CBCS SCHEME

USN | | | | | | | | | | |

18EC821

Eighth Semester B.E. Degree Examination, July/August 2022
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. Discuss the four principles of security in detail, each with an example. **(10 Marks)**

b. List the examples of application level attacks or network level attacks each of which has arisen in a real world (student can explain any real time example). **(10 Marks)**

OR

2 a. Discuss the active attacks and passive attack in detail. **(10 Marks)**

b. Explain the specific attacks sniffing, spoofing, phishing. **(05 Marks)**

c. Describe the terms virus, worms and cookies. **(05 Marks)**

Module-2

3 a. Draw the secure socket layer protocol stack and describe the working in details. **(10 Marks)**

b. Discuss the four stage handshake protocol with neat diagram. **(10 Marks)**

OR

4 a. Draw the Secure Shell (SSH) Protocol and describe the working in detail. **(10 Marks)**

b. What is the importance of HTTPS? Explain the connection initiation and Cloure of HTTP in detail. **(10 Marks)**

Module-3

5 a. Draw the flow chart of processing for outbound packets and processing model inbound packets. **(10 Marks)**

b. What are the IPSec services and explain. **(05 Marks)**

c. Explain about the IPSec documents. **(05 Marks)**

OR

6 a. With neat diagram explain the scope of ESP encryption in Tunnel mode and Transport mode. **(10 Marks)**

b. Explain the Internet Key Exchange Process using Diffie-Hellman algorithm with an example. **(10 Marks)**

Module-4

7 a. Name the three classes of intruders. Describe the Intruder behaviour patterns. **(10 Marks)**

b. Explain the Rule Based intrusion techniques, intrusion detection. **(10 Marks)**

OR

8 a. Explain types of malicious software in detail. **(10 Marks)**

b. Brief about the multiple threat Malware. **(05 Marks)**

c. Describe the four phase of virus. **(05 Marks)**

Module-5

9	a.	List out firewall characteristics and explain in brief.	(10 Marks)
	b.	What are the limitations of firewalls?	(05 Marks)
	c.	What are the firewall attacks and counter measures?	(05 Marks)

OR

10	a.	Name the types of firewalls and explain in detail.	(10 Marks)
	b.	Discuss the firewall configuration with neat diagram and example.	(10 Marks)

* * * * *

Scheme & Solutions

Eighth Semester B.E. Degree Examination, July/August 2022

Network Security (18EC821)

1a (i) Principle of Confidentiality: A will like to ensure that no one except B gets the envelope and even someone else gets it. She does not Come to know about the details of the cheque

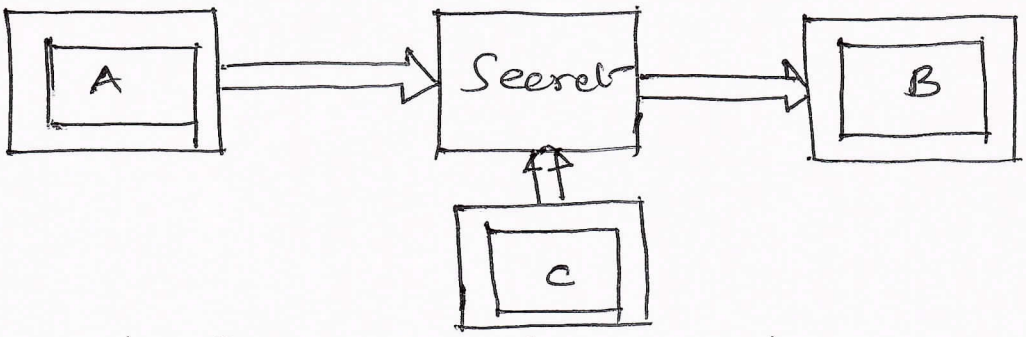
(ii) Principle of integrity: A & B make sure that no one can tamper with Content of the cheque

(iii) Principle of Authentication: B would like to assure that the cheque has indeed come from A and not from some one else posing as A

(iv) Principle of non-repudiation: If B deposits the cheque in her account, the money is transferred from A's accounts to the B's accounts and then A refuses.

2.5 × 4 = 10M

Confidentiality: only the sender and intended receipient should be able to access the Content of message. Confidentiality gets Compromised if an authorised person able to access a message

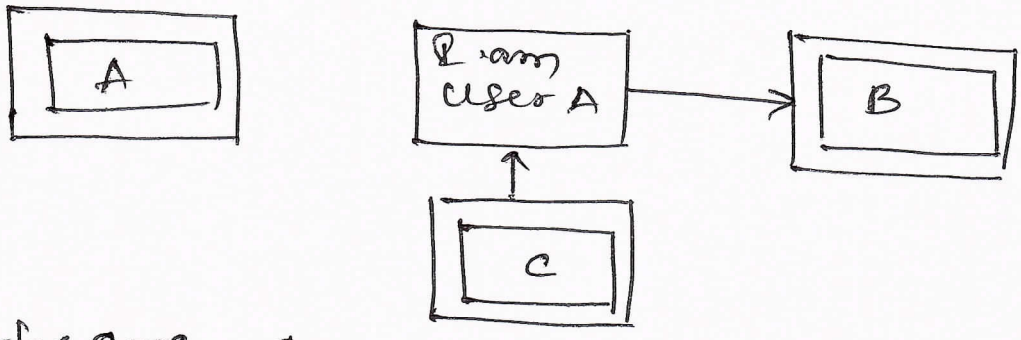


Loss of Confidentiality

Authentication: Mechanism help establish proof of Identities.

(1)

A sending a funds transfer request to bank B and bank transfer the funds from A's account to C's account



Absence of authentication

Integrity: The content of the messages are changed after the sender sends it, but before it reaches to the receiption: This is the integrity of message is lost

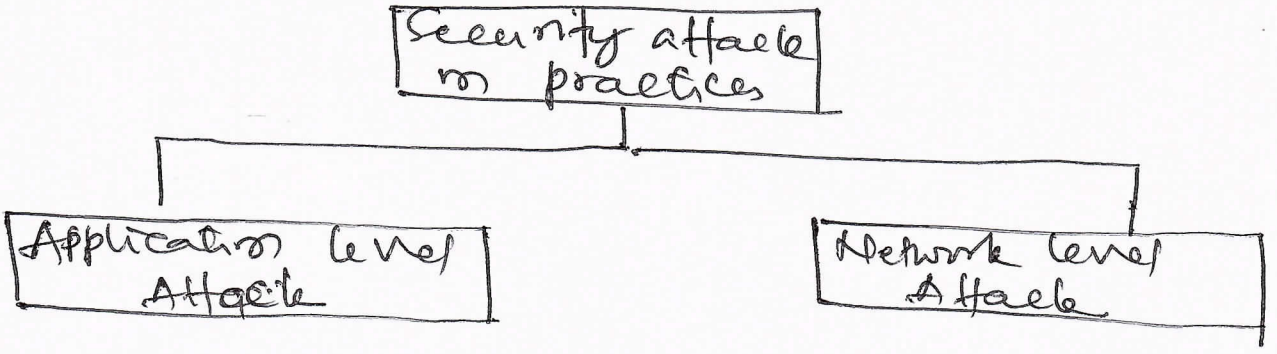
Modification causes loss of message integrity

Non Repudation: where user sends message and later on refuses that she had sent the message.

