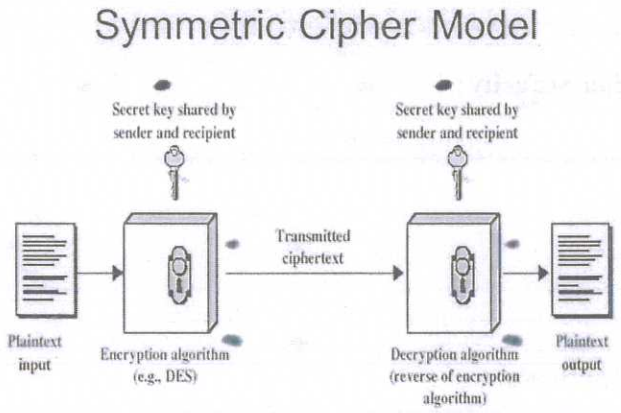
SCHEME OF EVALUATION
Scoring Indicators

Revision: 2015		Course code:5136		
Course Title: Information Security				
Sl No	**Scoring Indicator**	**Split up score**	**Sub Total**	**Total**
	PART A			
I(1)	Data Confidentiality, Privacy	1+1	2	10
I(2)	The process or action of proving or showing something to be true, genuine, or valid.	2	2	
I(3)	A **digital signature** is applied and verified, as follows: The document or message sender (signer) or public/private key supplier shares the public key with the end user(s). The sender, using his private key, appends the encrypted **signature** to the message or document.	2	2	
I(4)	1.Packet filtering firewall 2.Stateful inspection firewall 3.Application proxy firewall 4.Circuit – level gateway	0.5 each	2	
I(5)	A distributed denial-of-service (**DDoS**) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic.	2	2	
	PART B			
II (1)	• **Encryption**: It is the process of locking up information using cryptography. Information that has been locked this way is encrypted. • **Decryption**: The process of unlocking the encrypted information using cryptographic techniques. • **Key**: A secret like a password used to encrypt and decrypt information. There are a few different types of keys used in cryptography. In symmetric encryption same key is used for both encryption and decryption. • **Plain text:** The message to be sent. • **Cipher text:** The scrambled form of messages. • Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that	3	6	

can be used to maintain a private information link.



source: William Stallings

3

\+ 3

42

II (2)

Basic elements of Access control: subject, object and Access right

The basic elements of access control are:

1. subject,
2. object, and
3. access right.

1. Subject: 2

- A subject is an entity capable of accessing objects.
- Any user or application actually gains access to an object by means of a process that represents that user or application.
- Basic access control systems typically define three classes of subject, with different access rights for each class:
  - **Owner**
  - **Group**
  - **World**

\+

2. Object:

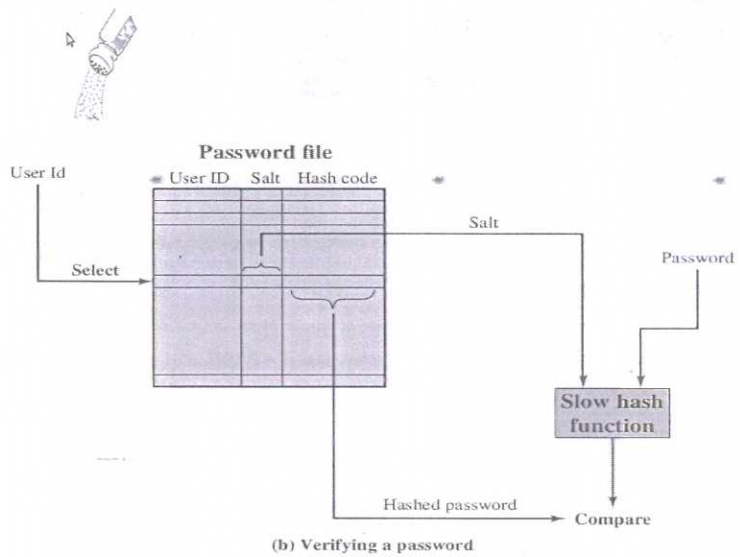
- An object is a resource to which access is controlled.
- An object is an entity used to contain and/or receive information. Examples include records, blocks, pages, segments, files, portions of files, directories, directory trees, mail boxes, messages, and programs. 2

