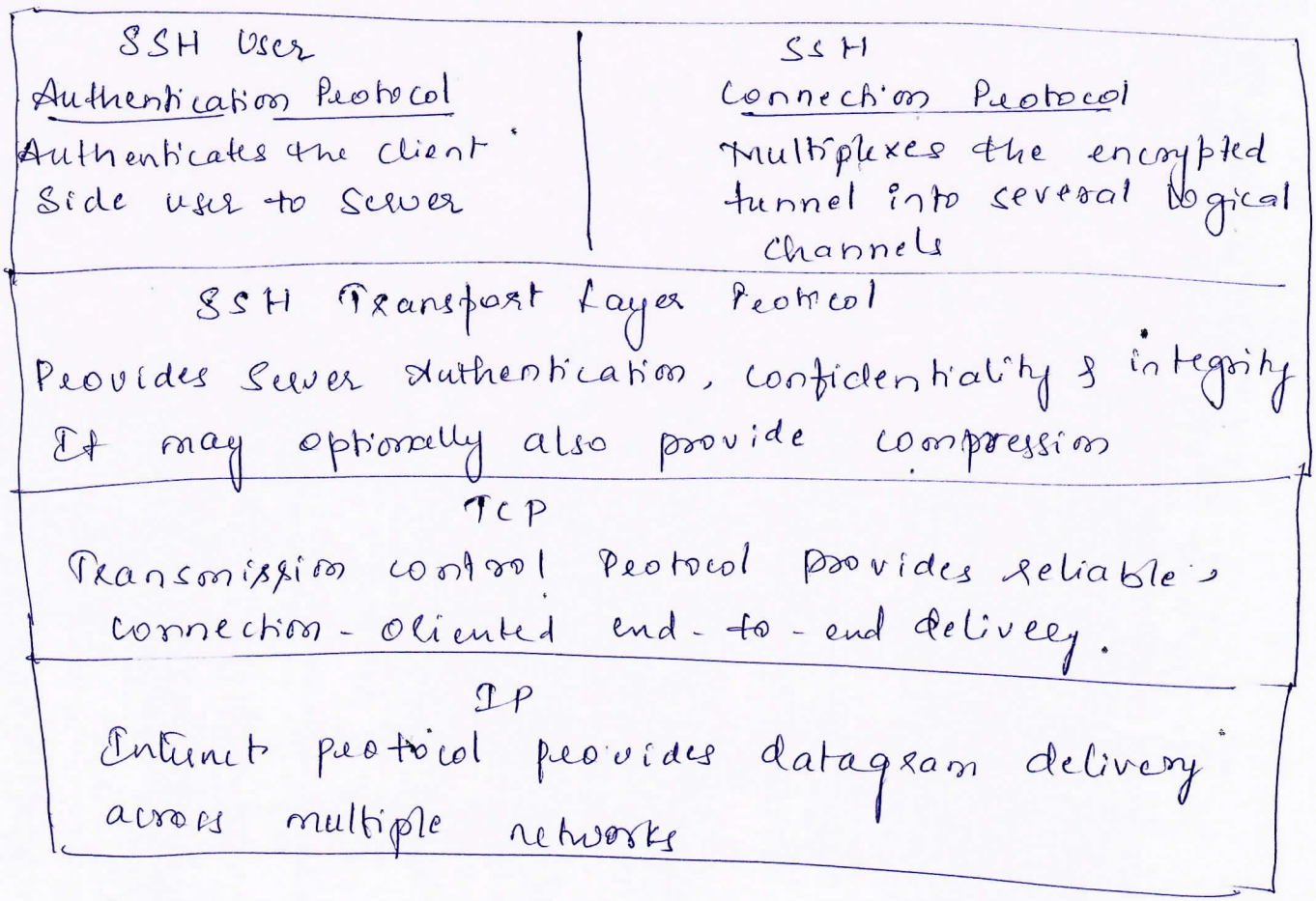


fig: SSH protocol Stack

Module -3

5a. Discuss application of IPsec — 05 marks

Sol:- applications of IP sec are

1) Secure branch office connectivity over the Internet: A company can build a secure virtual private network over the Internet or over a public WAN.

