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
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- Ashwini. G / Prof- Raghavendra. N
Course Name	:	Network Security
Course Code	:	21EC742
Year of Question Paper	:	Model question paper 2021 CBCS scheme
Date of Submission	:	16/1/25

Faculty Member

HoD 16.01.25

Head of the Department
Dept. of Electronic & Communication Engg.
K.L.S. V.D.I.T., HALIYAL (U.K.)

Dean (Acad.)

Model Question Paper-1/2 with effect from 2021(CBCS Scheme)

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

7th Semester B.E. Degree Examination

Subject Network Security

TIME: 03 Hours **Max. Marks: 100**

Note: 01. Answer any **FIVE** full questions, choosing at least **ONE** question from each **MODULE.**

		Module -1	BTL	COs	Marks
Q.01	a	Explain the various modern nature of attacks.	L2	CO1	05
	b	Explain the various types of Criminal attacks	L2	CO1	05
	c	Explain the following specific attacks with an example for each: i. Phishing ii. Phorming	L2	CO1	10
		OR			
Q.02	a	Explain the various authentication methods supported by EAP methods	L2	CO1	10
	b	Explain the various principles of security with an example for each	L2	CO1	10
		Module-2			
Q. 03	a	Explain SSL Record Protocol and its format with the corresponding diagrams	L2	CO2	08
	b	Explain how connection initiates and closes in HTTPS	L2	CO2	06
	c	Explain the Pseudo Random Function used in TLS with a neat diagram	L2	CO2	06
		OR			
Q.04	a	Explain SSL handshake protocol with a neat diagram	L2	CO2	12
	b	Explain Local and Remote port forwarding in SSH connection protocol	L2	CO2	08
		Module-3			
Q. 05	a	Explain IKEv2 exchanges with a neat diagram	L2	CO3	10
	b	Explain different categories of IP Security Documents in detail	L2	CO3	5
	c	Explain the selectors used to determine an security policy database	L2	CO3	5
		OR			
Q. 06	a	Explain the parameters of security association and security association database	L2	CO3	10
	b	Explain ESP packet format with the relevant diagrams	L2	CO3	10
		Module-4			
Q. 07	a	Explain various intrusion techniques with an example for each	L2	CO4	8
	b	Explain the general virus structure and the logic for compression virus	L2	CO4	12
		OR			
Q. 08	a	Explain Distributed intrusion detection with relevant diagrams	L2	CO4	10
	b	Explain the different generations of anti-virus	L2	CO4	10
		Module-5			
Q. 09	a	Explain the design goals for a firewall and the general techniques used by it to control access	L2	CO5	10
	b	Explain Baston-host firewall biasing	L2	CO5	10
		OR			
Q. 10	a	Explain Packet filtering firewall with example	L2	CO5	10
	b	Explain the working of distributed firewall with a neat diagram	L2	CO5	10

*Bloom's Taxonomy Level: Indicate as L1, L2, L3, L4, etc. It is also desirable to indicate the COs and POs to be attained by every bit of questions.

@#@

Model Question paper
Network Security (21EC742)

Q a) Explain the various modern nature of attacks 5M

→ 1) Automating attacks:- Humans dislike repetitive and difficult tasks Automating them can cause destruction more rapidly. Rather than producing fake currency on a mascal modern thieves will excel in stealing a very low amount from million bank accounts in a matter of a few munites

2) Privacy concern:- collecting information about people and later misusing it is turning out to be a huge problem the data mining applications gather process and tabulate all sorts of details about individuals peoples can illegally sell this information

3) Distance does not matter:- Thieves would earlier attack banks as banks had money these days money is in digital form and moves around using computer network it is easier for modern thief to attempt an attack on the computer system of the bank sitting at home.

b) Explain the various types of criminal attacks. 5M

→ * Fraud:- modern fraud attacks concentrate on manipulating some aspects of electronic currency credit cards electronic stores certificates cheques letters of credit purchase order ATM.

* Scams:- some forms of scams are scales of services allows multi level marketing schemes general merchandise and business opportunities people are tempted to send money in return of great profits but end up losing their money.

Ashu

Head of the Department
Dept. of Electronics & Communication Engg.

* Destruction:- The main motive behind these attacks is some sort of grudge Ex: Some unhappy employees attack their own organization terrorists strike at bigger levels
* Identity theft:- An attacker does not steal anything from a legitimate user instead he becomes that legitimate user.
* Intellectual Property theft:- Intellectual property theft ranges from stealing companies trade secrets databases digital music and videos electronic documents and books Identity theft Intellectual Property theft software

c) Explain the following specific attacks with an example for Each

i) Phishing ii) Phorming

→ a) Phishing :-

* In Phishing attackers set up fake websites which look like real web sites it is simple to create web pages as it involves simple technologies such as HTML Java Script Learning and using these technologies is quite simple
* The attacker decides to create his own web site which looks very identical to a real web site for Example the attacker can clone citibanks web site the cloning is so clever that human eye will not be able to distinguish between the real and fake sites now.
* the attacker sends an Email to the legitimate customers of the bank The Email itself appears to come from the bank For Ensuring this the attacker exploits the System to suggest that the Sender of the Some bank official
* This fake Emails warns the user that there has been Sort of attack on the citibanks Computer system and that the bank wants to issue new Passwords to all its customers or verify their existing Pin.

* This fake email warns the user that there has been some sort of attack on the citibanks computer systems and that the bank wants to issue new passwords to all its customer computer systems and that the bank wants to issue new passwords to all its customers or verify their existing Pin
* when the customer innocently clicks on the URL specified in the email she is taken to the attackers site and not the banks original site there the customer is prompted in the same email
* since the attackers fake site looks exactly like the original bank site the customer provides this information the attacker gladly accepts this information and display a thank you to the unsuspecting victim.

ii) Phorming:-

* This attack was earlier known as DNS spoofing or DNS poisoning is now called as pharming attack
* with the Domain System (DNS) People can identify web sites with human-readable names and computers can continue to treat them as IP addresses
* For this a special server computer called as a DNS Server maintains the mapping b/w domain names and the corresponding IP addresses the DNS server could be located anywhere usually it is with the internet service provider of the users.
* Suppose that there is merchant whose site domainname is www.bonus & address is 100.10.10.20 therefore the DNS Entry for bob is all the DNS servers
* The attacker manages to have 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 maintains by ISP

* when alice wants to communicate with Bob site her web browser queries the DNS server maintained by her ISP for Bob IP address providing it the domain name alice gets the replaced IP address which is 100.20.20.20
* Now alice starts communicating with truely believing that she is communicating with bob such attacks of DNS spoofing are quite common and cause a lot of havoc

