CBCS SCHEME

USN | | | | | | | | | | 15EC835

Eighth Semester B.E. Degree Examination, November 2020
Network and Cyber Security

Time: 3 hrs. Max. Marks: 80

Note: Answer any FIVE full questions irrespective of modules.

Module-1

1 a. Write the comparison of threats on the web. (08 Marks)
b. What is port forwarding? Explain local and remote forwarding. (08 Marks)

2 a. Explain different phases in a SSL handshake protocol. (10 Marks)
b. Explain the following with respect to transport layer security :
i) Pseudorandom function
ii) Alert codes. (06 Marks)

Module-2

3 a. Explain PGP message generation and reception techniques. (08 Marks)
b. With the help of function modules and standardized protocols explain internet mail architecture. (08 Marks)

4 a. Explain S/MIME functionality. (08 Marks)
b. With a neat diagram, explain DKIM functional flow. (08 Marks)

Module-3

5 a. Explain IPSec architecture. (08 Marks)
b. Explain the basic combinations of security associations. (08 Marks)

6 a. Discuss the processing model for outbound packets. (08 Marks)
b. Explain $IKEV_2$ exchanges. (08 Marks)

Module-4

7 a. Explain the primal design forces in cyber security domain. (08 Marks)
b. Explain the antipattern for policy–driven security certifications. (08 Marks)

8 a. Explain any two cybersecurity antipattern catalogs. (10 Marks)
b. Explain full cyber antipattern template. (06 Marks)

Module-5

9 a. Explain the Zachman framework for enterprise architecture. (10 Marks)
b. List the typical re-imaging sequence for the windows OS. (06 Marks)

10 a. Explain any two key techniques for architectural problem solving patterns. (08 Marks)
b. Explain any four host based security technologies. (08 Marks)

* * * * *

Scheme & Solutions Prepared by

Prof. Damodar. H.

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

Q.No | Sub: Network & Cyber Security (15EC835) : Nov-2020 QP Solutions. | Marks

1.a) Write the comparision of threats on the web | 08

Comparision of threats on the web interms of Integrity confidentiality, Denial of service and Authentication

* Integrity:

Threats	Consequences	Countermeasures	
* Modification of user data * Trojan horse browser * Modification of memory * Modification of message traffic in transit.	* Loss of information * Compromise of machine * Compromise of machine * Vulnerability to all other threats	* Cryptographic checksums	3

* Confidentiality

Threats	consequences	Countermeasures	
* Eavesdropping on net * Theft of information from server * Theft of data from client * Info about n/w configuration	* Loss of information * Loss of privacy	* Encryption, web policies	2

* Denial of service

Threats	Consequences	Countermeasures	
* Killing of user - threads * Flooding machine with bogus requests * Filling up disk or memory.	* Disruptive * Annoying * Prevent user - from getting work done	* Difficult to prevent	2

Q.No | Mar

* Authentication

Threats	Consequences	Countermeasures	
* Impersonation of legitimate users * Data forgery	* Misinterpretation of user * Belief that false information is valid	* Cryptographic techniques	1

1.b What is port forwarding? Explain local and remote forwarding. 08

* Port forwarding provides the ability to convert any insecure TCP connection into a secure SSH connection. This is also referred to as SSH tunnelling
* A port is an identifier of a user of TCP
* Any application that runs on top of TCP has a port number. 2
* Incoming TCP traffic is delivered to the appropriate application on the basis of the port number.
* An application may employ multiple port numbers.

> Local forwarding

* Allows the client to setup a hijacked process this will intercept selected application-level traffic and redirect it from an unsecured TCP connection to a secure SSH connection
* Example: Suppose we have an email client on desktop and use it to get email from your mail server via the Post Office Protocol (POP) The assigned port number for POP3 is port 110 we can secure this traffic in the following way. 3

1.) The SSH client setup a connection to the remote server
2.) Select the unused port number, say 9999

and configure SSH to accept traffic from this port destined for port 110 on the server

3.) The SSH client informs the SSH server to create a connection to the destination, in this case mail server port 110

4.) The client takes any bits sent to local port 9999 and sends them to the server inside the encrypted SSH session. The SSH server decrypts the incoming bits and sends the plaintext to port 110

5.) In other direction, the SSH server takes any bits received on port 110 and sends them inside the SSH session back to the client, who decrypts and sends them to the process connected to port 9999

> Remote Forwarding

* The user's SSH client acts on the servers' 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.

Steps:

1.) From work computer, setup an SSH connection to home computer. The firewall will allow this because it is a protected outgoing connection

2.) Configure the SSH server to listen on a local port say 22 and to deliver data across the SSH connection addressed to remote port, say 2222

3.) You can now go to your home computer and configure SSH to accept traffic on port 2222

MARKS

2.a) Explain different phases in a SSL handshake protocol. 10

* SSL Handshake protocol has four phases.

Phase 1: Establish Security capabilities

* The exchange is initiated by the client, which sends the client hello message with the following parameters:
  * Version: The highest SSL version understood by the client.
  * Random: A client generated random number which serves as nonce.
  * Session id: A variable length session identifier
    - A non zero value - client update
    - A zero value - client new connection
  * Ciphersuite: List of cryptographic algorithms supported by client in decreasing order of preference.
  * Compression method: List of compression methods supported by client.

2

Phase 2: Server Authentication and Key Exchange

* The server sends a server_key_exchange message which contains list of secret keys to be used for subsequent data.
* The Certificate_request message is sent which includes two parameters
  - Certificate type and Certificate_authorities
* The final message in phase 2 is the server_done message.
  - Indicates the end of the server hello and associated messages.