2) Secure remote access over the Internet: An end user whose system is equipped with IP security protocols can make a local call to an ISP and gain secure access to a company network.

3. 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

4. Enhancing electronic commerce security:- IP sec guarantees that all traffic designated by the network's administrator is both encrypted and authenticated, adding an additional layer of security to whatever is provided at the application layer.

5b. List and explain IP sec documents — 05 marks

Sol:- The IPsec documents are

1) Architecture: Covers the general concepts, security requirements, definitions and mechanisms defining IPsec technology. The current specification is RFC 4301, Security Architecture for the Internet Protocol.

2. Authentication Header (AH):- AH is an extension header to provide message authentication. Because message authentication is provided by ESP, the use of AH is deprecated. It is included in IPSecV3 for backward compatibility but should not used in new applications.

3. Encapsulating Security payload (ESP):- ESP consists of an encapsulating header and trailer used to provide encryption or combined encryption/ authentication

4. Internet key Exchange (IKE), This is a collection of documents describing the key managment schemes for use with IPsec

5. Cryptographic algorithms: This category ~~documen~~ encompasses a large set of documents that define and describe cryptographic algorithms for encryption, message authentication, Pseudorandom functions and cryptographic key exchange

Q4. Explain Transport and Tunnel Modes — 10 Marks

Sol:- Transport Mode

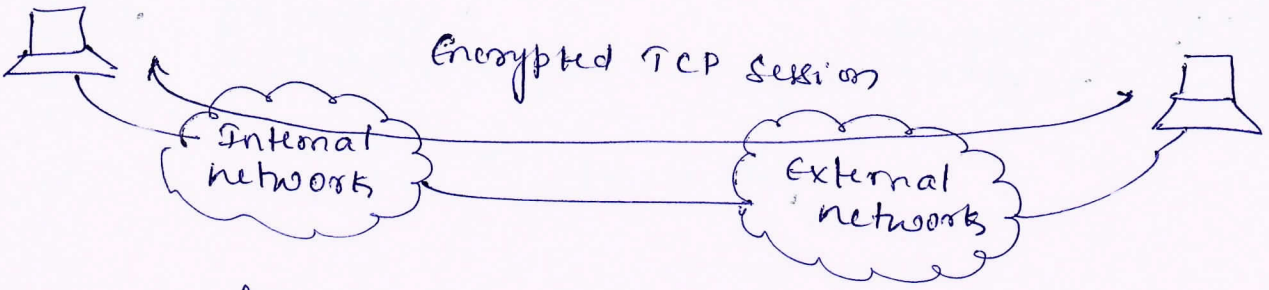
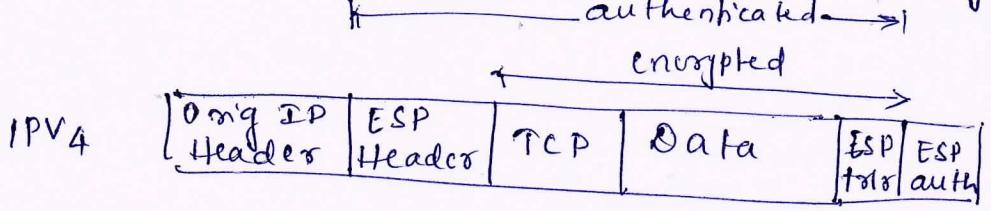