User A could send a funds transfer request to bank B over the internet Bank transfers as per As instruction. A could claim that she never sent the fund transfer instruction to the Bank.

Non repudation does not allow the sender of a message to refuse the claim of not sending that message.

1.b. practical side of attacks: Attack comes from a number of from a real life and classified into broad categories. Application level attacks & Network level attacks.



Application level attacks: These attacks happen at an application level where sensitive attacker attempts to access, modify or prevent access to information of particular application or application itself. EX: Trying to obtain some one Credit card information on the internet or Changing the Content of the message to change the amount in the transaction, etc.

Network level attacks: These attacks Generally aim at reducing the capabilities of a network by a number of

5x2 = 10

possible means. These attacks generally make an attempt to either slow down or completely bring to halt a computer network.

Note that this automatically can lead to the application level attack because once someone is able to gain access network usually she is able to access/modify at least some sensitive information causing harm

These attacks can be attempted by using various mechanisms. The above two categories span across the application as well as network level. Security attacks can happen at the application level or at the network level.

2a. Active attacks: Active attacks are based on the modification of the original message in some manner or on creation of the false message. These attacks can be prevented easily. They can be detected with some effort and attempts can be made to recover from them. The attack can be mainly of Port corruption, modification, and fabrication. Interruption attacks are called as masquerade attacks

2 1/2 x2 =5

Modification attacks can be classified further into replay attacks and alteration of message.

Fabrication causes Denial of service (DOS) attacks

Masquarade is caused when an un authorized entity pretended to be another entity.

Replay attack: A user captures a sequence of events or some data units and resends them

Alteration of message involves some change to the original message

Denial of service: Attacks makes an

5

attempt to prevent legitimate user from accessing some services which they are eligible for.

Passive attacks: where the attacker only engage in eavesdropping or monitoring of data transmission. The attacker can aims to obtain information that is in transit. The term passive indicates that the attacker does not attempt to perform any modifications of the data.

Passive attacks are harder to detect The general approach to deal with passive attacks is to think about prevention, rather than detection or correction actions. Passive attacks do not involves any modification to the content of the original message

Passive attacks are classified into two categories: ① Release of message contents & ② Traffic analysis

Release of message Content: when we send confidential email to our friend, we only she be able to access it: we can prevent this by encoding message. Attempt of analysing the encoded message with likely patterns, the work of traffic analysis attack.

4b. Sniffing: Packet Sniffing is passive attack on ongoing conversation. An attacker need not hijack a conversation but instead can simply observe packets as they pass by. To prevent an attacker from sniffing packets the information that is passing needs to be protected ① The data that is travelling can be encoded & The transmission link itself can be encoded. | 2x2 =4

Spoofing: In this technique an attacker sends packets with an incorrect source address; The receiver inadvertantly sends reply back to this forged address. called as spoofed address. not not to the attacker

(i) Attacker can intercept the reply
(ii) Attacker need not see the reply
(iii) Attacker does not want the reply.

pishing: Attacker creates identical fake ~~fake~~ im web site to a real website.

2c Virus: One can launch an application level attack or network level attack using virus.

Virus is a piece of program code that attaches itself to legitimate program code. and runs when the legitimate program runs.

It can infect other program in that Computer or program that are in the other computer, but on the same network virus can be repaired and its damage can be controlled by using good backup

Worms: Worm is actually different in implimentation. A virus modifies a program. A worm does not modify the program, it replicates itself again and again. Replication goes that ultimately Computer or network on which the worm resides

Cookies: Cookies were born as a result of specific Characteristics of the Internet HTTP protocol which is stateless.

Cookies is one or more piece of information stored as text strings in the text file on the disk of the client Computer.

2×2 = 4

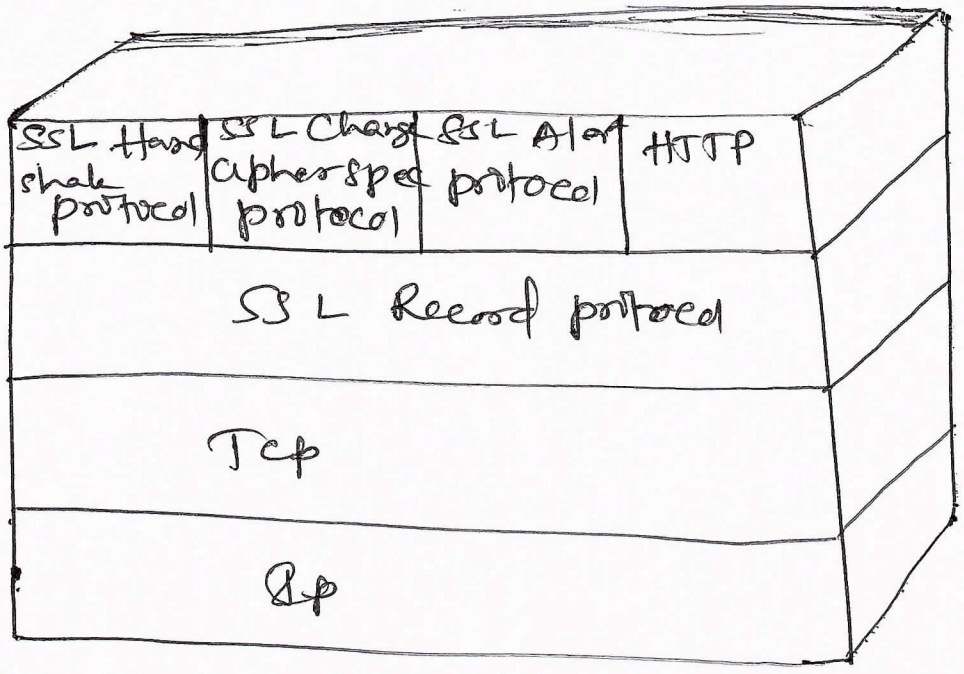
1

8

B9 Secure Socket layer protocol (SSL)

SSL is designed to make use of TCP to provide a reliable end-to-end secure service. SSL is not a single protocol but two layer protocol. SSL provides base security to higher layer protocols. HTTP provides the transfer service for web clients / servers interaction.

The two important SSL are the SSL Session and SSL Connection.



2M

Connection: A connection is a transport that provides suitable type of service. Such connections are peer to peer relationship. The connections are transient. Every connection associated with one session.