2

2

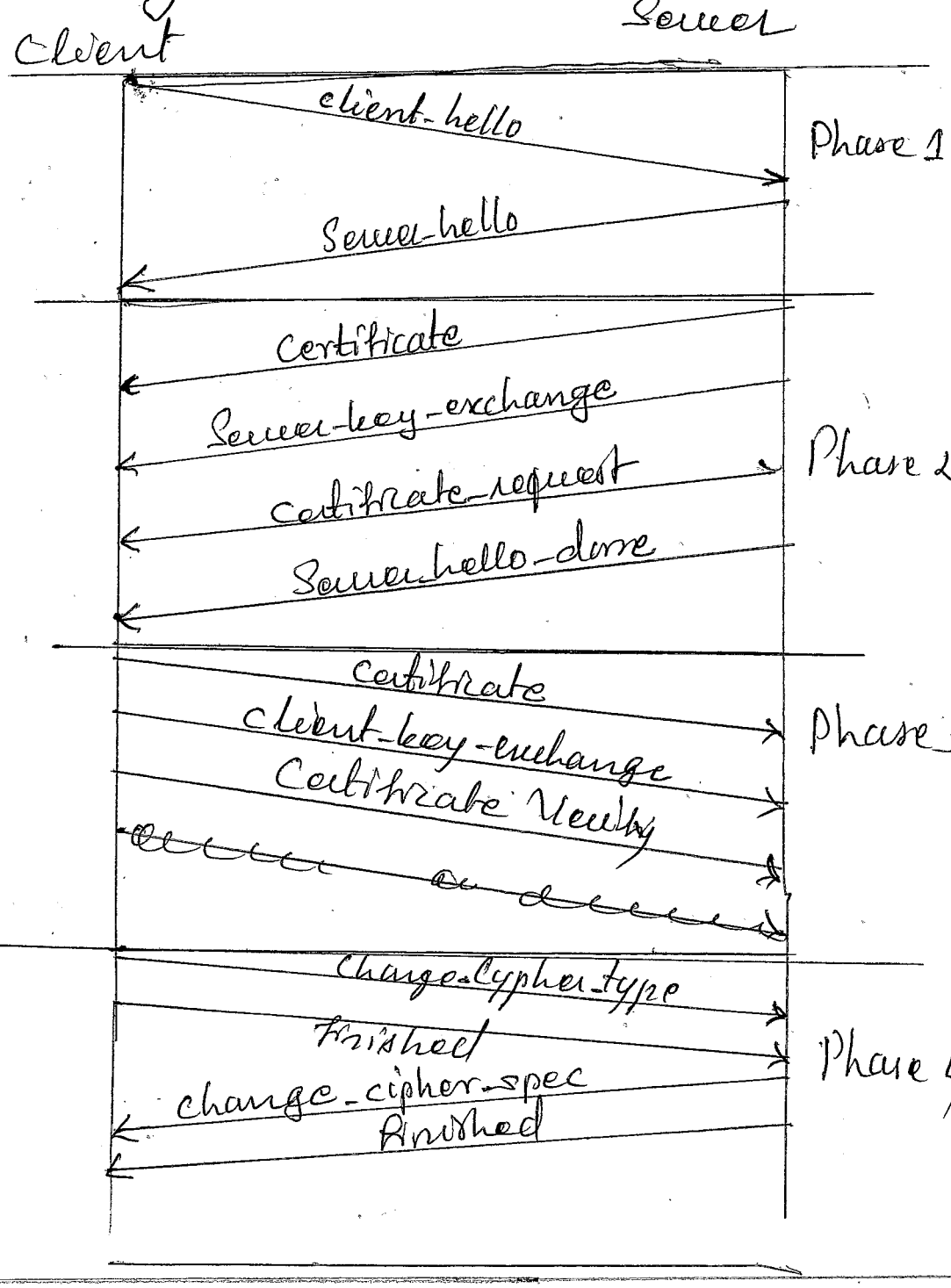
> Phase 3 : Client Authentication and key exchange

* The client verifies the server certificates and checks whether the server_hello parameters are acceptable
* If all is satisfactory, the client sends a certificate message. If the server has requested a certificate. If no suitable certificate is available, the client sends a no_certificate alert 2
* Next is the client_key_exchange message which has the same parameters as the server key_exchange message
* Similarly, the client may send a certificate verify message to provide explicit verification of a client certificate.
* The client encrypts all the previous messages and master secret with its finished key.

> Phase 4 : Finish

* This phase completes the setting up a secure connection
* The client sends a change_cipher_spec message and copies the pending Cipher Spec into the current Cipher Spec. 2
* Moreover, the client then immediately sends the finished message under the new algorithms, key and secrets.

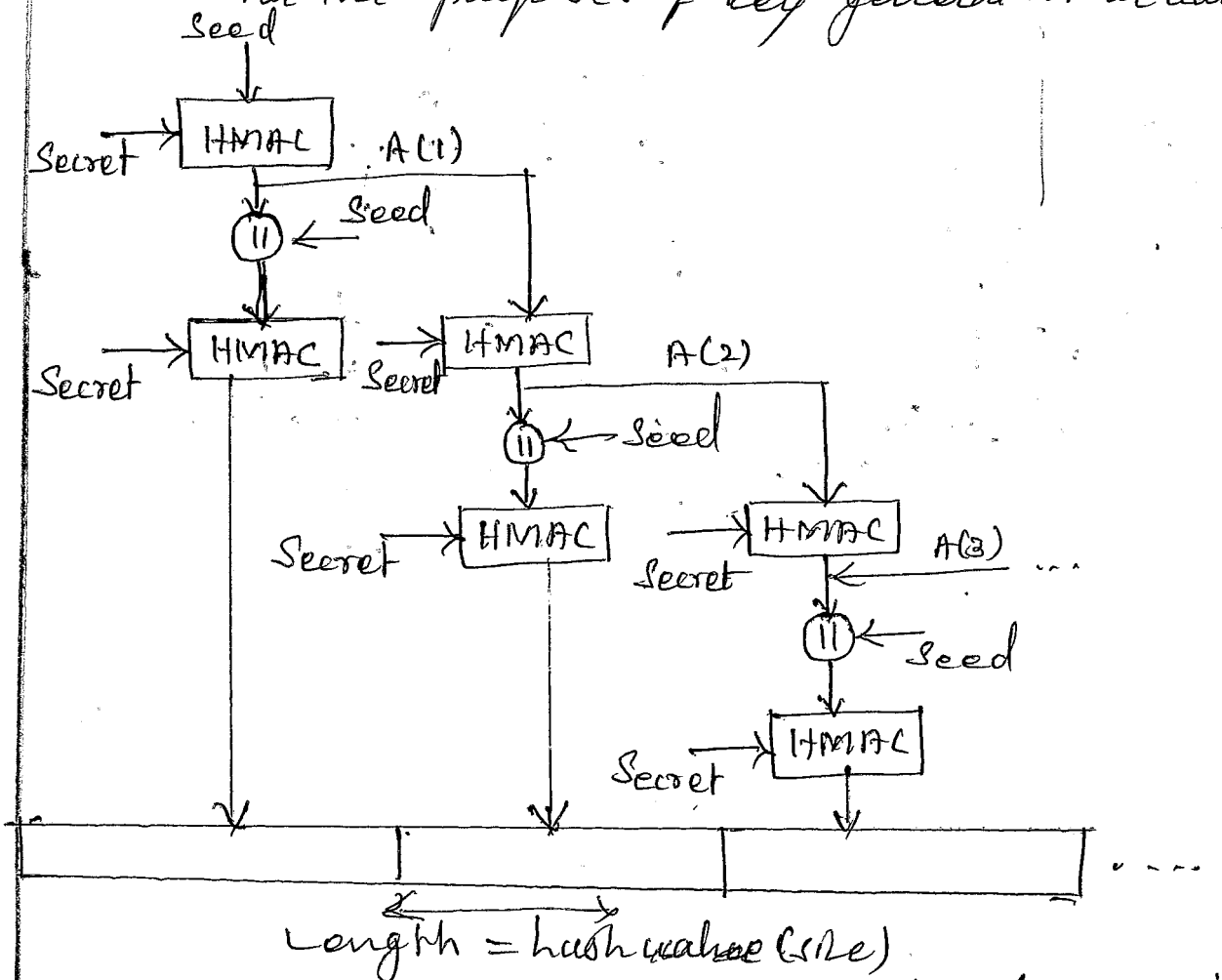
* The content of the finished message is the concatenation of two hash values
* The server sends its own change-cipher-spec message, transfer the pending to the current Cipher spec and sends it finished
* At this point the handshake is complete and the client and server may begin to exchange application layer data.