Q2 a) Explain the various authentication methods supported by EAP methods 10M

→ * Public key: the details of this method depend on the Public key algorithm chosen in essence the client sends a message to the server that contains the clients Public key with the message signed by the client Private key then the Server receives this message it checks whether the Supplied key is acceptable for authentication and if so it check whether the signature is correct
* Password :- the Client sends a message containers a plain text password which is protected by encryption by the transport layer protocol
* host based :- Authentication is performed on the client host rather than the client itself thus a host that support multiple clients would provide authentication for all its clients this method works by having the client send a Signature created with the Private key of the client host
* Biometric authentication :- uses unique biological traits like fingerPrint facial recognition retinal scan to Verify identity
* Token Based Authentication :- Utilizes tokens to grant access Example hardware tokens & Software based tokens (JWT)

(3) Integrity:-

* when the contents of the message are changed after the sender send it but before it reaches the intended recipient the integrity of the message is lost

Ex: Suppose you write a cheque of $100 to pay for the goods bought from the store but in the account statement it is observed that the cheque resulted in a payment of $1000 this is the case of loss of message integrity.

4) Non-Republication:-

* there are situations when a user sends a message and later refuses that messag was sent this is repudeation

Ex:- User A could send a fund transfer request to bank B over the internet After the bank perform the funds transfer as per A's request A could claim that he never sent the fund transfer request to the bank

5) Access control:-

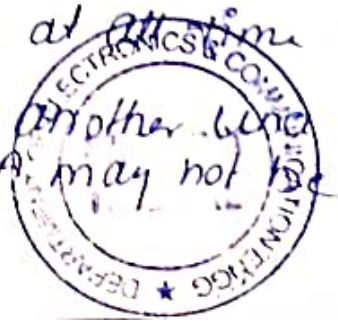
* the Principle of accen control determines who should able to accen what

* For instance we should able to specify that user A can view the records in a database but cannot update them. However another user B might be allowed to make updates as well an access control mechanism can be set up to Ensure this

6) Availability:-

* the Principles of availability states that resources should be available to authorized parties at all times

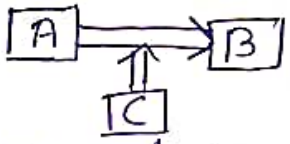
* Ex:- Due to the intentional actions of another unauthorized user C an authorized user A may not be able to content a server computer B



2b Explain the various Principles of security with an Example for Each 10M

→ 1) Confidentiality:

* the Principle of confidentiality specifies that only the Sender and the intended recipient should be able to acces the contents of a message
* Confidentiality gets compromised if an unauthorized person is able to acces a menage.

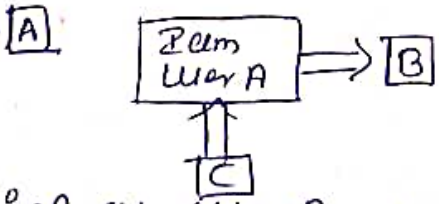


* Here the user of computer A sends a menage to the user of computer B. another user C gets acces to this message which is not desired and therefor defeats the purpos of Confidentiality.

* Ex: A confidential Email menage sent by A to B which is accessed by C without the permission of A and B. this type of attack is called as interception

2) Authenticaleon:-

* Authenticaleon Establishes proof of identities.
* the authenticaleon Proces Ensures that the original of an Electronic message document is correctly identified
* For instanee suppos that user C sends an Electronic document over the Internet to user B. Posing as user A How would user B know that the message has come from user C who is Posing as user A



* Ex:- User C Posing as User A send a funds transfer request to bank B the Bank will transfer the funds from A account to C account thinking that user A

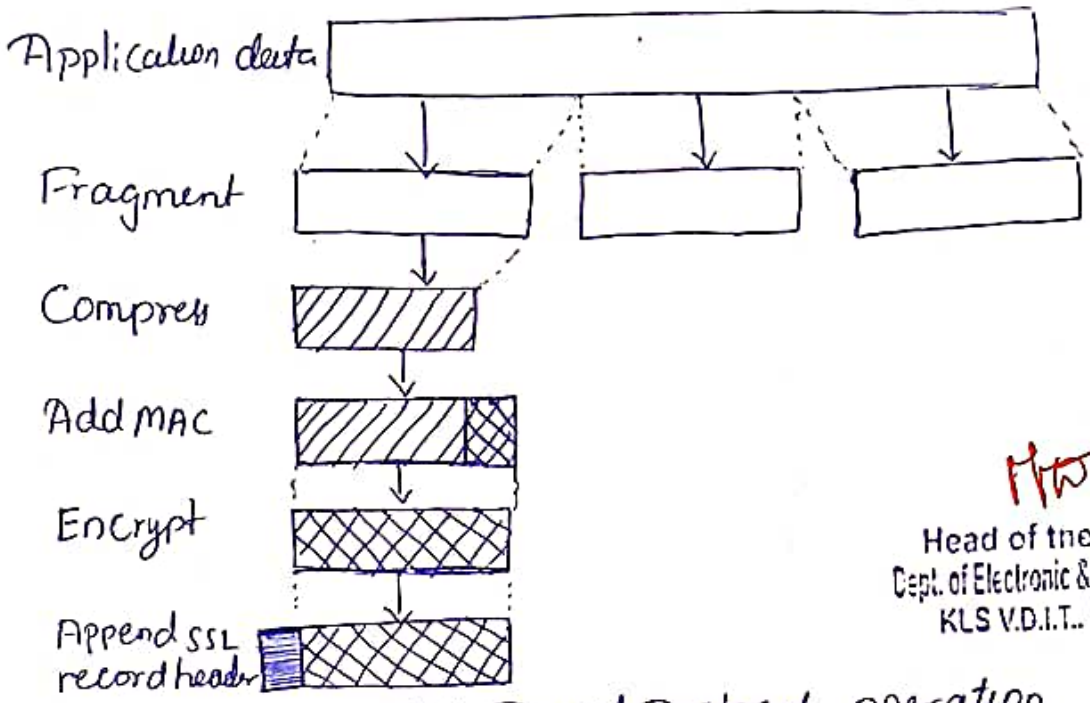
* For instance, consider ...

Q.3 a) Explain SSL Record Protocol and its format with the corresponding diagram 8M

→ The SSL Record Protocol provides two services for SSL Connection

1) Confidentiality:- The handshake Protocol defines a shared Secret key that is used to conventional Encryption of SSL Payload.