fig: Transport-level security



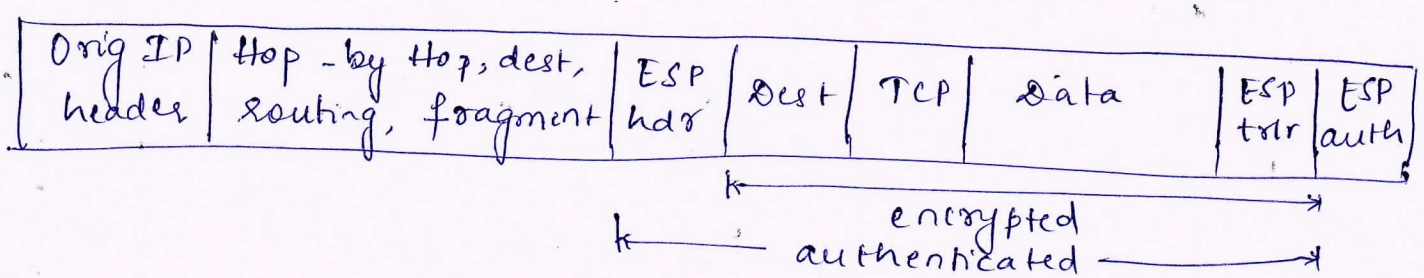


fig: Transport Mode (Scope of ESP Encryption & Authentication)

Transport mode ESP is used to encrypt and optionally authenticate the data carried by IP. For this mode ~~IPV4~~ using IPV4, the ESP Header is inserted into the IP packet immediately prior to the transport-layer header and an ESP Trailer is placed after the IP packet. If authentication is selected, the ESP Authentication Data field is added after the ESP trailer. The entire transport level segment plus the ESP trailer are encrypted. Authentication covers all of the ciphertext plus the ESP Header.

In IPV6, ESP is viewed as an end-to-end payload, i.e it is not examined or processed by intermediate routers.

a) Tunnel Mode :-

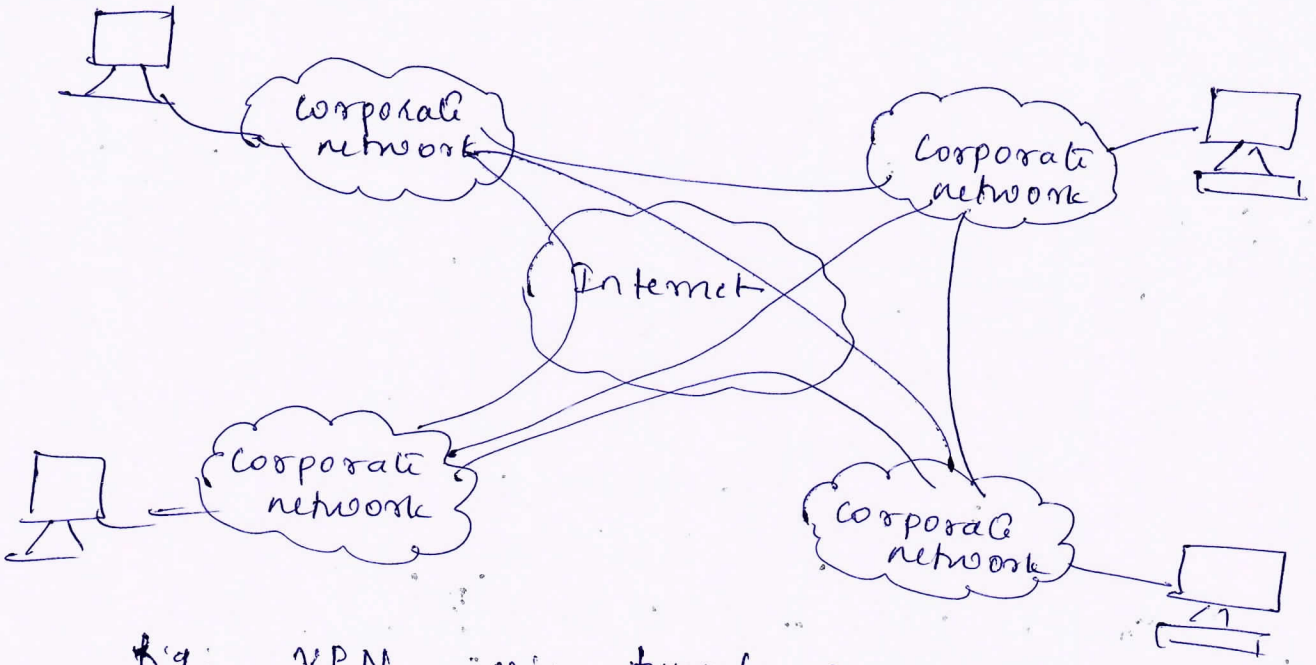
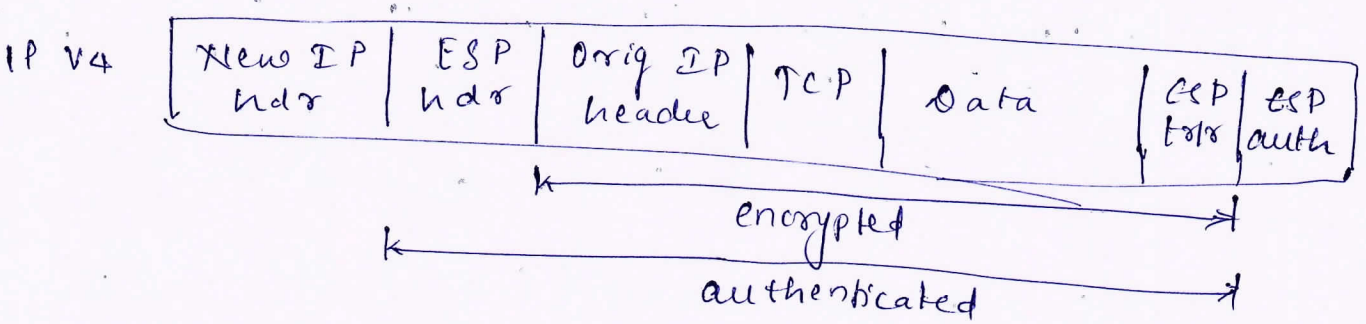