Q.No		Marks
2.b	Explain the following with respect to transport layer security (i) Pseudo random function (ii) Alert codes	06

(i) Pseudo random function:

* TLS makes use of a pseudorandom function referred to as PRF to expand secrets into blocks of data for the purposes of key generation or validation



3

* PRF takes as input a secret value an identifying label, and a seed value and produces an output of arbitrary length.

(ii) Alert Codes

TLS alert codes * Fatal and other ~~fatal~~ alert code

Fatal: * Unknown_ca, * Access_denied * Decode error, * Protocol_version, * Insufficient_security * Unsupported_extension, * Internal error, * Decrypt error

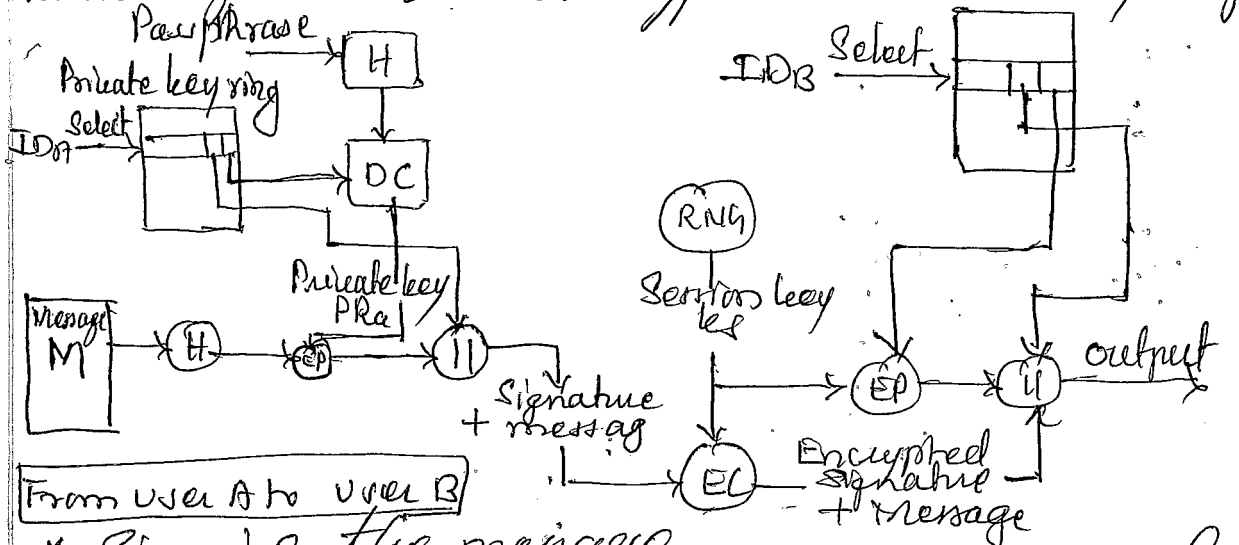
3

Non fatal alert codes
* User_cancelled * No_renegotiation
Explanation of any - 2

3 a) Explain PGP messages generation and reception techniques. 08

> Message transmission

Figure shows the steps during message transmission assuming that the message is to be both signed and encrypted.



2

* Signing the message
* PGP retrieves the sender's private key from the private-key ring using user id as an index
* PGP Prompts user for Pass Phrase
* Signature component of the message is constructed.

* Encrypting the message
* PGP generates a session key and encrypts the message
* PGP retrieves the recipient's public key from the public key ring using user id as an index
* The session key component of the message is constructed.

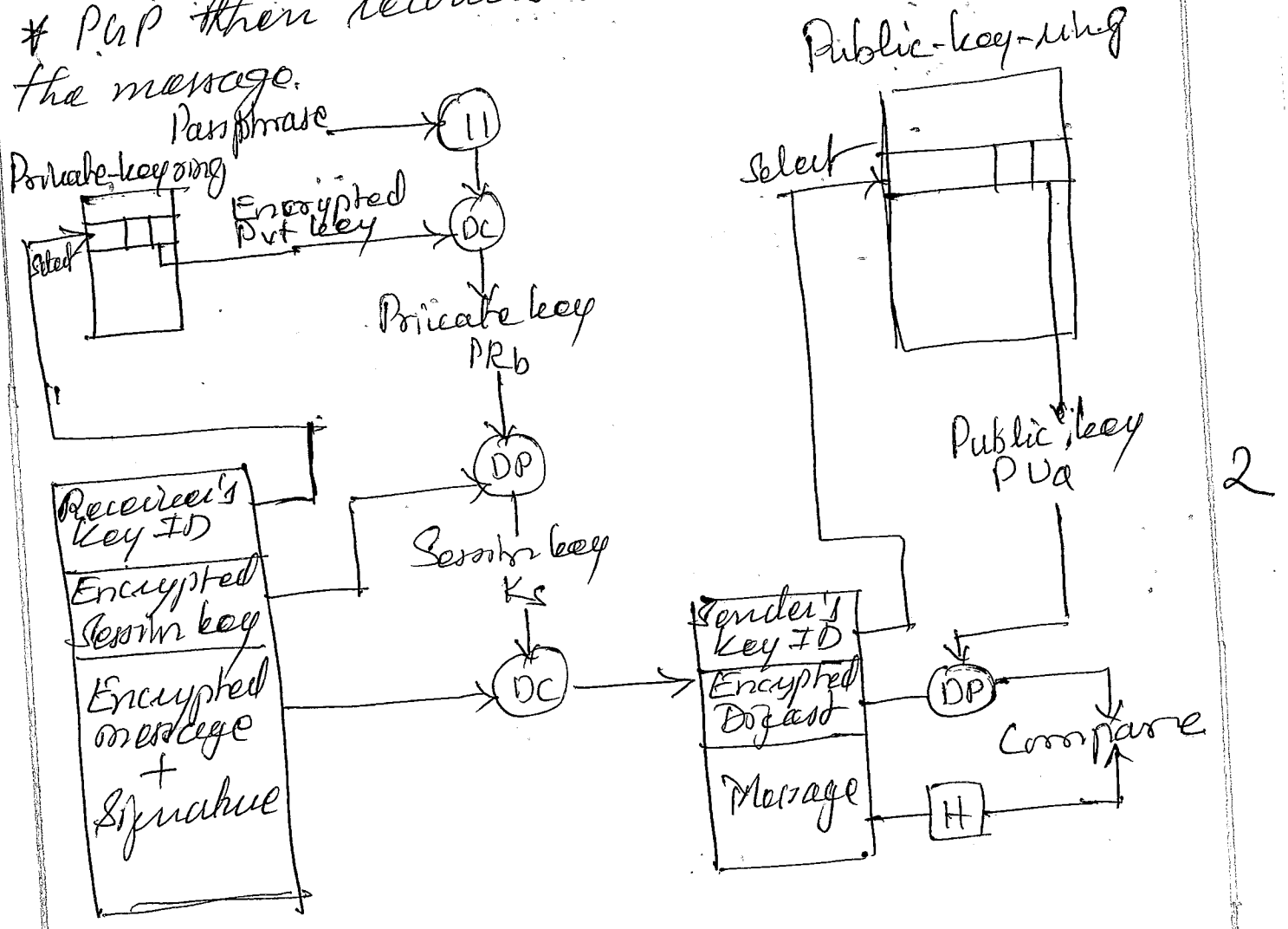
3

Message Reception

The receiving PGP entity performs the following steps

2

* PGP retrieves the receiver's private-key ring using the key ID field in the session key component of the message as an index.
* PGP prompts the user for the passphrase to recover the unencrypted Private key.
* PGP then recovers the session key & decrypts the message.