2) Message integrity:- The handshake protocol is defined a shared Secret key that is used to form a message authentication code.



SSL Record Protocol operation

* Fig indicates the overall operation of the SSL Record protocol the record Protocol takes an application message to be transmitted, fragments
* the data into manageable blocks optionally compressed the data applies the MAC Encrypt adds a header and transmit the resulting unit in a TCP segment Received data are decrypted verified decompressed and reassembled before being delivered to higher level users
* The first step is fragmentation Each upper layer message is fragmented into blocks of 2 bytes or less
* Compression is optionally applied compression must be lossless and may not increase the content length by more than 1024 bytes
* next message authentication code (MAC) over the compressed data

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

3b) Explain how connection initiates and closes in HTTPS. 6M

→ A normal HTTP connection uses port 80. if HTTPS is specified Port 443 is used.

Connection Initiation

* the client initiates a connection to the server on the appropriate port and then sends the TLS client Hello to begin the TLS handshake when the TLS handshake has finished the client may then initiate the first HTTP request.
* At the HTTP level an HTTP client requests a connection to an HTTP server by sending a connection request to the next lower layer
* At the level of TLS a session is established between a TLS client and a TLS server this session can support one or more connections at any time

Connection closure

* An HTTP client or server can indicate the closing of a connection by including the following line in an HTTP record: connection : close
* This indicates that the connection will be closed after this record is delivered. the closure of an HTTPS connection requires that TLS close the connection with the peer TLS entity on the remote side which will involve closing the underlying TCP connection
* At the TLS level the proper way to close a connection for each side to use the TLS alert protocol to send a close-notify alert. TLS implementation must initiate an exchange of closure alert before closing a connection
* A TLS implementation may after sending a closure alert the connection without waiting for the peer to peer to send its closure alert generate an incomplete close
* TCP connection is terminated without a prior close notify alert and without a connection.

3 c) Explain the Pseudo Random Function used in TLS with a neat diagram 6M

→ * TLS makes use of a pseudo random function referred to as PRF to expand secrets into blocks of data for purposes of key generation or validation.

* The objective is to make use of a relatively small shared secret value but to generate longer blocks of data in a way that is secure from the kinds of attacks made on hash function and MACs

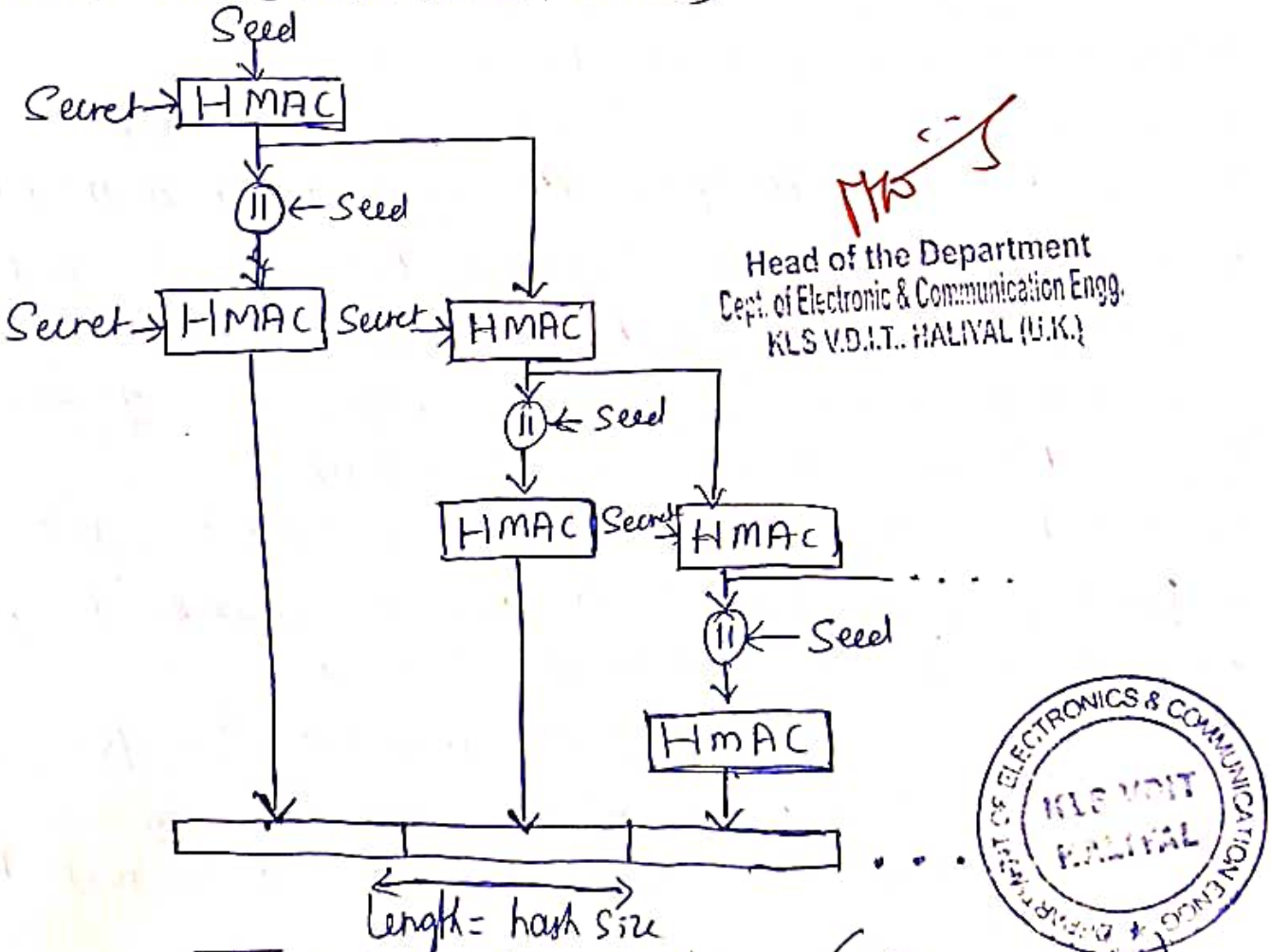
The PRF is based on the data expansion function

P_hash = HMAC_hash (Secret, A(1) || seed) ||
HMAC_hash (Secret, A(2) || seed) ||
HMAC_hash (Secret, A(3) || seed || ---

where A() is defined as

A(0) = Seed

A(i) = HMAC_hash (secret, A(i-1))



TLS Function P_hash (Secret, seed)