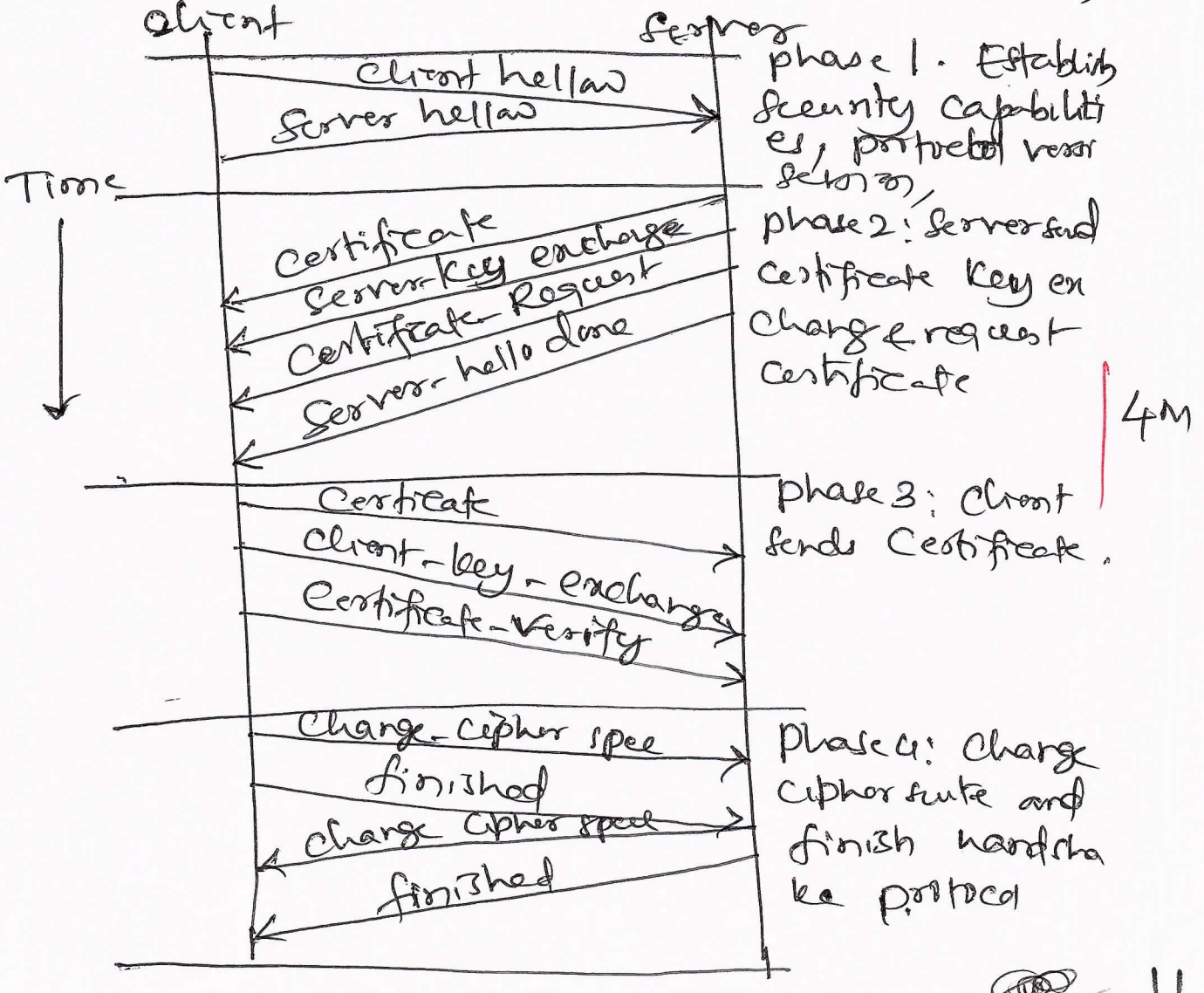
8

9

Session: SSL session is associated between a client and server. Sessions are created by the handshake protocol. session defines a set of cryptographic security parameters. which can be shared among the multiple connections. The sessions are used to avoid the expensive negotiations of new security parameters. for each connections. There are the number of states associated with each session.

Session Identifier: chosen by server,
Peer Certificate: X509.V3 certificate of peer
Compression method: Algorithm to compress data
Cipher spec: Bulk data encryption algorithm
Master Secret: 48byte secret shared between
Is resumable: Indicating new connection
Connection states:
Server and client random: Byte chosen
Server write MAC secret: data by server
Client write MAC secret: data by client
Server write key: Encryption & decryption
client write key: symmetric key
Initialization vector: Chain Block Cipher (CBC)
Sequence number: for Transmitted & Received messages.

3b. The most complex part in SSL is handshake protocol. This allows server and client to authenticate each other and negotiate encryption and MAC algorithm used to protect the data sent in an SSL record. Series of message exchanged by client & server and each message has 3 fields.
Type (1 byte): Indicates one of 10 message.
Length (3 byte): The length of the message
Content: The parameters associated with each



Phase 1: Establish security capabilities: Initiate a logical connection and to establish the security capabilities that will be associated with it. Client messages with version, Random, session id, cipher suite and compression method. and key exchange supported, RSA, Diffie-Hellman, Fortezza. cipher spec - cipher algorithm, MAC, cipher type,

phase 2: Server Authenticates and key exchange: Server begins this by sending the certificates to authenticate message, Server key exchange and Server can request certificate from the Client, includes two parameter Certificate_type and certificate authorities.

phase 3: Client authentication and key exchange: Receiving the server done message the client should verify the server provided a valid certificate and check the server parameters are acceptable. If all is satisfactory the client sends one or more message back to the server.

phase 4: Finish - This phase completes the setting up of the Secure Connection. The finished message verifies the key exchange and authentication process were successful.

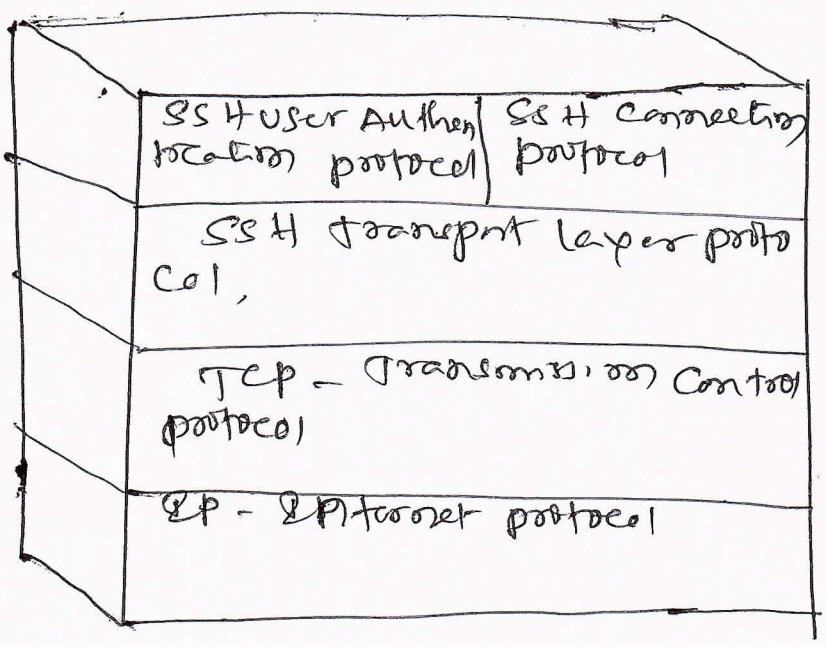
6M

12

4a. Secure Shell (SSH): SSH is a protocol for secure network communication designed to be relatively simple and inexpensive to implement. SSH also provides more general client/server capability and can be used for such network functions as file transfer and e-mail. SSH2 fixes number of security flaws in original scheme

SSH client and server applications available for most of the operating systems

SSH is organized as three protocols that run on TCP



4M

Transport layer protocol: provides server authentication, data integrity with forgery secrecy. optionally provides compression.

User authentication protocol: Authenticates user to the server.