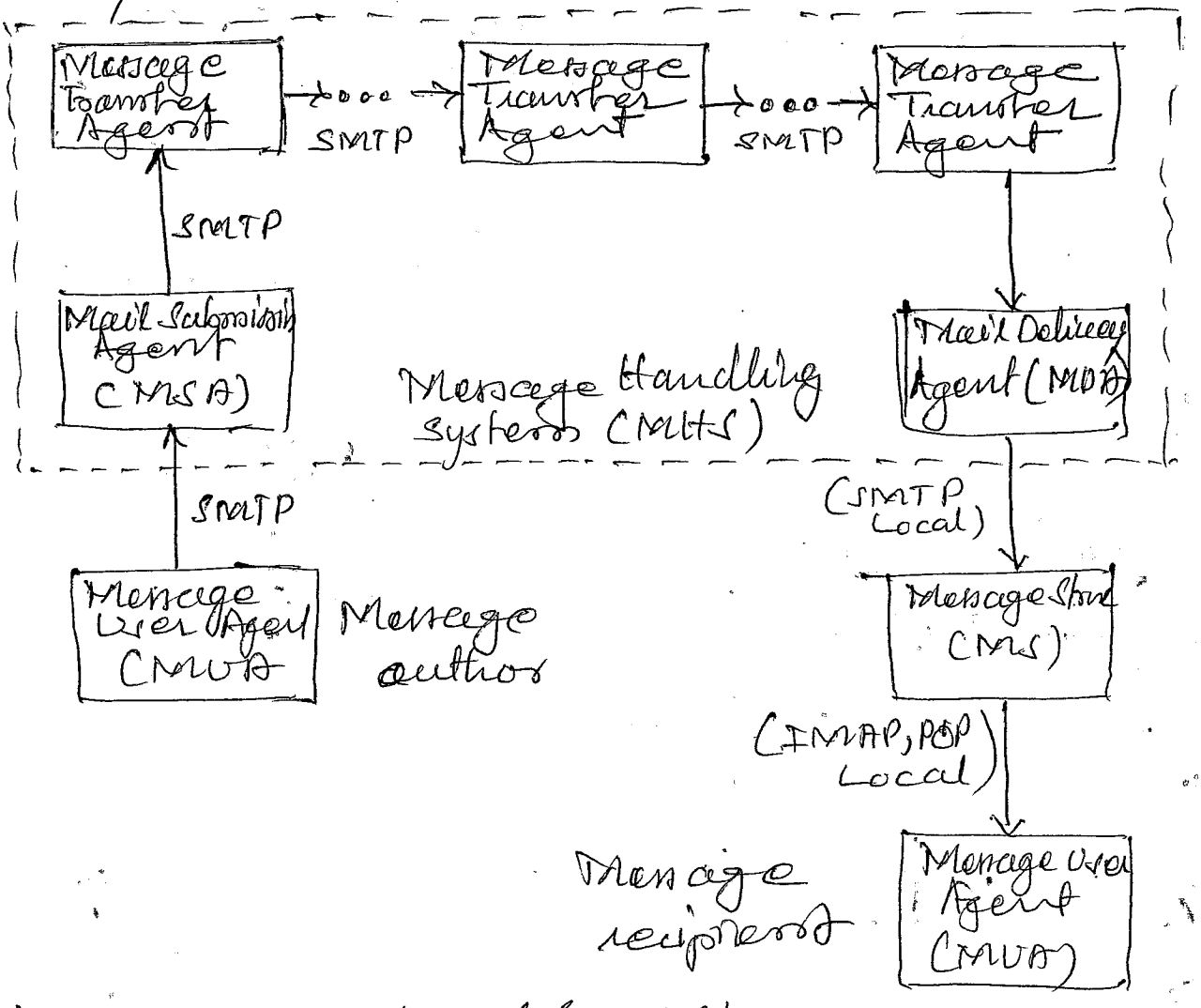


2

Marks

3.b With the help of function modules and standardized protocols explain Internet Mail Architecture. 08

Figure shows Internet Mail Architecture and its key function modules



2

> Message User Agent (MUA)

* Operates on the behalf of users actors and user applications
* Referred as a client email program or local n/w email server
* Formats message and performs initial submission into MHS via a MSA 2
* Receipient MUA processes received mail for storage and/or display to the receipient user

- Mail Submission Agent (MSA)
  - * Accepts the message submitted by an MUA and enforces the policies of the hosting domain and the requirements of Internet standards.
  - * The Simple Mail Transfer Protocol (SMTP) is used between the MUA and the MSA

- Message Transfer Agent (MTA)
  - * Relays mail for one application-level hop
  - * makes routing assessments
  - * Relaying of message is performed by a sequence of MTA's until the message reaches a destination MDA.
  - * Adds Trace information to the message header

2

- Mail Delivery Agent
  - * Responsible for transferring the message from MTS to the MS

- Message Store (MS)
  - * Located on remote server or on the same machine.
  - * An MUA retrieves messages from a remote server using POP (Post Office Protocol) or IMAP (Internet Message Access Protocol)

2

Q. No		MARKS
4.a.	Explain S/MIME functionality	08

S/MIME provides the following functions

1.) Envelope data: This consists of encrypted content of any type and encrypted content encryption keys for one or more recipients 2

2.) Signed data: A digital signature is formed by taking the message digest of the content to be signed and then encrypting with the private key of the signer. A signed data message can be only be viewed by a recipient with S/MIME capability. 2

3.) Clear-signed data: As with signed data, a digital signature of the content is formed.

* Only digital signature is encoded using base 64. 2
* Recipients without S/MIME capability can view a message content.