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

DEPT. OF ELECTRONICS & COMMUNICATION ENGG. KLS VDIT HALIYAL

* Data Expression function makes use of the HMAC algorithm with MD5 or SHA 1 as hash function
* P_hash can be iterated as many times as necessary
* Each iteration involves two execution of HMAC
* PRF uses two hash algorithm.
  PRF (Secret, label, seed) = Phash (S1, label || seed)
* PRF takes as input secret value an identifying label and a seed value and produces output

Q4 a) Explain SSL Handshake Protocol with a neat diagram. 12M

→ * the handshake 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
* the handshake protocol consists of a series of messages exchanged by client and server all of them have the format

1 byte	3 byte	≥ 0 bytes
Type	Length	Content

* Type (1 byte) :- indicates one of 10 messages.
* Length (3 bytes) :- The length of the message in bytes
* Content (bytes) : The parameters associated with this message
* below fig shows the initial exchange needed to establish a logical connection between client and server, the exchange can be viewed as having four phases

1) Phase 1 - Establish Security Capabilities
2) Phase 2 - Server Authentication and key Exchange
3) ~~Client~~ Phase 3 - Client Authentication and key Exchange
4) Phase 4 - Finish Handshake Protocol

1) Phase 1 - Establish Security Capabilities :- this phase is used to initiate a logical connection and to establish the Security capabilities that will be associated with it

Phase-2 - In phase 2 the server Authenticate itself if needed the Server may send its certificate its public key and may also request certificate from the client At the end the Server announces that the server-hello process is done

Phase 3 - Phase 3 is designed to authenticate the client

Phase 4 - This phase completes the setting up of a Secure Connection.

4b) Explain Local and Remote Random Port format forwarding in SSH connection Protocol 8M

→ * Local forwarding :- allows the client to set up a hijacker process this will intercept selected application level traffic and redirect it from an unSecured TCP connection to a Secure SSH tunnel

* SSH is configured to listen to selected ports SSH grabs all traffic using a selected port and sends it through an SSH tunnel.

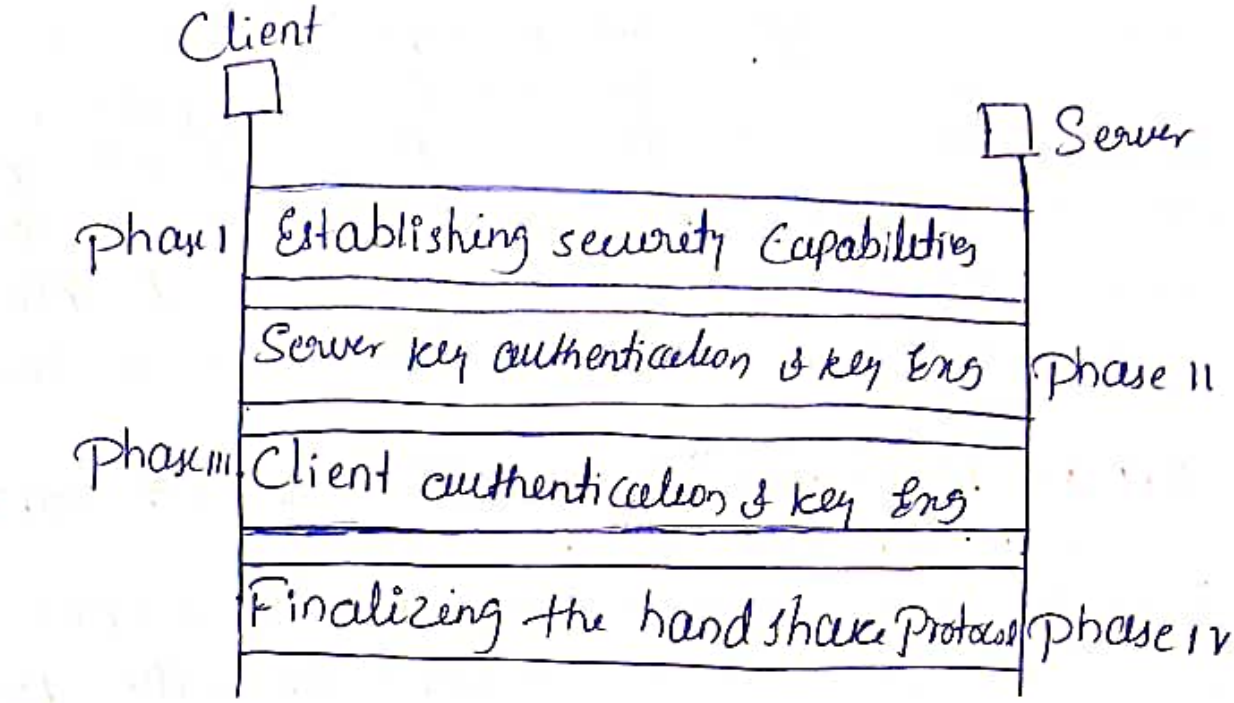
* on the other hand the SSH server sends the incoming traffic to the destination port dictated by the client app's