13

connection protocol: multiplexes multiple logical communication channel over a single, underlying SSH connection.

Server authentication occurs at the transport layer based on the server processing a public/private key pair. Server may have multiple host keys using multiple different asymmetric encryption algorithm.

Client has the local data base that associates each host name with corresponding server public host key.

Certification authority (CA): client knows the CA root key and verify the validity of all the host keys certified by accepted CAs

Packet exchange: once the connection is established the client and server exchange data organized to as packet. Each packet has format, packet length, padding length payload, Random padding, message authentication code (MAC) 6M

Key generation: The keys used for encryption and MAC are generated from the shared secret key K the hash value from the key exchange H.

User authentication protocol: This provides client to authenticated to the server

Message types and formats:

4b HTTPS refers to the combination of HTTP and SSL to implement secure communication b/w web browser and a Web server.
HTTP Connection uses port 80, HTTPS is specified port 443 is used which invokes SSL
HTTPS is used the following elements
URL of the requested document, Content of the document, contents of browser forms Cookies sent from the browser to server and server to the browser, Contents of HTTP header. 5M

HTTPS is documented in RFC 2818,
Connection initiation: HTTPS the agent acting like HTTP client and also acts as TLS client. All HTTP data is to be sent as TLS application data
there are the three levels of awareness of HTTPS, ① HTTP Client request the Connection to the HTTP server by sending a Connection request to the next lower layer. the next lower layer is TCP (TLS/SSL) TLS session establishes between TLS client and TLS server. TLS request the Connection between TCP entity at Client and the TCP entity on the server side.

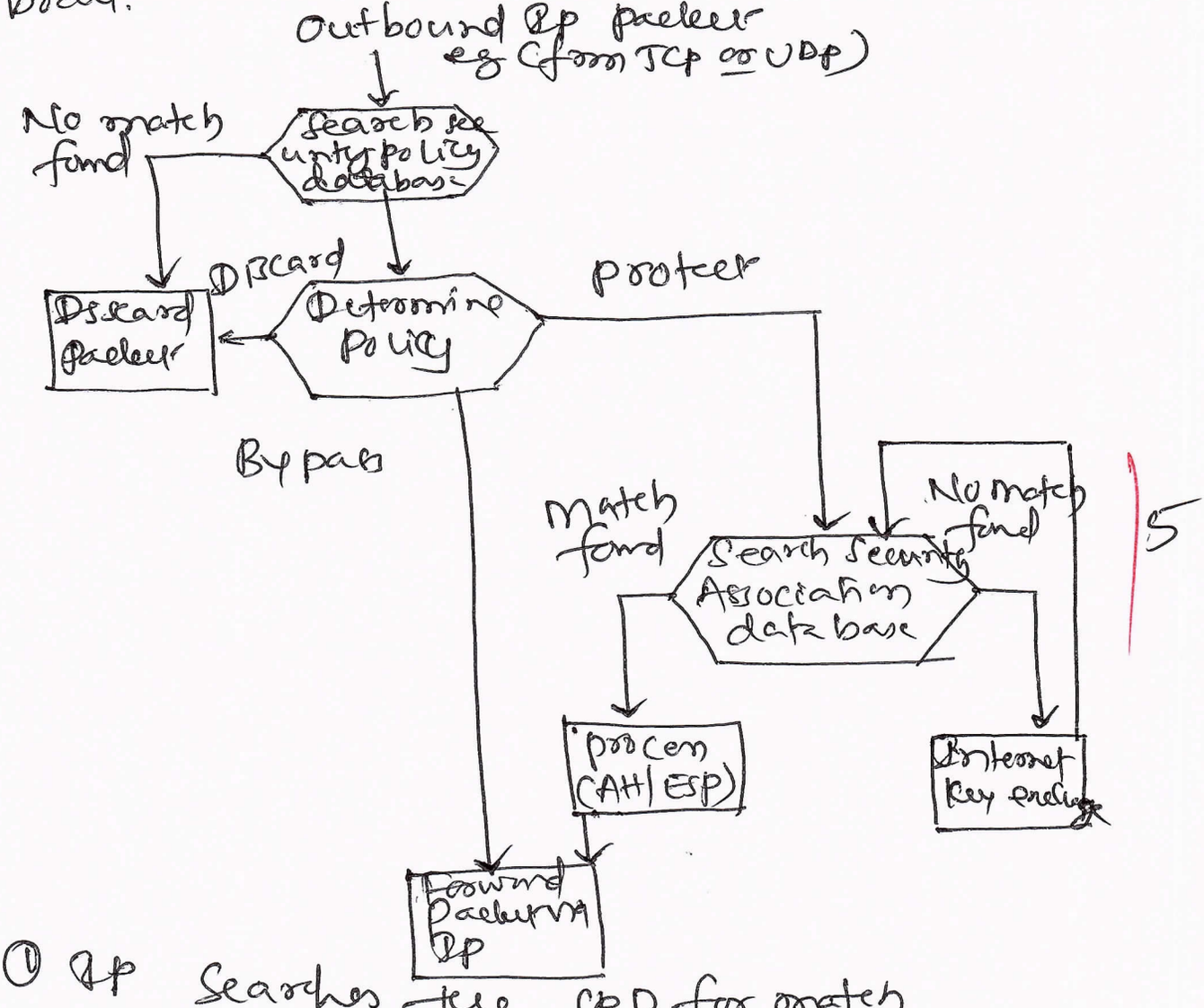
15

Connection Closure: Indicate the closing of the Connection by including line in an HTTP record: Connection: Close. Connection is closed after this record o delivered the closure of HTTPS Connection requires that TLS Close the Connection with the peer TLS entity on the remote side. which invokes the closing the underlying TCP Connection. The proper way to close the Connection for each side. The TLS alert protocol to send Close_notify-alert After sending the closure alert close the connection without waiting for peer to send the closure alert generating an incomplete close

2.5 x2 =5

HTTP client also must be able to cope with situation which is underlying TCP connection terminated without prior notify. and without Connection Close indicator. TCP closure should be evidence of some sort of attack and HTTPS client should issue some sort of security warnings.

Sol Outbound Packets : This is the main element of IPsec processing for outbound traffic. A block of data from higher layers is passed down to the IP layer and IP packet is formed consisting of an IP header and IP body.



5

① IP Searches the SPD for match
② No match found packet is discarded & error message generated
③ If match is found further processing is determined by SPD. If policy discarded the packet is discarded.