4.) Signed enveloped data:

* Signed only and encrypted only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted. 2

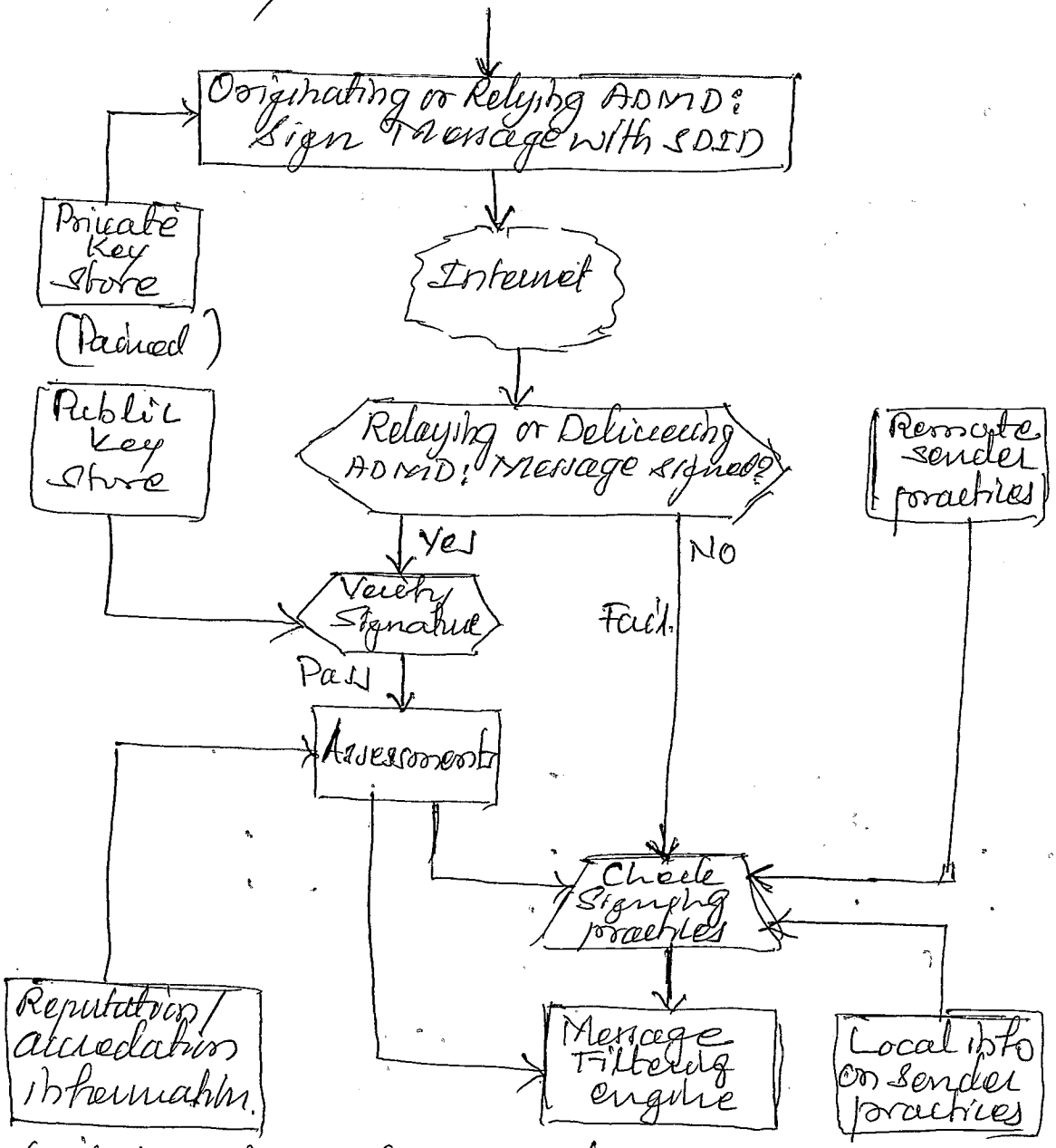
4.b.	With neat diagram, explain DKIM function flow.	08

Figure shows DKIM function flow.

* Basic message processing is divided between a signing Administrative Management Domain (ADMD) and verifying ADMD.

M

* Signing is performed by an authorized module within the signing ADMD and uses private information from a key store



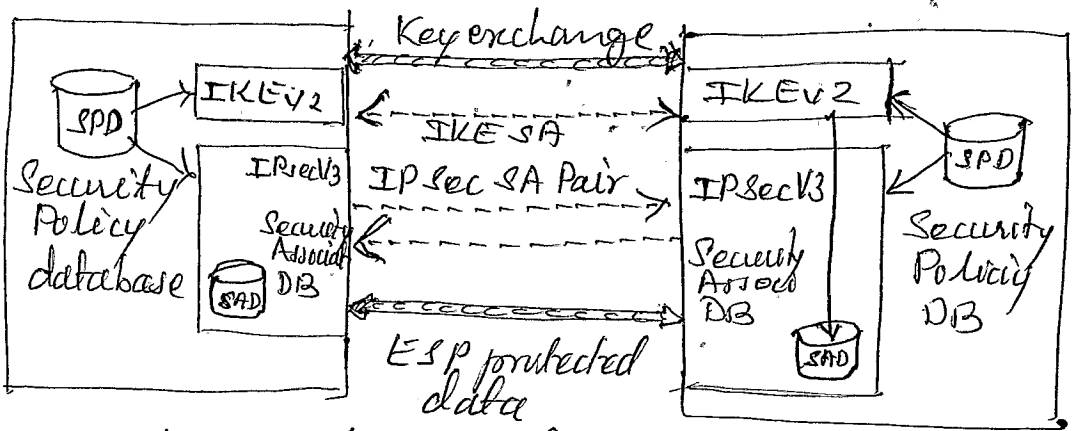
4

* Verifying is performed by an authorized module within the verifying ADMD, verifying might be performed by an MTA, MDA or MUA.
* Verifying the signature uses public information from key store. If the signature passes, reputation information is used to asses the signer and that information is passed to the message filtering system.
* If the signature fails, information about signing practices of authors can be retrieved remately or locally

4

* The signature includes a number of fields
  * v = DKIM version
  * a = Algorithm used to generate the signature
  * c = Canonicalization used on the header and body
  * d = A domain name used as an identifier to refer to the identity of a responsible person or organization
  * s = Selector, a name associated with a key
  * h = Signed Header fields
  * bh = hash
  * b = Signature data in base 64 format.

5a) Explain IP Sec Architecture. 8



2

* Fundamental to the operation of IPsec is the concept of a security policy applied to each IP packet that transits from a source to a destination
* IPsec policy is determined primarily by the interaction of two databases, the security association database (SAD) and security policy database (SPD)
* Security Association is a one way logical connection between a sender and a receiver that affords security services to the traffic carried on it.