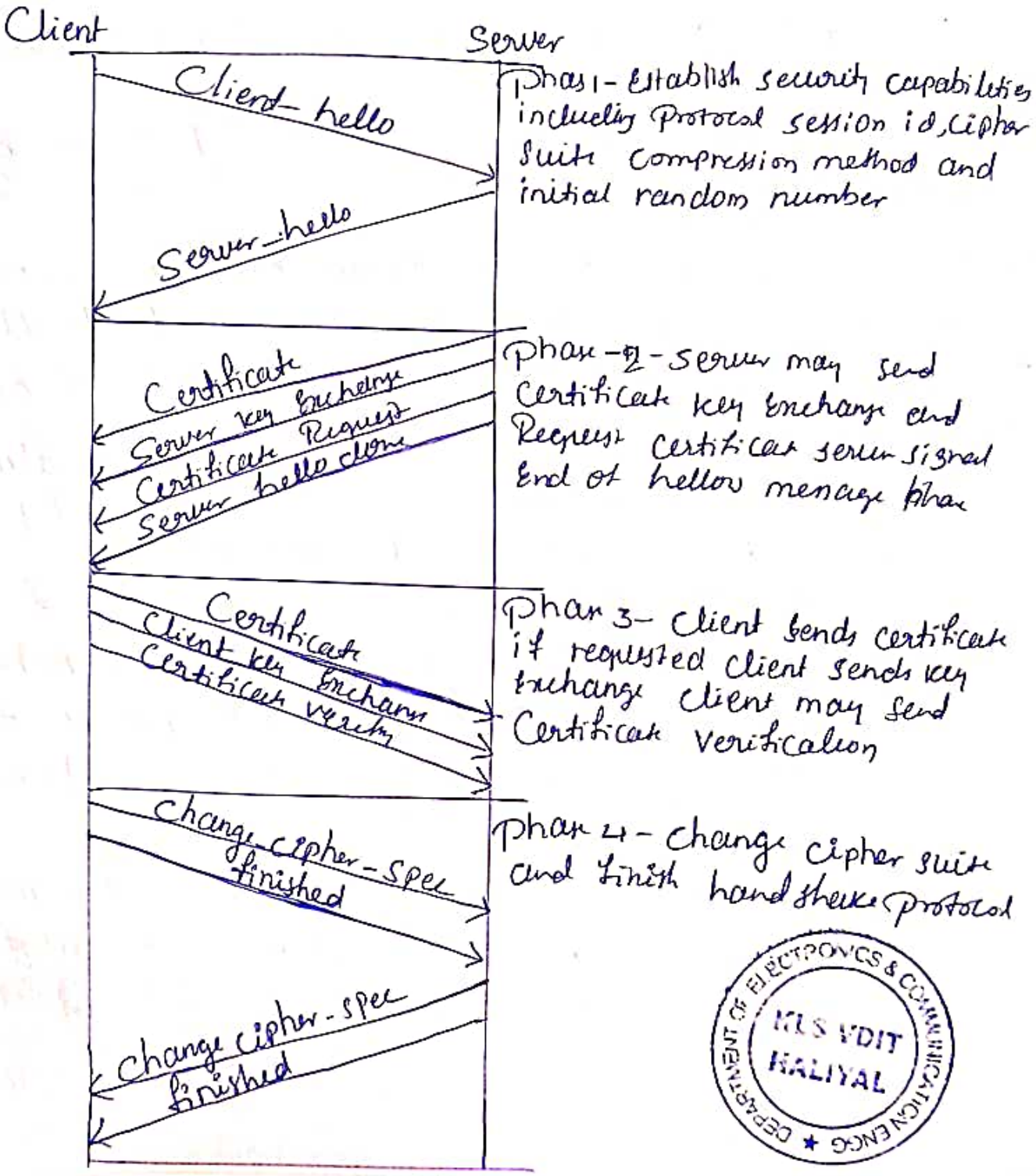
↔ Remote forwarding :- the user's SSH client acts on the server behalf

* the client Receives traffic with a given destination port number places the traffic on the correct port and sends it to the destination the user chooses

Ex :- you wishes to access a server at work from your home computer Because the work server is behind a firewall it will not accept an SSH request from your Home Computer you can set-up SSH tunnel using remote forwarding

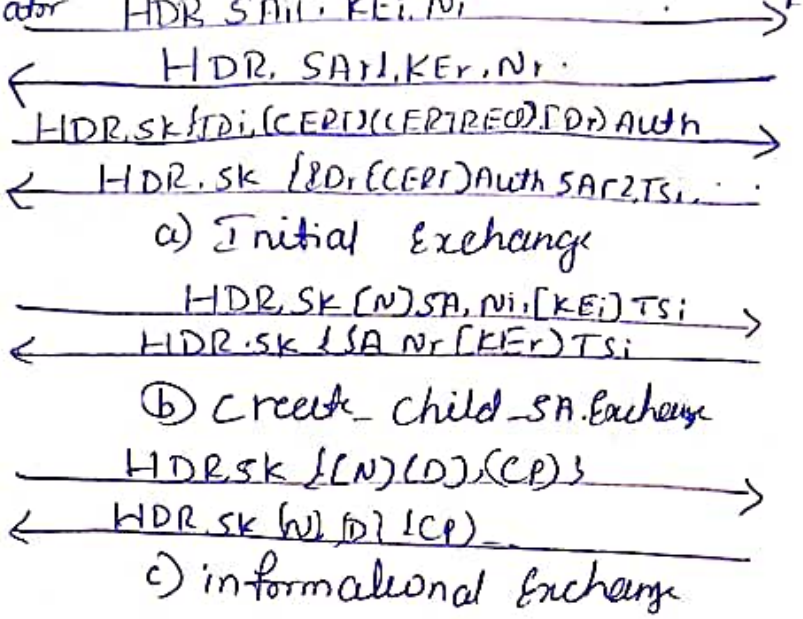
Ex :- Local forward :- Suppose you have an E-mail client On your desktop and use it to get E mail from your Email server via the Post office protocol





5 a) Explain IKEv2 Exchange with a neat diagram 10M

→



* The IKEv2 protocol involves the Exchange of messages in Pairs the first two pairs of Exchange are referred to as the initial Exchanges as in fig In the first Exchange the two Peers Exchange information concerning Cryptosraphy algorithm and other security algorithm they are willing to use along with nonces and Diffie-Hellman Values the Result of this Exchange is to set up a Special SA called the IKE SA this SA defines parameter for a special Secure channel between the peers over the subsequent message Exchange take place. In the Second Exchange the two parties authenticate One another and set up a first IPsec SA to be Placed in the SADB and used for Protecting ordinary Communications between Peers

* the Create child SA Exchange can be used to Establish further SAs for protecting traffic. the informational Exchange is used to Exchange - ment information IKEv2 Error message.

5b) Explain different categories of IP Security Documents in detail 5m

→ * Architecture:- Covers the general concepts security requirements definations, mechanisms defining IP sec technology.

* Authentication header:- AH is an Extension header to Provide message authentication the current specification is RFC 4302 IP Authentication header

* Encapsulating Security payload (ESP):- ESP consists of an Encapsulating header and trailer used to provide Encryption

* Internal key Exchang (IKE):- This is Collection of documents describing the key management schemes for use with IPsec

* Cryptographic algorithms:- this category Encompass a large set of documents that define and describe. Cryptographic algorithm for Encryption message authentication, Pseudorandom function and cryptographic key Exchange.

5c) Explain the Selector used to determine an security policy database 5m

→ * Remote IP Address: This may be a single IP address an Enumerated list or range of addresses or a wildcard address The latter two are required to support more than one destination system sharing the same SA

* Local IP address:- This may be a single IP address an Enumerated list or range of addresses or a wildcard address the latter two are required to support more than one Source system sharing the same SA

* Next layer Protocol:- The IP Protocol header includes a field that designates the protocol operating IP this is Individual Protocol number ANY. OPAQUE

* Name:- A user identifier from the operating s/m this is not a field in the IP header but is available

if IPsec is running on the same operating sys as the user

* Local and Remote ports:- These may be individual TCP or UDP port values an Enumerated list of ports or a wildcard port.