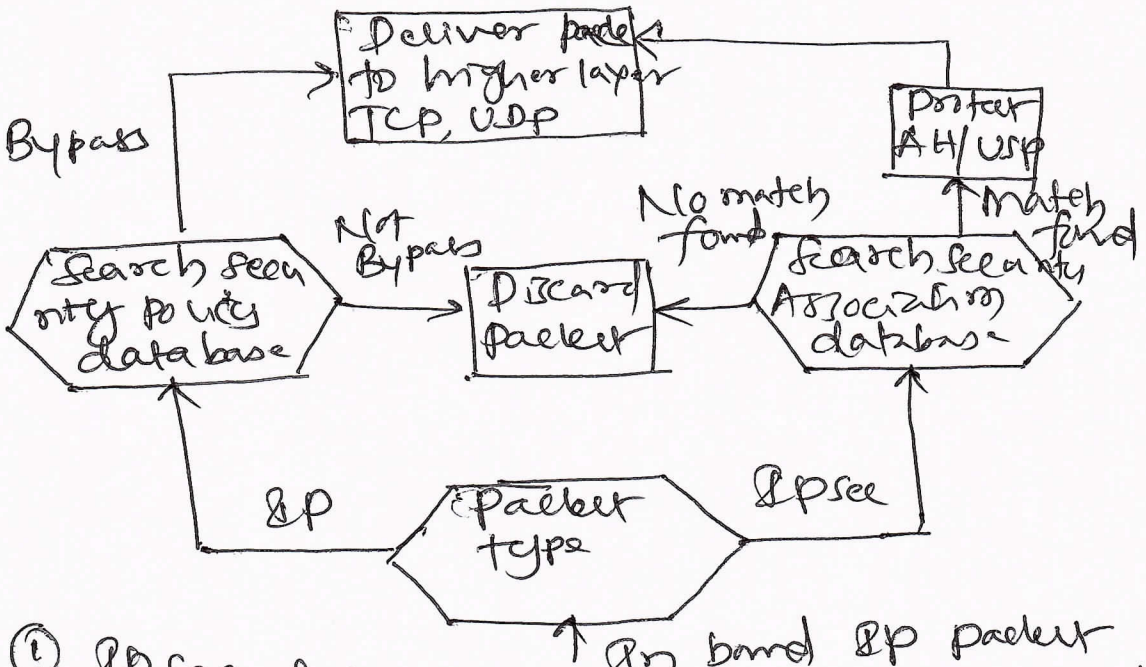
17

If the policy is BYPASS and then there is no processing and packet is forwarded to the networking for transmission

4. If the policy is protect then search is made of the SAD

Matching entry in the SAD determines the processing for the packet, either encryption

Inbound processing: The main elements of IPsec processing for inbound traffic.



(1) IPsec determines unsecured IP packets as ESP or header

(2) If IP packet is unsecured, IP search es the SPD for match, policy of Bypass. If no matching the packet is Discarded

(3) If packet secure IPsec searches the SAD. If no match found packet is discarded otherwise applies ESP or AH processing.

5b. IP.Sec : IPsec provides the security services at the IP layer by enabling a system to select the required security protocol. Two protocols are used to provide the security Authentication protocol are used to provide security designed by the header of the protocol and combined format of packet for the protocol Encapsulating security payload (ESP). RFC 4301 . List of the fallowing services

2M

Access Control
Connection less integrity
Data origin authentication
Rejection of Replayed packets
Confidentiality
Limited traffic flow Confidentiality.

3M

5c. Ipsec documents: Ip-sec encompasses three functional areas authentication, confidentiality and key management. Ipsec document road map and document categorized into the following groups

Architecture: Covers the general concept security requirements, definitions and mechanisms defining Ipsec technology

Authentication header (AH): AH is an extension header to provide the message authentication. Authentication is provided by ESP, The use of AH is depricated.

Encapsulating security payload (ESP): Consists of header and trailer and provides encryption. The current spec is RFC4303 | 5M

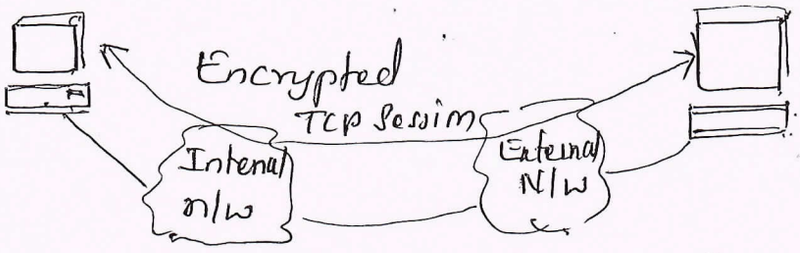
Internet key exchange (IKE): This is a collection of document describing the key management scheme. The current version RFC 4306 & number of Related RFC

Cryptographic algorithms: describes cryptographic algorithms for encryption, message authentication, Pseudo random function (PRF)

Other: Ipsec related RFC including with security policy and management information base (MIB)

20

6.a) With neat diagram explain the scope of ESP encryption in Tunnel mode and Transport mode. 10

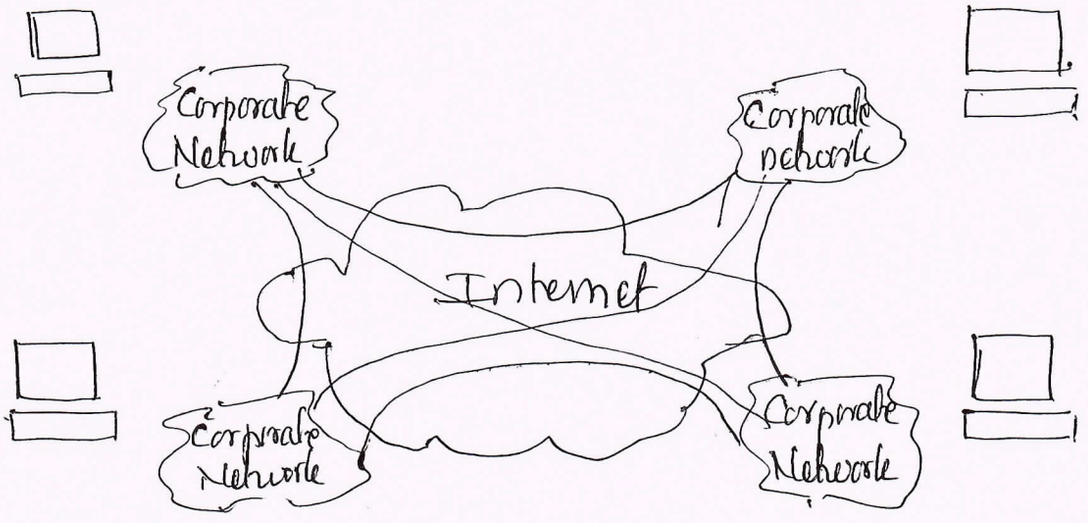


2

Transport-level security

* Transport mode ESP is used to encrypt and optionally authenticate the data carried by IP (e.g. a TCP segment) as shown in the above figure.
* IPv4, the ESP header is inserted into the IP packet immediately prior to the transport-layer header (e.g. TCP, UDP, ICMP), and an ESP trailer (Padding, Pad Length, and Next Header fields) is placed after IP packet. 3
* The entire transport-level segment plus the ESP trailer are encrypted.
* In the context of IPv6 ESP is viewed as an end-to-end payload.

Tunnel Mode



2

21

* Tunnel mode operation provides encryption of an entire IP packet.
* ESP header is prefixed to the packet and the packet plus the ESP trailer is encrypted
* This method can be used to counter traffic analysis
* 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. 3
* Tunnel mode is useful in configuring firewall or other sort of security gateway that protects a trusted network from external networks

---

6.5) Explain the Internet Key Exchange Process using Diffie-Hellman algorithm with an example. 10

Diffie-Hellman Key Exchange Algorithm

Global Public Elements

q	Prime number
α	$\alpha < q$ and α a primitive root of q.