Fig: VPN via tunnel Mode



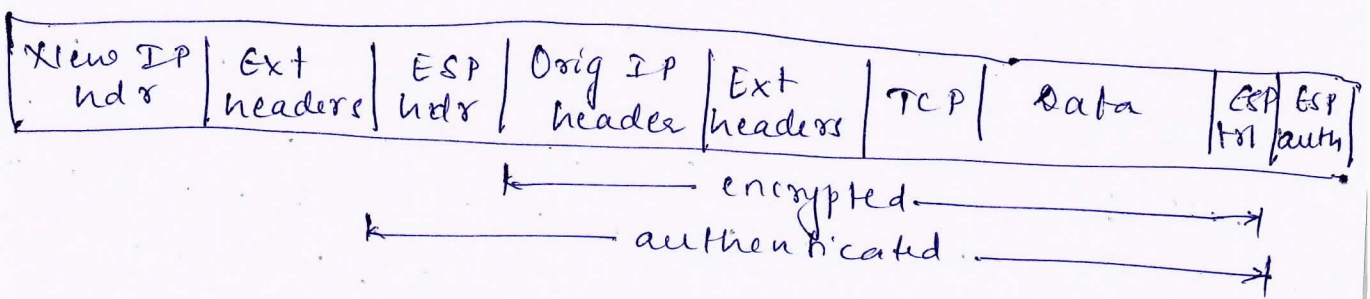


Fig: Tunnel Mode

Tunnel mode ESP is used to encrypt an entire IP packet. For this mode, the ESP header is prefixed to the packet and then the packet plus the ESP trailer is encrypted. This method can be used to counter traffic analysis. The IP header contains the destination address and possibly source routing directive and hop-by-hop option information, it is not possible simply to transmit the encrypted IP

packet prefixed by the ESP Header. Intermediate routers would be unable to process such a packet. Therefore, it is necessary to encapsulate the entire block with a new IP header that will contain sufficient information for routing but not for traffic analysis.