Q6 a) Explain the Parameters of Security ~~association~~ policy and Security association database. 10M

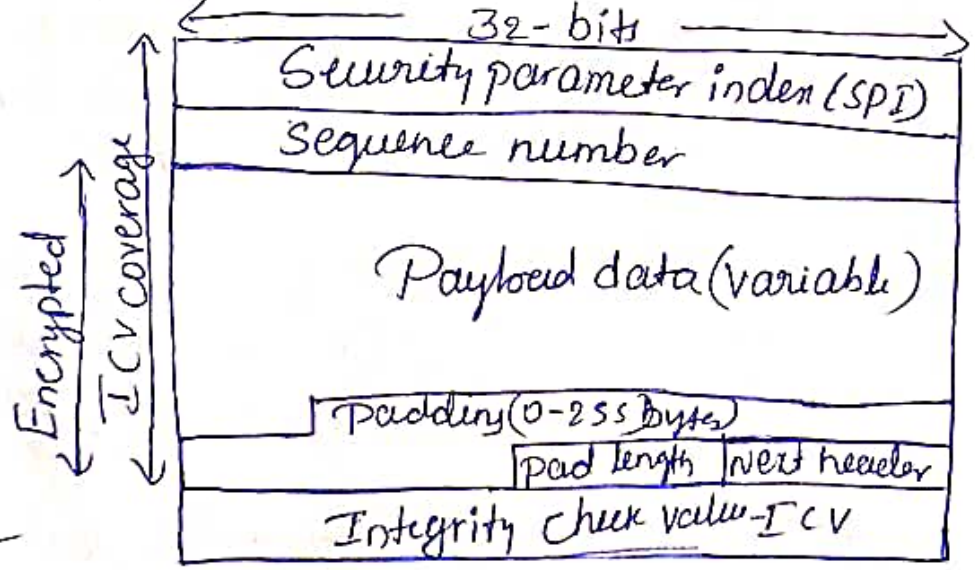
→ Security association Parameters

* Security parameter Index (SPI):- A bit string assigned to this SA and having local significance only the SPI is carried in AH and ESP headers to enables the receiving system to select the SA under which a received packet will be processed
* IP destination Address:- This is the address of destination End point of SA which may be an End user system or a network system such as firewall.
* Security Protocol Identifier:- This field from the outer IP header indicates whether the association is an AH or ESP Security association
* Security association Database:-
* Security Parameter Index:- A 32 bit value selected by the receiving End of an SA to uniquely identify the SA In an SAD entry for an outbonds SA the SPI is used to construct the packets AH or ESP header in an SAD Entry of inbond SA the SPI und to map traffic to the appropreate SA
* Sequence number Counter:- A 32-bit value und to generate the Sequence number field in AH or ESP headers
* Anti replay window:- Und to determine whether an inbond AH or ESP Packet is a replay.
* AH information:- Authentication algorithm, keys, key lifetimes and related Parameters being und with AH

* ESP information:- Encryption and authentication algorithm key initialization values key lifetime and related parameters being used with ESP.
* lifetime of this security association:- A time interval or byte count after which an SA must be replaced with a new SA plus an indication of which of these actions should occur
* Ipsec Protocol mode:- Tunnel or transport mode
* Path MTU:- any observed path maximum transmission unit and aging variables.

6b) Explain ESP packet format with the relevent diagram 10m

→* Security Parameter index (32 bits):- Identifies a Security association
* Sequence number (32-bits):- A monotonically increasing counter value this provide an anti-replay function as discussed for AH
* Payload Data (variable):- this is a transport-level segment that is protected for AH
* Padding (0-255byte) The purpose of this field is discussed later
* Pad length (8 bits):- indicates the number of pad bytes immediately Preceding this field.
* Next header (8 bits): Identifies the type of data contained in the payload data field by identifying the first header in that payload.

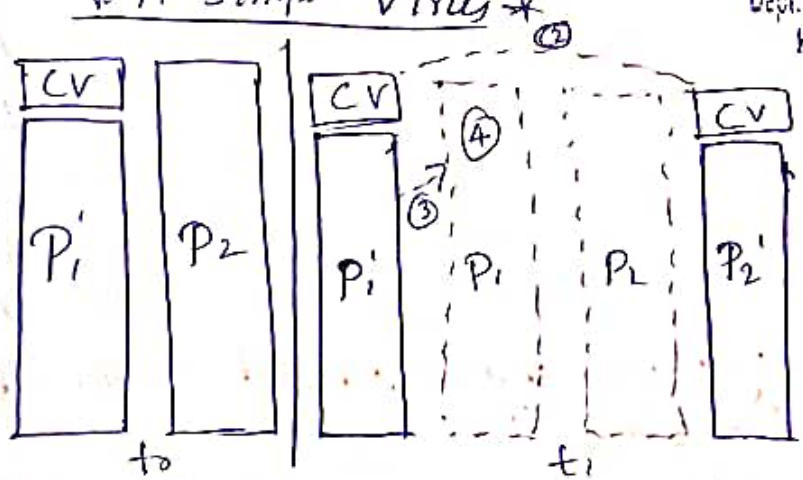


* The infected program begins with the virus code.
* The first line of code is a jump to the main virus program
* The second line is a special marker that is used by virus to determine whether not a potential victim program
* When the program is invoked control is immediately transferred to the main virus program.

```
Program V:=
{goto main;
 1234567;
 Subroutin infect Executable:=
 {loop:
 file:=get-random-Executable-file;
 if (first-line of file =1234567)
 then goto loop
 Else Prepend V to file;}
 Subroutin do damage:=
 {whether damage is to be done}
 Subroutine trigger-pulled:=
 {return true if some condition holds}
main main-program:=
 {infect-Executable;
 if trigger-pulled then do-damage
 go to next;}
next:
}
```

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

* A Simple Virus *



A Compression Virus

Q7 a) Explain various intrusion techniques with an examples each 8M

→ * 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 a fixed-length output is produced

Ex:- Cryptographic has function such as SHA 256 and produce a fixed-size ~~length~~ string of bytes typically a hash code.

Lets take input menage "hello"

* using the SHA-256 hash function the output would be-

2cf2adba5fb03ae26083b2c5b9e1b1

This has code is unique to the input hello its straight forward to compute the hash from the input but its extremly difficult to reverse the proces and determine the original input just from the hash code

* Access control:- Access to the password file is limited to one or a very few accounts if one or both of these counter-measures are in place some effort is needed for a potential intruder to learn passwords. On the basis of a survey of the literature and interview with a number of password.