* User A Key generation 5

Select private X_A $X_A < q$

Calculate public Y_A $Y_A = \alpha^{X_A} \bmod q$

* User B Key generation

Select private X_B $X_B < q$

Calculate public Y_B $Y_B = \alpha^{X_B} \bmod q$.

* Calculation of Secret Key by User A

$$K = (Y_B)^{X_A} \bmod q$$

* Calculation of Secrete key by user B

$$K = (Y_A)^{X_B} \bmod q.$$

> Example:

Prime number $(q) = 353$

and primitive root, $\alpha = 3$

A and B select secret keys $X_A = 97$ and $X_B = 233$, respectively. Each computes its public key:

A computes $Y_A = 3^{97} \bmod 353 = 40$

B computes $Y_B = 3^{233} \bmod 353 = 248$

After they exchange public keys, each can compute the common secret key: 5

A computes $K = (Y_B)^{X_A} \bmod 353 = 248^{97} \bmod 353 = 160$

B computes $K = (Y_A)^{X_B} \bmod 353 = 40^{233} \bmod 353 = 160$

7a) Name the three classes of intruders. Describe the Intruder behaviour patterns 10

Three classes of intruders

* i) 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.

ii) Misfeasor: A legitimate user who accesses data, programs or resources for which such access is not authorized, or who is authorized 5

for such some access but misuses his or her privileges

iii) Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection

* Intruder behaviour patterns

i) Hacker: Attackers often look for targets of opportunity and then share the information with others

Example: Break-in at a large financial institution. The intruder took advantage of the fact that the corporate n/w was running unpatched services. The key to break-in was the pcAnywhere application.

ii) Criminals: Organized group of hackers have become a widespread and common threat to Internet-based systems. They have specific targets or at least classes of targets in mind. Once a site is penetrated, the attacker acts quickly, scoping up as much valuable information as possible.

Example: A common target is credit card info at an ecommerce server. Attackers attempt to gain root access. The card numbers are used by organized crime gangs to purchase expensive items and are then posted to carder sites, where others can use accounts and use the account numbers. This obscures usage patterns and

5

complicates investigation.

iii) Insider attacks are most difficult to detect and prevent
Employees already have access and knowledge about the structure and content of the corporate databases
Example: The case of Kennath Pattersons, fired from his position as data communications manager for American Eagle Outfitters. Patterson disabled the company's ability to process credit card purchases during three days of the holiday season of 2002

7b) Explain the Rule Based intrusion techniques, intrusion detection 10

* Intrusion Techniques

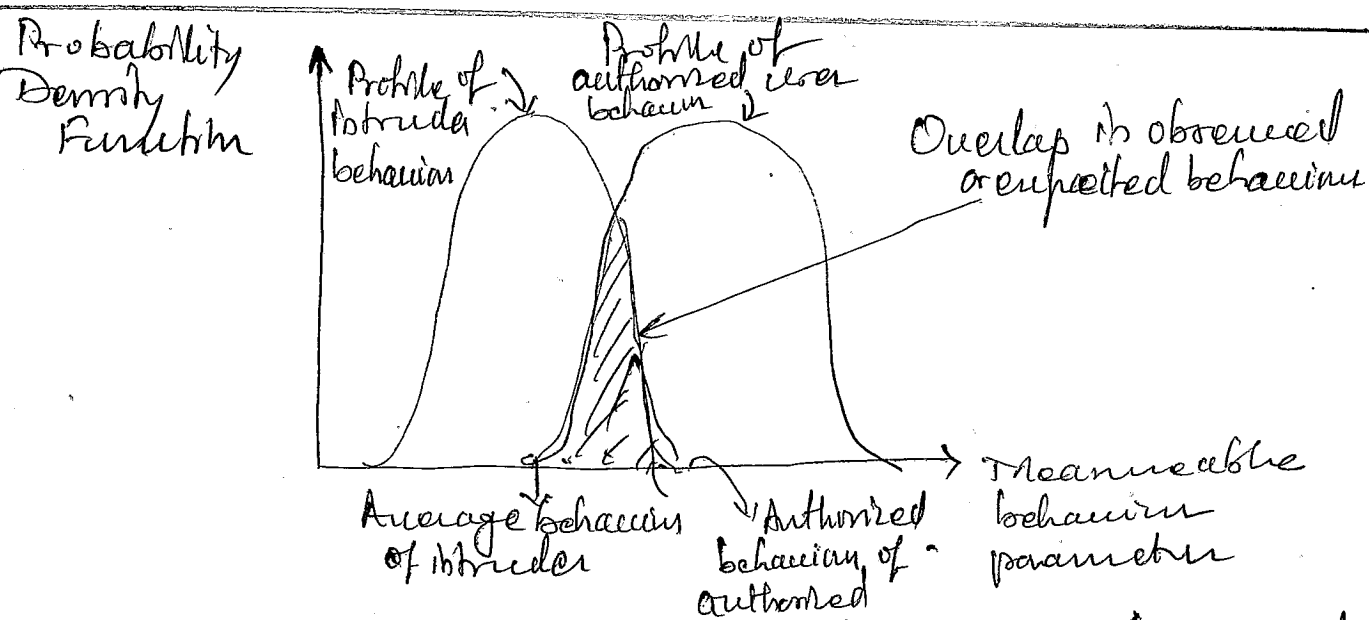
i) One-way function: The system stores only the value of a function based on the user's password. When the user presents a password, the system transforms that password and compares it with the stored value. In practice, the system usually performs a one-way transformation in which the password is used to generate a key for the one-way function and in which a fixed-length output is produced. 5

ii) Access Control: Access to the password file is limited to one or a very few accounts

* Intrusion Detection:

Intrusion detection is based on the assumption that the behaviour of the intruder differs from that of a legitimate user in ways that can be quantified. Figure suggests intrusion detection system.

23



Probbes of Behaviours of Intruders and Authorized users

Rule-based detection: Involves an attempt to define a set of rules that can be used to decide that a given behaviour is that of intruder. 5

> Anomaly detection: Rules are developed to detect deviation from previous usage patterns.

> Penetration identification: An expert system approach that searches for suspicious behavior

8 a) Explain types of malicious software in detail 10M

* Virus: Malware that, when executed, tries to replicate itself into other executable code; when it succeeds the code is said to be infected.

* Worm: A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network. 10

* Logic Bomb: A program inserted into software by an intruder. A logic bomb is triggered when certain unauthorized after predefined condition is met 26

8 b) Brief about the multiple threat malware 5

* A multipartite virus infects in multiple ways
* It is capable of infecting multiple files, so that virus eradication must deal with all of the possible sites of infection.

A blended attack uses multiple methods of infection or transmission, to maximize the speed of contagion and the severity of the attack

* An example of blended attack is Nimda - attack, erroneously referred to as simply a worm. Nimda uses four distribution methods

i) Email; ii) Windows share iii) Web services iv) Web Clients 5

Thus, Nimda has worm, virus and mobile code characteristics. Blended attacks may also spread through other services such as instant messaging and peer-to-peer file sharing.

8 c) Describe the four phase of Virus 5

* Dormant Phase: The virus is idle, the virus is eventually be activated by some event such as a date, the presence of another program or file. Not all viruses have this stage.
* Propagation Phase: The virus places a copy of itself into other programs or into certain system areas on the disk.