OR

6 a. Discuss the purpose of padding and Anti-replay Service — 10 Marks

Sol:- Padding serves several purposes

1) If an encryption algorithm requires the plaintext to be a multiple of some number of bytes, the padding field is used to expand the plaintext to the required length.

2) The ESP format requires that the Pad length and Next Header fields be right aligned within a 32-bit word. Equivalently, the ciphertext must be an integer multiple of 32-bits. The padding field is used to assure this alignment

3) Additional padding may be added to provide partial traffic-flow confidentiality by concealing the actual length of the payload.

Sri

Anti - Replay Service

A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence. The Sequence Number field is designed to thwart such attacks.

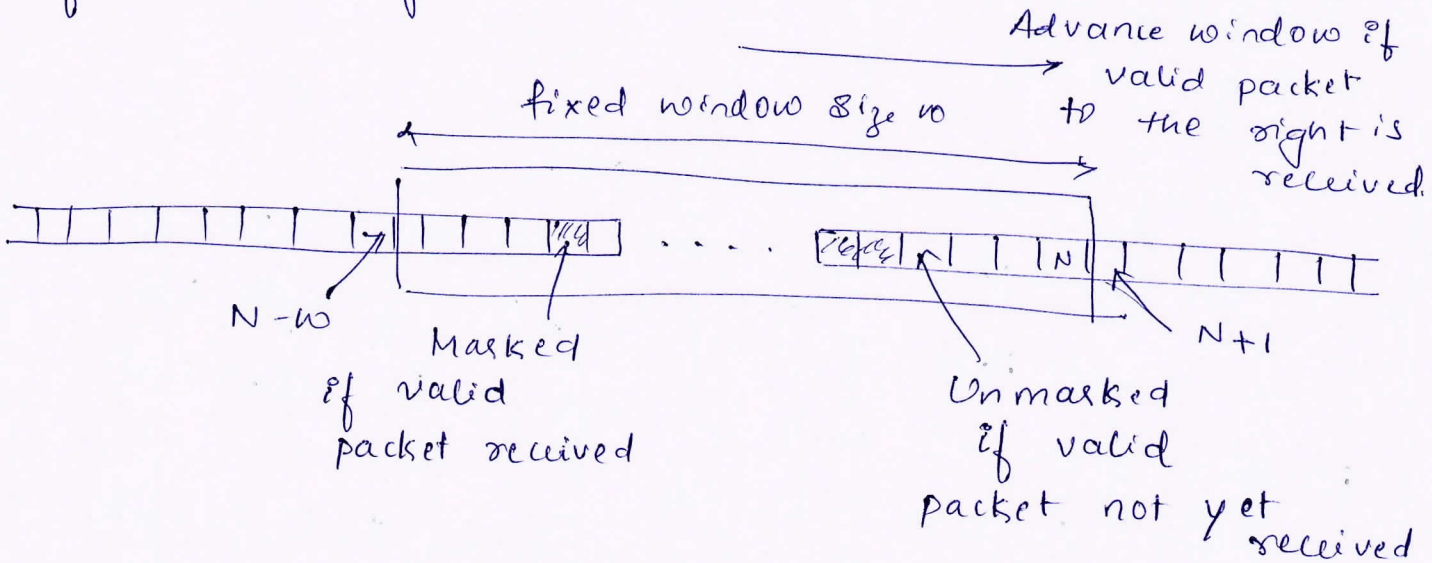


fig: Anti - replay mechanism.

Inbound processing proceeds as follows when packet is received.

1. If the received packet falls within the window and is new, the MAC is checked. If the packet is authenticated, the corresponding slot in the window is masked.