Ex:- Only authorized employees can access the company Internal network, Every employee is having Authentication as username and password to access network

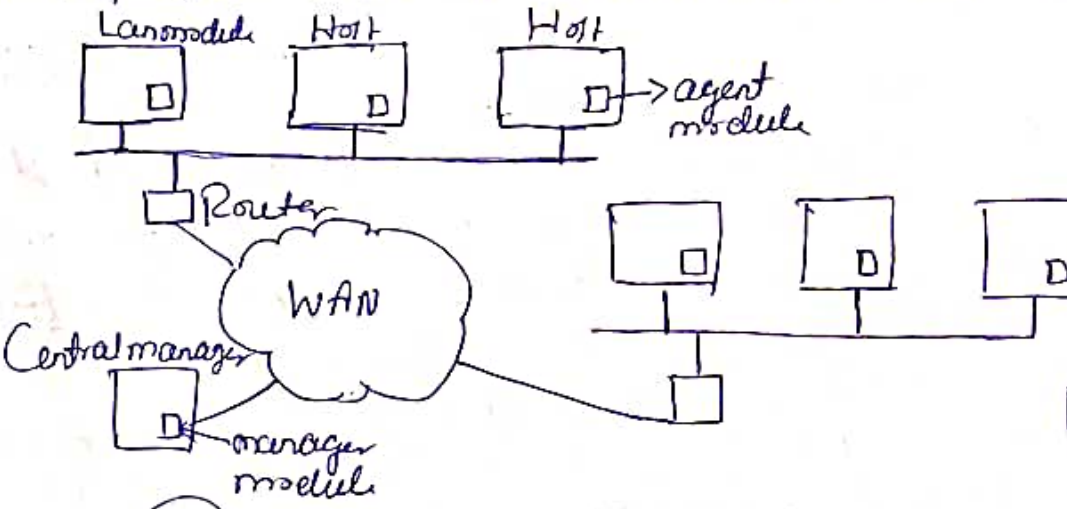
7 b) Explain the general virus structure and the logic for Compression virus 12M

→ The virus structure as shown in this case virus code V is prepended to infected program and it is assumed that the entry point to the program

1) For each uninfected file P2 that is found the virus first compresses that file to produce P1 which is shorted than the original program by the size of the virus
2) A copy of the virus is prepended to the compressed program
3) the compressed version of the original infected program is uncompressed
4) the uncompressed original program is executed.

Q8 a) Explain distributed intrusion detection with relevant diagram 10M

→ * A distributed intrusion detection system may need to deal with different audit record formats in a heterogeneous environment different systems will employ different nature audit collection systems and if using intrusion detection may employ different formats for security related audit records
* One or more nodes in the network will serve as collection and analysis points for the data from the systems on the network thus either raw audit data or Summary data must be transmitted across the network



* Architecture for Distributed intrusion Detection
* Host agent module:- An audit collection module operating as a background process on a monitored system its purpose is to collect data

* LAN monitor agent module:- Operate in the same fashion as a host agent module except that it analyzes LAN traffic and reports the results to the central manager
* Central manager module:- Receives Reports from LAN monitor and host agents and processes and correlates these reports to detect intrusion.

8 b) Explain the different generations of anti-virus. 10M

→ * First generation – Simple scanners
* Second generation - heuristic scanners
* Third generation – activity traps
* Fourth generation - full-featured protection.

* First generation:- Scanner requires a virus signature to identify a virus the virus may contain 'wildcards' but has essentially the same structure and bit pattern in all copies such signature specific scanners are limited to the detection of known viruses another type of first generation scanner maintains a record of the length of programs and looks for changes in length.
* Second generation:- Scanner does not rely on a specific signature Rather the scanner uses heuristic rules to search for probable virus infection one class of such scanners look for fragments of code that are often associated with virus.
* another second generation approach is integrity checking checksum is appended to each program. if a virus infects the program without changing the checksum then an integrity check will catch the change
* Third generation:- Programs are memory resident programs that identify a virus by its actions rather than its structure in an infected program Such programs have the advantage that it is not necessary to develop signature and heuristics for a wide array of viruses Rather than it is necessary only to identify the small set of actions that indicate an infection is being attempted.

* Fourth generation:- products are packages consisting of a variety of antivirus techniques used in conjunction these include scanning and activity trap components in addition such a package include access control capacity which limits the ability of virus to penetrate a system and then limits the ability of a virus to update files in order to pass on the infection.

9 a) Explain the design goals for a firewall and the general techniques used by it to control access. 10M

→ Design goals:-

* All traffic from inside to outside and vice versa must pass through the firewall this is achieved by physically blocking all access to the local network except via the firewall

* Only authorized traffic as defined by the local security policy will be allowed to pass various types of firewall are used which implement various types of security policy

* The firewall itself is immune to penetration this implies the use of a hardened system with a secured operating system trusted computer system are suitable for ~~hard~~ hosting a firewall and often required in government applications.

→ Control access

* Service control:- Determines the types of Internet service 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 interpreted each service request before passing on

* Direction control:- Determines the direction which particular service request may be initiated and allowed to flow through the firewall

* User control:- Controlls the access to a service according to which user is attempting to access

-it this feature is typicaly applied to users inside the firewalls perimeter it may also be applied to incoming traffic from external users

* Behaviour control: Controls how particular services are used 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) Explain Baston host firewall biasing :10M

→ * A Bastion host system identified by the firewall administration as critical strong point in the networks Security Typically the bastion host server as a platform for an application

* the bastion host hardware Platform execute a Secure version of its operations system making it a hardened System

* Only the Services that the network administrator Considers enential are installed on the bastion host these could include Proxy applications for DNS, FTP.

* the bastion host may require adelitional authentication before a user is allowed access to Proxy Server

* Each Proxy is configured to allow access only to specific host system this means that the limited Command / feature set may be applied Only a subset of System on the protected network

* Each Proxy maintains details audit information logging all traffic

* Each Proxy module is a very small software specifically designed for network security.