27

Trojan horse: A computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms.

Back door: Any mechanism that bypasses a normal security check; It may allow unauthorized access to functionality.

Mobile Code: Software code that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics

Exploits: Code specific to a single vulnerability or set of vulnerabilities.

Downloaders: Program that installs other items on a machine that is under attack. Usually, a downloader is sent in an e-mail.

Auto-rooter: Malicious hacker tools used to break into new machines remotely.

Kit: Set of tools for generating new viruses automatically

Root kit: Set of hacker tools used after attacker has broken into a computer system and gained root-level access

Spyware: S/w that collects information from a computer and transmits it to another system.

Adware: Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.

* Triggering phase: The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be ~~caused~~ caused by variety of system events.

* Execution phase: The function is performed The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files

---

9 a) List out firewall characteristics and explain in brief. 10

---

* Service control: Determines 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.

> Direction control: Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall 10

> User Control: Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter. It may also be applied to incoming traffic from external users.

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 local Web server.

b) What are limitations of firewall 5

1) The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP.

2) The firewall may not protect fully against internal attacks, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker. 5

3) An improperly secured wireless LAN may be accessed from outside the organization

4) A laptop, PDA, or portable storage device may be used and infected outside the corporate network, and then attached and used internally.

c) What are the firewall attacks and counter measures 5

* IP address spoofing: The intruder transmits packets from the outside with a source IP address field containing an address of an internal host. Counter measure: Discard the packets with an inside source address if the packet arrives on an external interface.

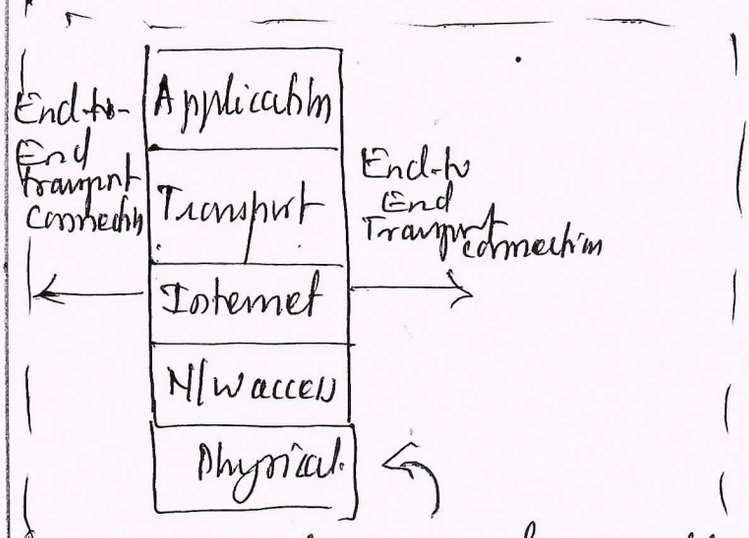
* Source routing attacks: The source station specifies the route that a packet should take as it crosses the Internet, in the hope by passing security measures

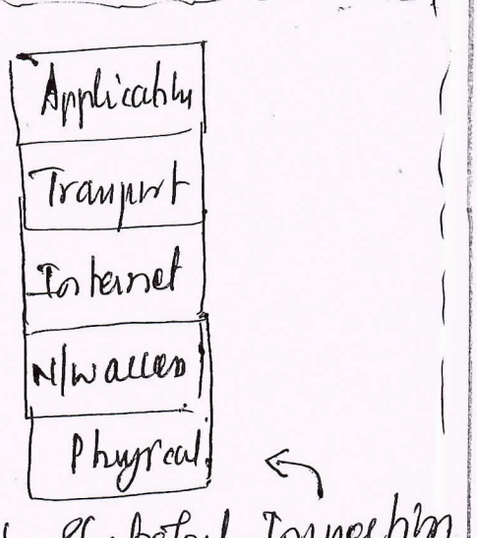
Counter measure: Discard all packets that use this option

* Tiny fragment attacks: The intruder uses IP fragmentation option to create extremely small fragments and force the TCP header information into a separate packet fragment. 5

Counter measure: By enforcing a rule that the first fragment of a packet must contain a predefined minimum amount of the transport header.

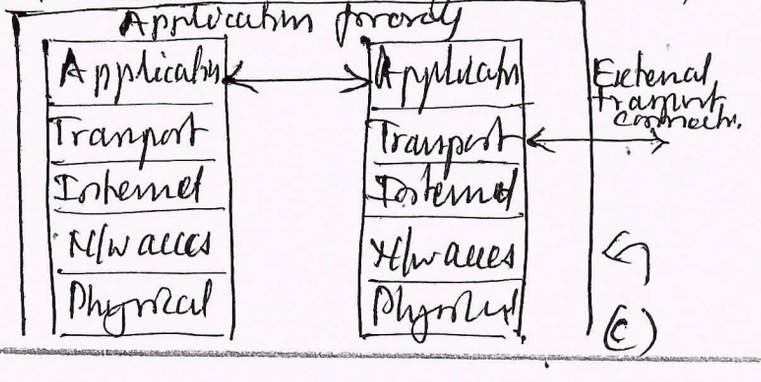
10a) Name the types of firewalls and explain in detail 10

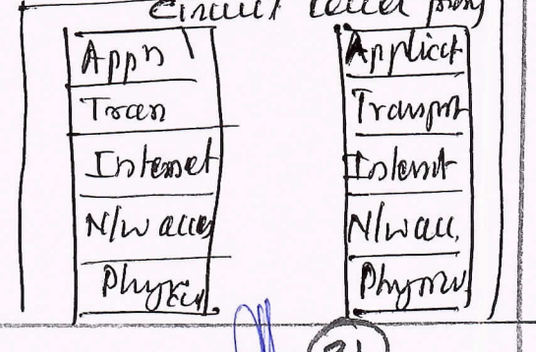




a) Packet filtering firewall

b) Stateful Inspection firewall 5





a) A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and the forwards or discards the packet

b) * Stateful Inspection firewall tightens up the rules for TCP traffic by creating a directory of out bound TCP connections.
* Reviews packet information as a packet filtering firewall, but also records information about TCP connections.

c) Application-Level Gateway also called an application proxy, acts as a relay of application level traffic
* The user contacts the gateway using a TCP/IP application such as Telnet or FTP.

d) 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

10 b) Discuss the firewall configuration with neat diagram and example.

* DMZ networks as shown in figure(1) suggest the most common ~~suggestion~~ distinction between an internal and an external firewall
* An external firewall is placed at the edge of a local or enterprise network.
* One or more internal firewalls protect the bulk of enterprise networks.
* Between these two types of firewalls are networked devices in a region referred to as

5

10

2

DMZ (demilitarized zone) network.