2. If the received packet is to the right of the window and is new, the MAC is checked. If the packet is authenticated, the window is advanced so that this sequence number is the right edge of the window, corresponding slot in the

... of the received packet is to left of the window or if authentication fails, the packet is discarded

6b. Illustrate the working of basic combinations of security associations — 10 Marks.

Sol:- Security associations may be combined into bundle in two ways

1. Transport adjacency:- Refers to applying more than one security protocol to the same IP packet without invoking tunneling. This approach to combining AH and ESP allows for only one level of combination further nesting yields no added benefit since the processing is performed to one IPsec instance, the destination.

2. Iterated Tunneling:- Refers to the application of multiple layers of security protocols effected through IP tunneling. The approach allows for multiple levels of nesting. Since each tunnel can originate, or terminate at a different IPsec site along the path.

The two approaches can be combined, for example, by having a transport SA between hosts travel part of the way through a tunnel SA between security gateways.

Module - 4

7 a. Explain 3 classes of intruders with examples, discuss intruder patterns of behavior — 10 Marks

Sol :— The three classes of intruder are

1) Masquerader: 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

2) Misfeasor :- 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.

3) clandestine User :- An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or suppress audit collection.

The masquerader is likely to be an outsider, the misfeasor generally is an insider and the clandestine user can be either an outside or an insider.

Intruder attacks range from the benign to the serious. At the benign end of the scale, there are many people who simply wish to explore internets and see what is out there.

diagram, illustrate the profiles of intruder and authorized users. Also discuss approaches to intrusion detection — 10 Mark

Sol:- The two principal counter measures for intruders are
1) detection or prevention

1) Detection is concerned with learning of an attacks, either before or after its success

2) Prevention is a challenging security goal and an uphill battle at all things

The following are the approaches to intrusion detection

1) Statistical anamaly detection:- Involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior

- Threshold detection
- Profile based

2 Rule-based detection:- Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder

1) Anamaly detection
2) Penetration identification

OR

8 a. Describe the overall taxonomy of software threats -10 Marks

Sol:- Malicious software is software that is intentionally included or inserted in a system for a harmful purpose. The most sophisticated type of threats to computer systems are presented by programs that exploit vulnerabilities in computing systems. Such threats are referred to as malicious software or malware.

Malicious software can be divided into two categories

Those that need a host program & those that are independent. The former, referred to as parasitic, are essentially fragments of programs that cannot exist independently of some actual application program, utility, or system program. Viruses, logic bombs and backdoors are example

Independent malware is a self-contained program that can be scheduled and run by the operating system. Worms and bot programs are example.

Q5. Explain the anti-virus approaches and also in detail discuss the generations of antivirus software — 10 Marks

Sol:- The ideal solution to the threat of viruses is prevention: Do not allow a virus to get into the system in the first place, or block the ability of a virus to modify any files containing executable code or macros.

This goal is, in general, impossible to achieve, although prevention can reduce the number of successful viral attacks.

The four generations of anti virus software

1. first generation: Simple Scanners
2. Second generation: Heuristic Scanners
3. Third generation: activity traps
4. Fourth generation: full-featured protection.

1. first generation:- Scanner requires a virus signature to identify a virus. The virus may contain "wildcards" but has essentially the same structure and bit patterns in all copies. Such signature specific scanners are limited to the detection of known viruses. ~~Another~~

2. Second generation:- Scanner do not rely on specific signature. Rather the scanner uses heuristic rules to search for probable virus infection.

· Third generation :- Programs are memory resident programs that identify a virus by its actions rather than its structure in an infected program.

Fourth-generation:- Products are packages consisting of a variety of antivirus techniques used in conjunct These include scanning and activity trap components. In addition such a package includes access control capability, which limits the ability of viruses to penetrate a system & then limits the ability of a virus to update files in order to pass on the infection.

Module - 5

9 a. Explain the four techniques that the fire wall use to control access — 05 marks

Sol :- The four techniques that the fire wall use to control access are

1) Service control :- Determine the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address, protocol or port number. may provide proxy software that receives and interprets each service request before passing it on, or may host the servers software itself, such as web or mail service.