9 No | Marks

* A security association is uniquely identified by three parameters: Security Parameter Index (SPI)
  * * SPI is a 32-bit unsigned integer assigned to this SA and has local significance only
  * IP Destination Address: This is the address of the destination endpoint of the SA
  * Security Protocol Identifier: Indicates whether the association is an AH or ESP security association

2

* Security Association Database defines the parameters associated with each SA
* A security association is defined by the following parameter in SAD entry
  * Security Parameter Index
  * Sequence Number counter
  * Sequence Counter overflow
  * Anti-Replay Window
  * AH information
  * ESP Information
  * IP Sec Protocol mode
  * Path MTU

2

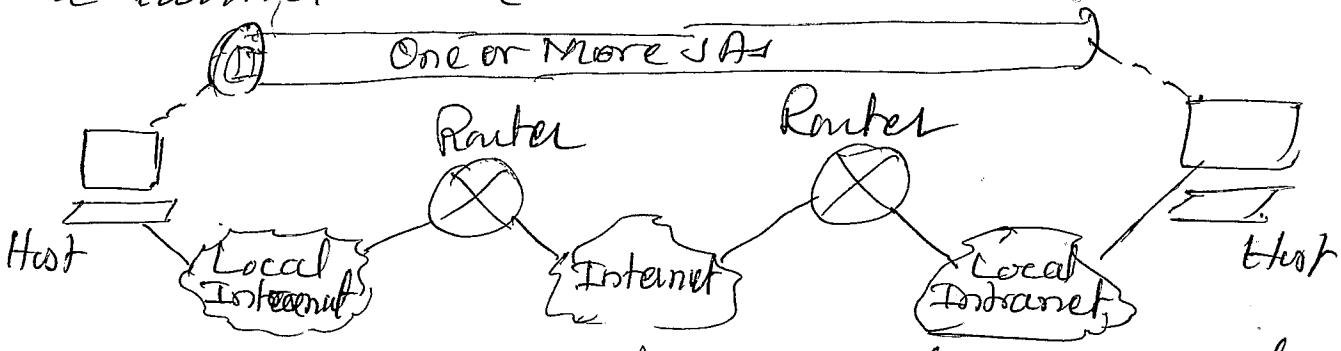
* Security Policy Database:
  * Contains entries which defines a subset of IP traffic and points to an SA for the traffic
  * Each SPD entry is defined by a set of IP and upper layer protocol field values, called selectors
  * These selectors are used to filter outgoing traffic in order to map each it into a particular SA.

2

Q.No | Marks

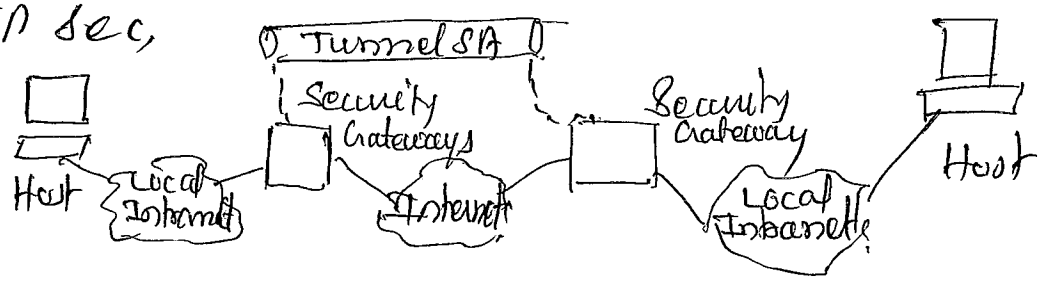
5b) Explain the basic combinations of Security associations | 08

* The IPsec Architecture document lists four examples of combinations of SAs that must be supported by compliant IPsec hosts or security gateways
* These are illustrated in figure shown below
  * The lower part of each case in the figure represents the physical connectivity of the elements; the upper part represents logical connectivity via one or more nested SAs | 2
  * Each SA can be either AH or ESP
  * For host-to-host SAs, the mode may be either transport or tunnel; otherwise it must be tunnel mode

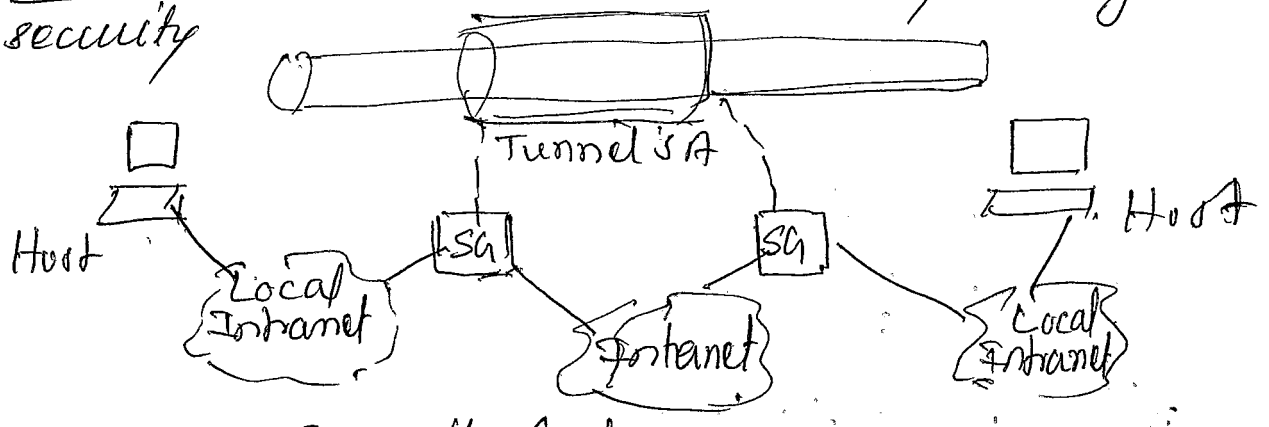


Case 1: All security is provided between end systems that implement IPsec | 2

Case 2: Security is provided between gateways (routers, firewalls, etc) and no hosts implement IPsec,



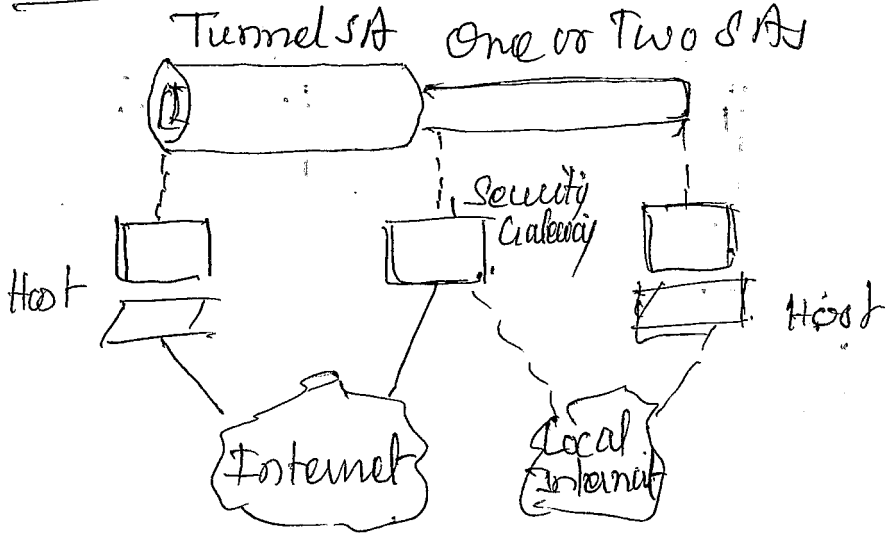
Case 3: This builds on case 2 by adding end-to-end security



SG - Security Gateway

2

Case 4:

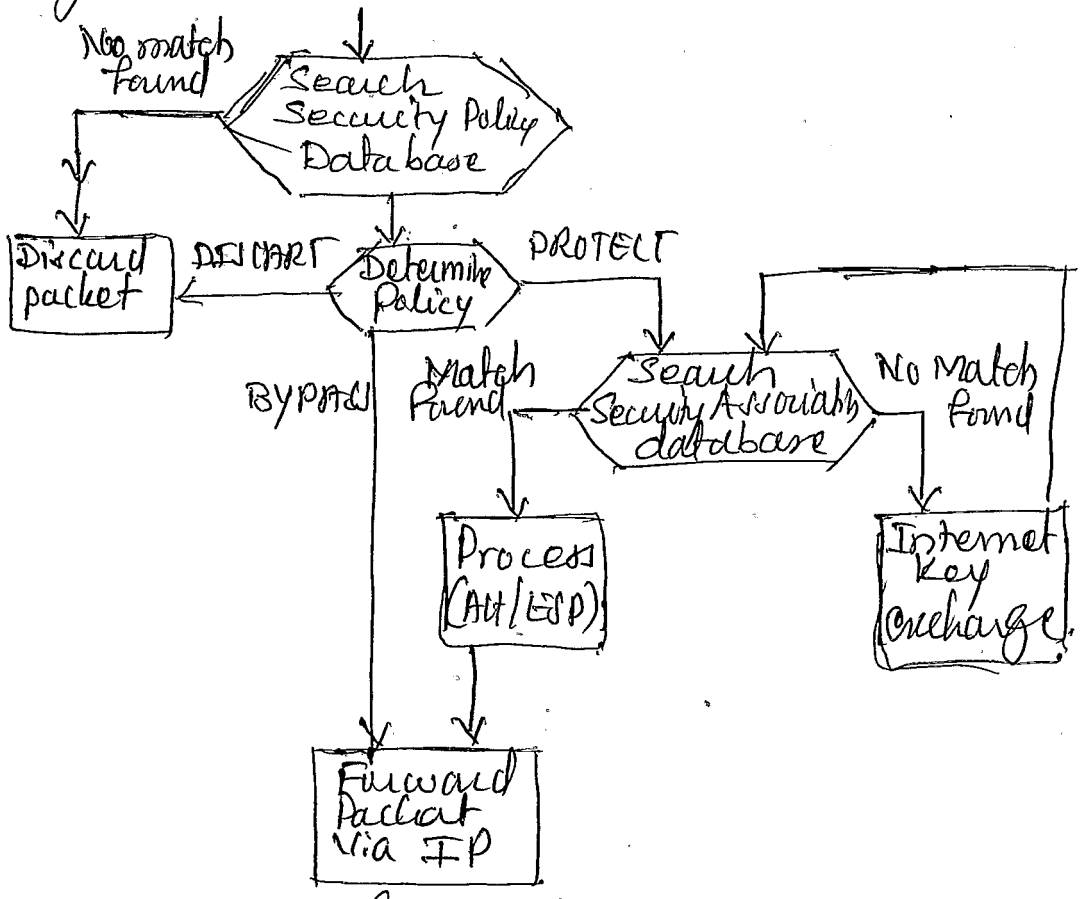


2

* Provides support for a remote host that uses the internet to reach an organization's firewall and gain access to some server or workstation behind the firewall.
* Only tunnel mode is required between the remote host and the firewall.
* As in case 1, one or two SAs may be used between remote host and the ~~firewall~~ local host

Q.No 6 a) Discuss the processing model for outbound packets 08

Figure highlights the main elements of IPsec processing for outbound traffic



4

* A block of data from higher layer, such as TCP, is passed down to the IP layer and an IP packet is formed, consisting of an IP header and an IP body.
* IPsec searches the SPD for a match to this packet
* If no match is found, then the packet is discarded, and an error message is generated.
* If a match is found, further processing is determined by the first matching entry in the SPD.
* If the Policy is PROTECT, then search is made.
* The matching entry in the SPD determines the process of packet.

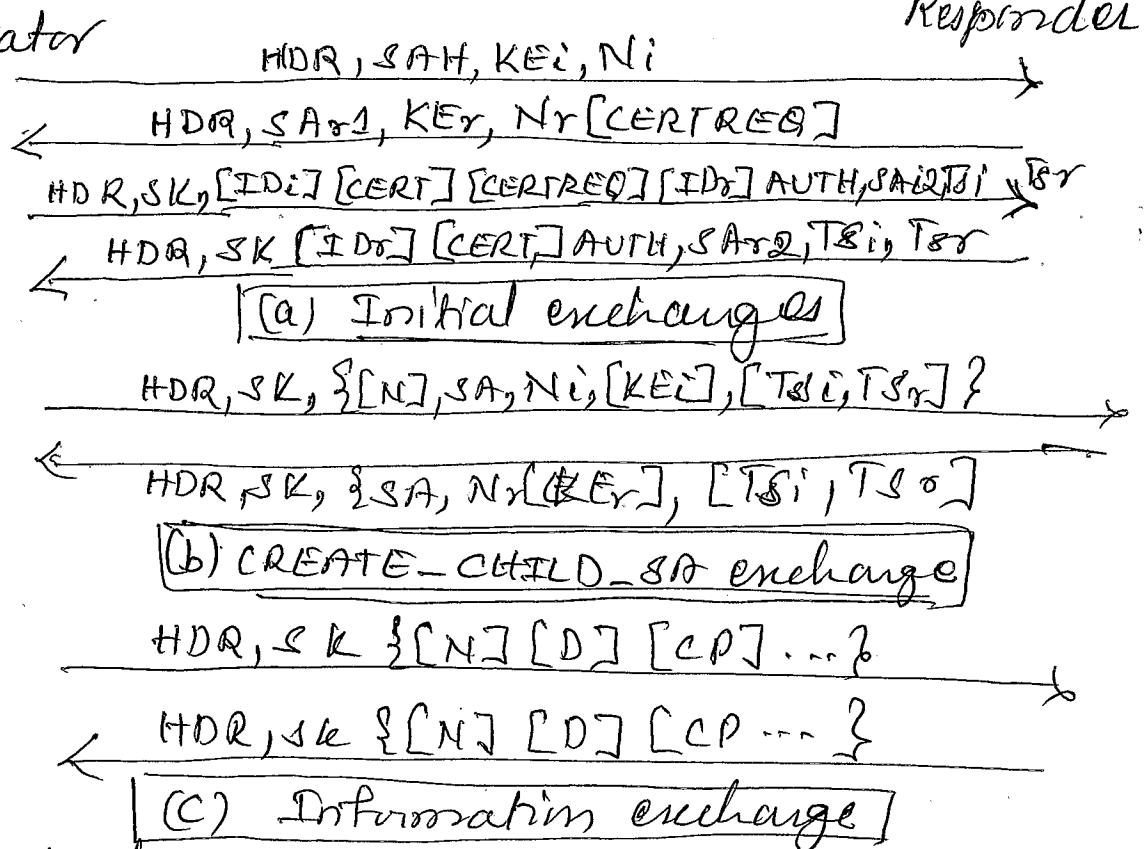
4

Q.No 6 b) Explain IKE V2 exchanges

Marks 08

* IKEv2 protocol includes the exchange of messages in pairs
* The first two pairs of exchanges are referred to as the initial exchanges.
* In the first exchange, the two peers exchange information concerning cryptographic algorithms and other security parameters they are willing to use along with nonces and Diffie-Hellman (DH) values. The result of this exchange is to set up a special SA called the IKE SA. 4
* In the second exchange, the two parties authenticate one another and setup a first IPsec SA.