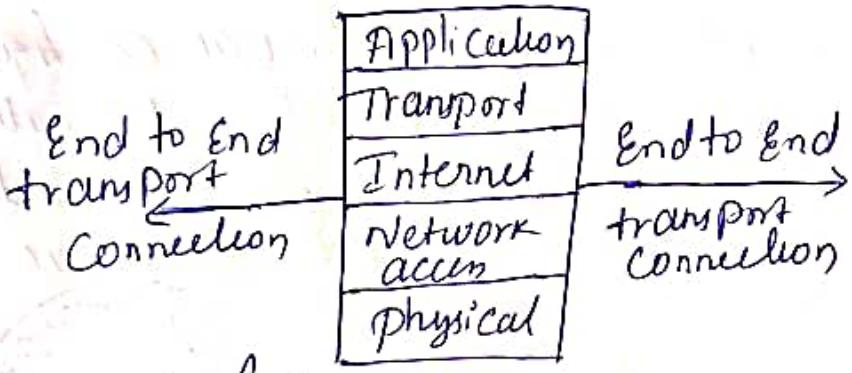
* Each Proxy is independent of other proxies on the bastion host if their is a problem with the operation of any Proxy

* Each Proxy runs as a non Priviledge user in a private and secured directory on the bastion host.

10a) Explain packet filtering firewall with example (10M)

→ * Packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards the firewall is typically configured to filter packets going in both direction. Filtering rules are based on information contained in a network packet

* Source IP address:- The IP address of the system that originated the IP packet (Ex: 192.178.1.1)
* Destination IP address: the IP address of the system the IP packet is packet is trying to reach (Ex: 192.168.1.2)
* Source and destination transport level address:- the transport level port number which defines applications such as SNMP or telnet
* IP Protocol field: Defines the transport protocol.
* 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 filter is set up as a list of rules based on matched to fields in the IP or TCP header



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

* Packet filtering Example

Rule set A

Action	ourhost	port	theirst	Port	Comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	Connection to our SMTP port

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGG. KLS VDIT HALIYAL

* Inbound mail is allowed but only to a gateway host However packets from a particular External host SPAM are blocked because that host has a history of Sending massive files in E-mail messages.

10b) Explain the working of distributed firewall with a neat diagram. 10m

→ * A distributed firewall configuration involves stand alone firewall devices plus host based firewalls working together under a central administrative control.

* Administrator can configure host resident firewalls on hundreds of servers and workstations as well as configure Personal firewalls on local and remote user system
* Tools let the network administrator set policies and monitor Security across the Entire network these firewalls protect against internal attacks and provide protection tailored to specific machines and applications
* Stand alone firewall provide goods protection including internal firewalls and an External firewall
* With distributed firewalls it is possible to Establish both an Internal and External DMZ.
* An important aspect of distributed firewall configuration is Security monitoring such monitoring typically includes log aggregation and analysis firewalls statistics and fine-grained remote monitoring of individual hosts if needed.

Ashwa

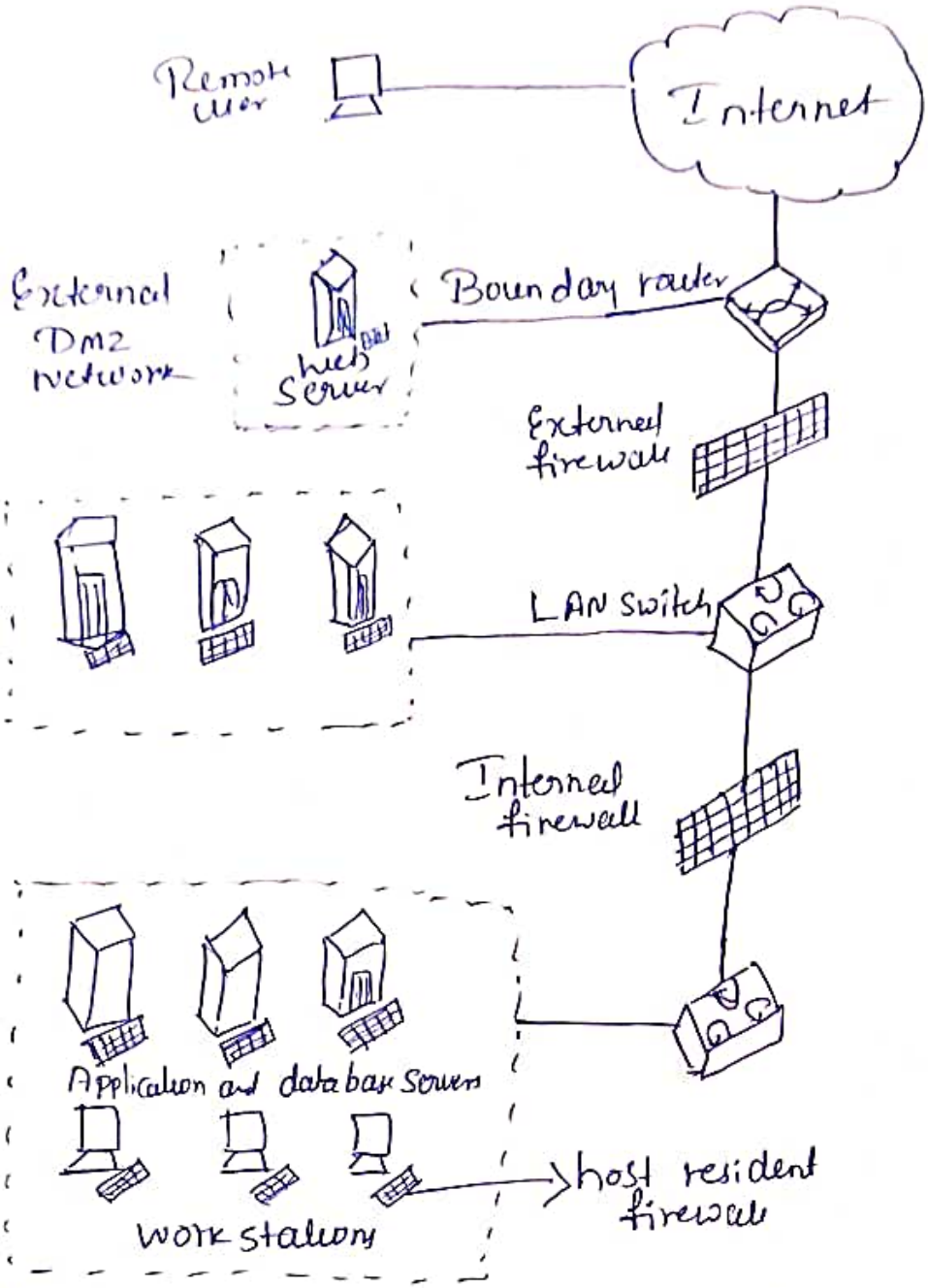


fig:- Distributed firewall configuration