2) Direction control :- Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall

3) User control : control access to service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter.

4) Behavior control :- controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam or it may enable external access to only a portion of the information on a local web server.

9b. Discuss the capabilities which one within the scope of a firewall — 05 Marks

Sol :- The following capabilities are within the scope of firewall

1. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.

2. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system

3. A firewall is a convenient platform for several Internet functions that are not security related. These include address translator, which maps local addresses to Internet addresses, a network management function that audits or logs Internet

4. A firewall can serve as the platform for IPsec. Using the tunnel mode capability, the firewall can be used to implement virtual private networks.

Q. With a neat diagram, describe the working of packet filtering firewall — 10 Marks.

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

1) Source IP address :- The IP address of the system that originated the IP packet

2) Destination IP address :- The IP address of the system the IP packet is trying to reach

3) Source & Destination transport level address :- The transport level, port number, which defines applications such as SNMP or TELNET

4) IP protocol field :- Defines transport protocol

5) Interface :- for a firewall with three or more ports, which interface of the firewall the packet came from or which interface of the firewall the packet is destined for.

Smi

The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP hea If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken.

Two default policies are possible

- Default = discard : That which is not expressly permitted is prohibited
- Default = forward : That which is not expressly prohibited is permitted.

10 b.

OR

10 a. Discuss the characteristics of Bastion Host — 10 marks.

Sol:- A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. Typically, the bastion host serves as a platform for an application level or circuit level gateway. Common characteristics of a bastion host are as follows.

1) The bastion host hardware platform executes a secure version of its operating system, making it a hardened system

2) Only the services that the network administrator considers essential are installed on the bastion host. These could include proxy applications for DNS, HTTP and SMTP

3) The bastion host may require additional authentication before a user is allowed access to the proxy services. In addition each proxy services may require its own authentication before granting user access.

4) Each proxy is configured to support only a subset of the standard application's command set.

5) Each proxy is configured to allow access only to specific host systems.

6) Each proxy maintains detailed audit information by logging all traffic, each connection & the duration of each connection.

7) Each proxy module is a very large small software package specifically designed for network security.

8) Each proxy is independent of other proxies on the bastion host.

9) Each proxy runs as a non privileged user in a private and secured directory on the bastion host.

10) A proxy generally performs no disk access other than to read its initial configuration file.

Explain host based and personal firewalls — 06M

Sol:- A host-based firewall is a software module used to secure an individual host. Such modules are available in many operating systems or can be provided as an add-on package.

There are several advantages to the use of a server-based or workstation based firewall

1) filtering rules can be tailored to the host environment, specific corporate security policies for servers can be implemented, with different filters for servers used for different application.

2) Protection is provided independent of topology. Thus both internal and external attacks must pass through the firewall

3) Used in conjunction with stand-alone firewalls, the host based firewall provides an additional layer of protection.

Personal firewall

A personal firewall controls the traffic between a personal computer or workstation on one side and the internet or enterprise network on the other side. Personal firewall functionality can be used in the home environment and on corporate intranets.

Personal firewalls are typically much less complex than other server-based firewalls or stand-alone firewalls. The primary role of the personal firewall is to deny unauthorized remote access to the computer. The firewall can also monitor outgoing activity in an attempt to detect and block worms and other malware.

10 c. Explain the different purposes for which internal firewall can be used — 04 marks

Sol:— The different purpose of internal firewall serves three purpose

1. The internal firewall adds more stringent filtering capability, compared to external firewall, in order to protect enterprise servers & workstations from external attacks.

2. The internal firewall provides two-way protection with respect to the DMZ.

3. Multiple internal firewalls can be used to protect portions of the internal networks from each other.

Head of the Department
Dept. of Electronics & Communication Engg.
KLS VDIT, HALIYAL (U.K.)