Figure shows the steps



4

HDR = IKE header
SAx1 = DH algorithm
N = Notify
KEx = DH Pub key
Nx = Nonces
D = Delete
CP = Configuration
IDx = identity
CERT = certificate
SK{...} = MAC & encrypt

Qr No		Marks
7a)	Explain the primal design forces in Cybersecurity domain	08

* The primal forces in the cybersecurity domain include:

* Management of functionality:
  * It drives the other forces
  * Systems are granted accreditation with respect to a defined level of functionality
  * Functionality is tested and certified by the developers prior to security testing

2

* Management of confidentiality
  * Confidentiality is the protection of information on the system
  * Sensitivity of information defines the level of risk and security priority for each system or database element

2

* * Management of Integrity
  * Integrity is protection of the coherence of the data and system metadata. For example — configuration
  * The significant threat of damage to data can be very costly to remediate.
  * Malware can migrate to different parts of a network device through normal and erroneous operations.

2

* Management of availability
  * Availability is the continuous readiness of the system to execute its functionality

(20)

Q.no		Marks
	in response to users and other systems requests and the ability to continually access its data * Availability is an aspect of the more general concept of Quality of Service (QoS) * QoS is a service-level requirement for the system	2
20b	7b) Explain the antipattern for policy-driven security certifications	08
	* The gold standard of professional security certifications is the Certified Information System Security Professional (CISSP) * Paper based qualification requiring a great deal of memorization in 10 diverse security domains such as physical security, communication security and systems security. * CISSP is required by the U.S. Department of Defense (DoD) for both management and technical security workers, and demanded in the job-market * The goal of this certification is to prepare security professionals for effective communication with upper management * This is not useful feature for combating emerging cyber threats * This paradox was addressed by the Center for Strategic and International Studies (CSIS) * It states that such a certification creates dangerously false sense of security.	4 4

Q.No

Marks

8 a) Explain any two Cybersecurity antipattern catalogs

(i) Can't Patch Dumb

Antipattern Name: Can't Patch Dumb

Also known As: Social Engineering, Phishing Spam, Spyware, Driveby Malware, Ransomeware Autoplay attacks

Refactored Solution Names: Security awareness

Unbalanced Primal forces: Confidentiality, Integrity

Anecdotal Evidence: "Technology is not the problem; people are the problem" and "Technology is easy; people are difficult.

05

(ii) Unpatched Applications:

Antipattern Name: Unpatched Applications

Also known as: Vendor-Specific updates
Default configurations

Refactored Solution Name: Patch Management

Unbalanced Primal forces: Management of Integrity

Anecdotal Evidence: Most new attacks are going after the applications, not the operating systems.

05

8b) Explain full cyber antipattern template 06

The full cyber antipattern template has two main parts: a header and a body.

* Header: Gives a gist/sense of the antipattern and solution.
* Body: Contains the pattern details 03

* Header fields
  * Antipattern Name: A unique pejorative noun phrase.
  * Also known as: Analogous names
  * Refactored solution: One or more names for alternative solutions.
  * Unbalanced Primal Forces: Poorly resolved design forces
  * Anecdotal Evidence: Characterizes antipattern

* Body fields
  * Background: Provides useful explanation
  * Antipattern Solution: Defines antipattern solution through diagrams, explanations, examples and discussion of design forces
  * Causes, Symptoms, and Consequences — This bulleted lists the typical causes, common symptoms and resulting consequences of the antipattern solution 02
  * Known Exceptions
  * Refactored Solutions and examples
  * Related solutions: Other potential solutions

Q.No | Marks

9 a) Explain the Zachman Framework for enterprise architecture | 10

* The Zachman Framework, invented by John A. Zachman, is an intellectual tool for describing enterprises
* This framework slices and dices complexity into rows and columns.
* The columns are the six basic questions you could ask about any subject.
  * Includes: What? How? Where? who? When? why? | 5
  * These are the same questions journalists ask to write newspaper stories
  * When a journalist has answered these six questions, he or she can claim to have a complete story
* The Zachman Framework further slices and dices complexity into rows, the rows represent a general overview of the human roles
* The hierarchy of every complex enterprise has : executives, business management, architects engineers, technicians and users. | 5
* Each of these roles can ask the same six questions, hence six cells per row.
* Each row-column intersection, is a cell to be populated with models and specifications which are representations of the enterprise

Q.No | Marks

9b) List the typical re-imaging sequence for the windows OS | 06

* Reimaging sequence for the windows OS

1.) Obtain the installation disks for windows

2) Verify that the system is not connected to the network. Secure the system before allowing it on production networks

3) Power on the machine and open CD/DVD drive. Insert the first windows install disk. Reboot or power down and restart. 1 X 6 = 6

4) Follow the on-screen instructions for installation. It is better to set the Administrator password after Windows boots

5) Insert DVD containing device drivers for the system.

6) The next section continues the installation instructions which includes how to download patches, burn CDs, transfer files, secure the network with antimalware tools and install applications.

3.Nov

Marks

10 a) Explain any two key techniques for ~~enterprise~~ architectural problem Sol pattern ~~architecture~~

(i) Business Question Analysis

Also known As : Classifying the Possibilities by — Zachman column

Problem Solving Type : Convergent Thinking

Process Roles : Task Lead

Content Roles : Principal Architect, Business SME

Communication techniques : Small Group Discussion.

Range of duration : 1 hour to 3 days.

* Background : Answer important questions from Business owners

* Preparation : Document the key questions from business owners

* Procedure : Gather knowledge from enterprises to find out what quests the business management has.

4

(ii) Document Mapping.

Also known as : Document Analysis

Problem Solving Type : Divergent Thinking

Process Roles : Lead, Principal architect

Content roles : The Team

Communication Techniques : Document Inspection

Range of duration : 1 day to 1 month.

4

Mau

* Background: Customer documents
* Preparation: Collect as many customers documents as possible
* Procedure: Moving into enterprise document

10 b) Explain any two host based security technologies 6s

* Host Based Security (HBS) can be implemented with a combination of location protections and services and enterprise services that manage local configurations and services.
  * Antivirus protection scans for malicious files. 2
    * Scan can be on demand, scheduled and continuous
    * Antivirus protection recognizes malware through signatures usually by matching the hash function with known malware database.
  * Anti-Spyware searches for suspicious applications that might be collecting data without the user's knowledge.
    * Spyware applications are often installed covertly 2
    * Both antivirus and anti-spyware programs either quarantine or remove the malicious file
  * Host-Based Firewall : Determines which ports are open or closed. 2

9/11/16

* Patch management:

  * Ensures that the OS and applications have the latest developer-recommended updates
  * Application patching remains a major vulnerability.
  * Microsoft initiated a ritual monthly update called Patch Tuesday.
  * It is the second Tuesday of each month and coincides with patch updates from many vendors.

———— x ————