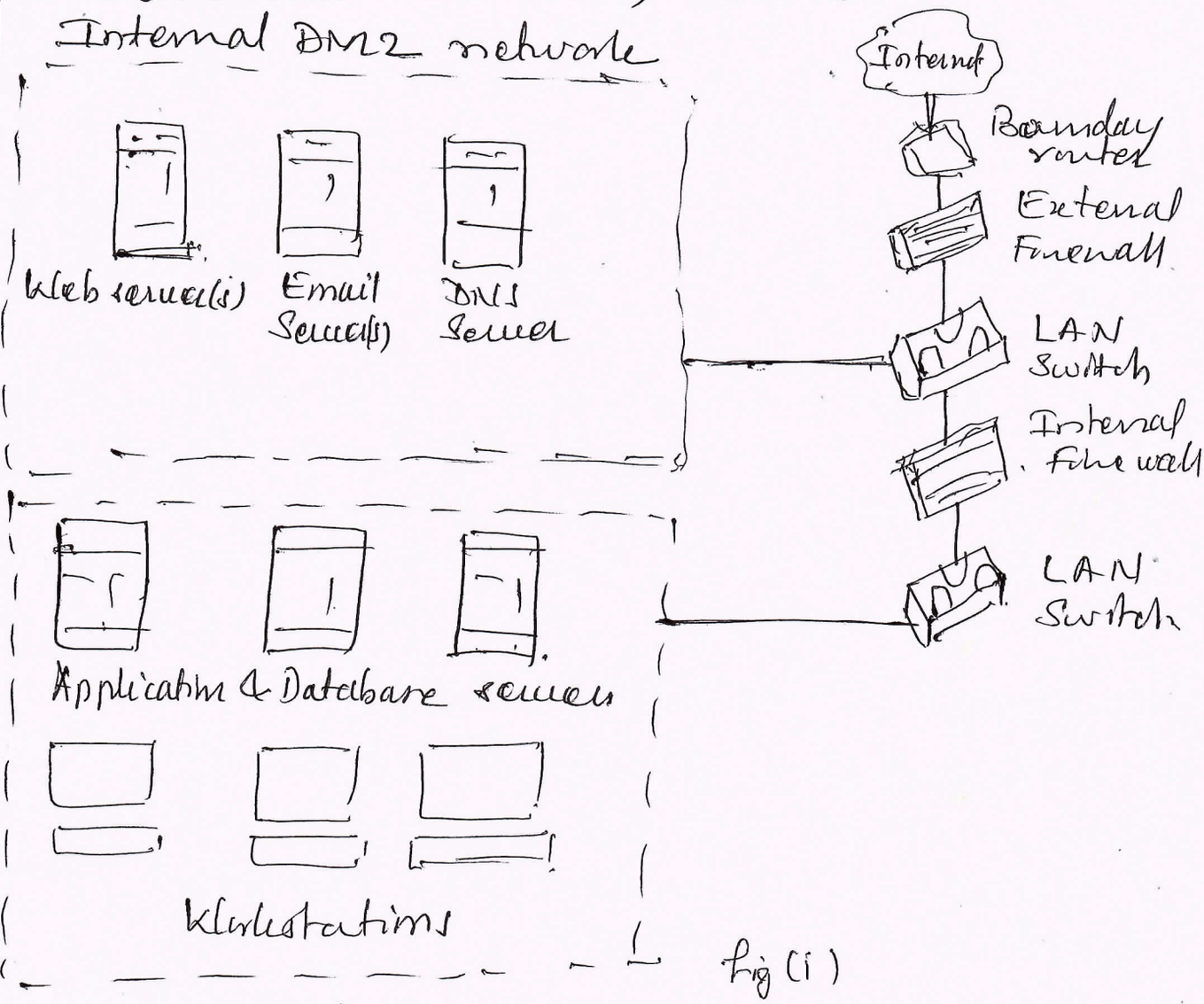


fig (1)

2

> Virtual Private Networks

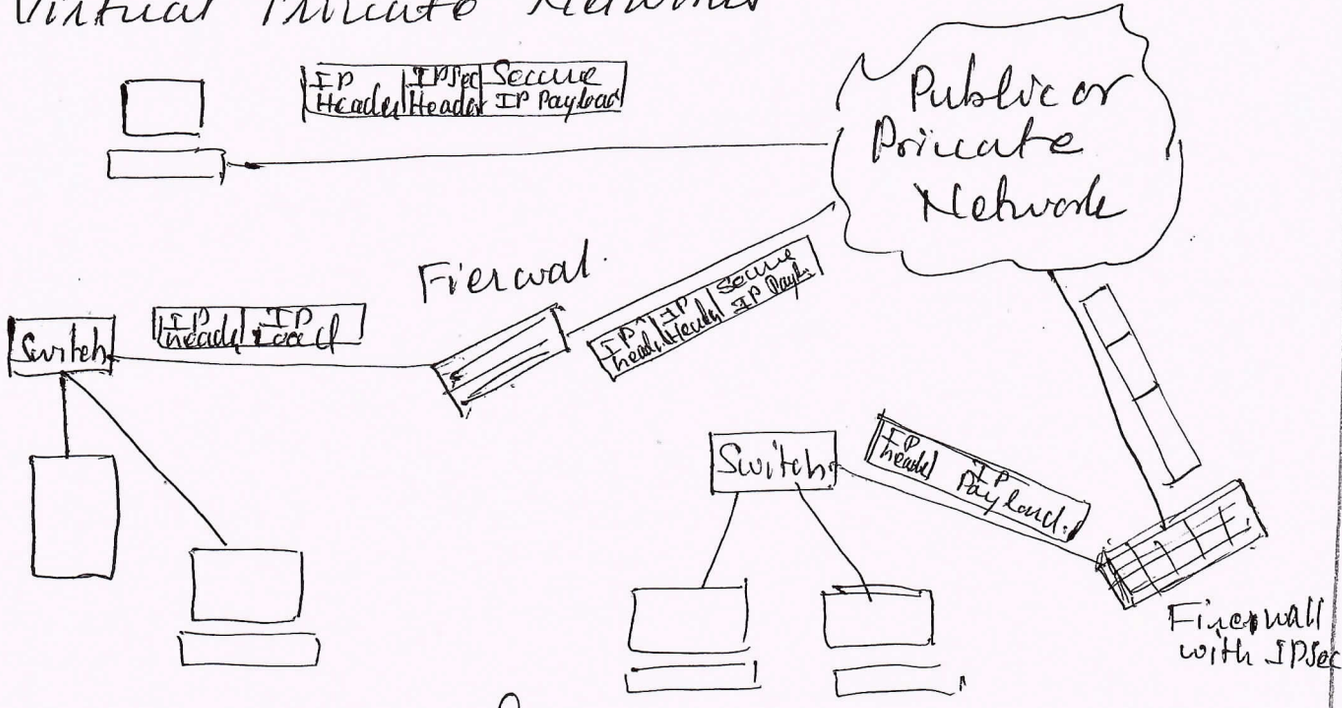


fig (2)

2

* VPN consists of a set of computers that interconnect by means of a relatively unsecure network and that make use of encryption and special protocols to provide security.

* At each corporate site, workstations, servers, and databases are linked by one or more local area networks (LANs)

* The Internet or some other public network can be used to interconnect sites providing a cost savings over the use of a private network and offloading the wide area network management task to the public network provider.

> Distributed Firewalls

* A distributed firewall configuration includes stand-alone firewall devices plus host based firewalls working together under a central administrative control

* Administrators can configure host resident firewalls on local and remote user systems

* Tools let the network administrator set policies and monitor security across the entire network

* These firewall protects against internal attacks and provide protection tailored to specific machines and applications.

Related Figure.

—— x ——