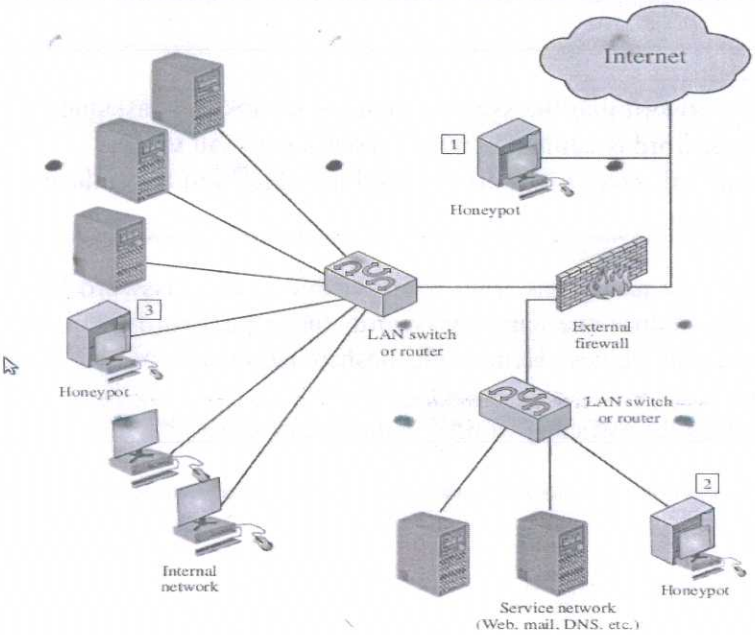
6

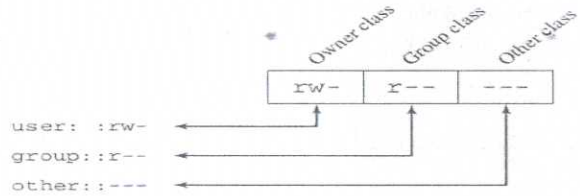
3. Access right:

- An access right describes the way in which a subject may access an object.
- Access rights could include the following:
  - **Read**.
  - **Write**
  - **Execute**
  - **Delete**
  - **Create**
  - **Search**

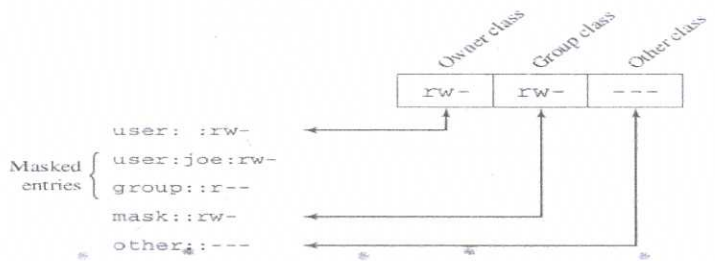
\+ 2

II (3)	**Hashed password:** •To load a new password into the system, the user selects or is assigned a password. This password is combined with a fixed-length salt value •The password and salt serve as inputs to a hashing algorithm to produce a fixed-length hash code. •The salt serves three purposes: ○ It prevents duplicate passwords from being visible in the password file. Even if two users choose the same password, those passwords will be assigned different salt values. Hence, the hashed passwords of the two users will differ. ○ It greatly increases the difficulty of offline dictionary attacks.  (b) Verifying a password	3 + 3	6	
II (4)	**Honeypot** •Decoy systems designed to: ○ lure a potential attacker away from critical systems – collect information about the attacker's activity ○ encourage the attacker to stay on the system long enough for administrators to respond •filled with fabricated information that a legitimate user of the system wouldn't access •resource that has no production value ○ incoming communication is most likely a probe, scan, or attack ○ outbound communication suggests that the system has probably been compromised •once hackers are within the network, administrators can observe their behaviour to figure out defences.	3 +	6	





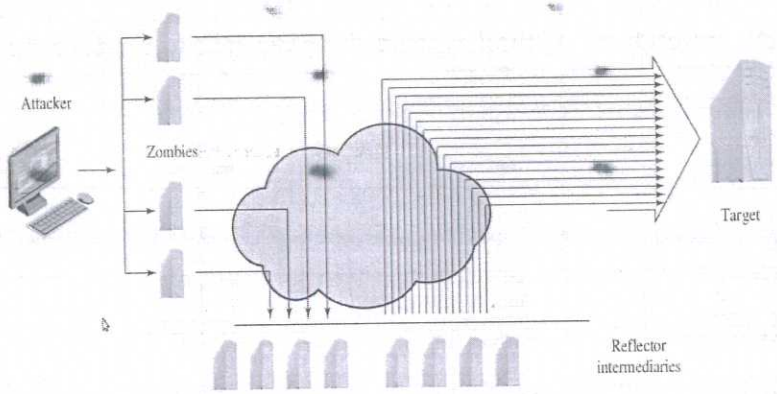
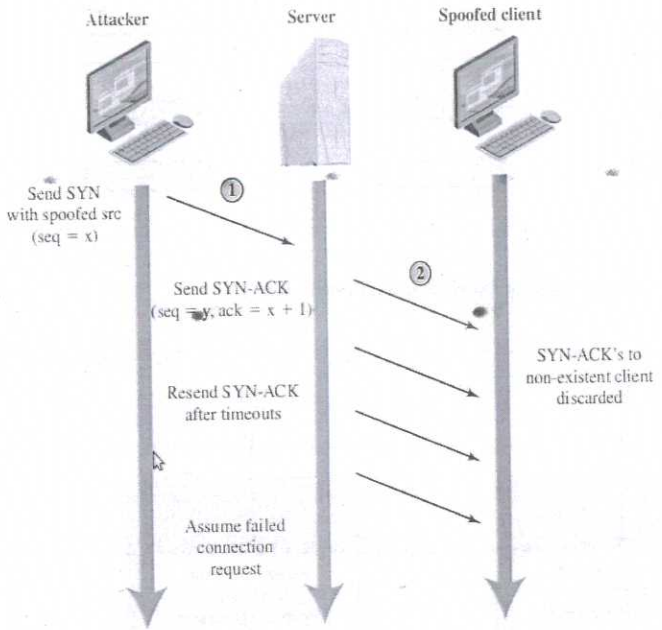
(a) Traditional UNIX approach (minimal access control list)



(b) Extended access control list

Figure 4.6 **UNIX File Access Control**

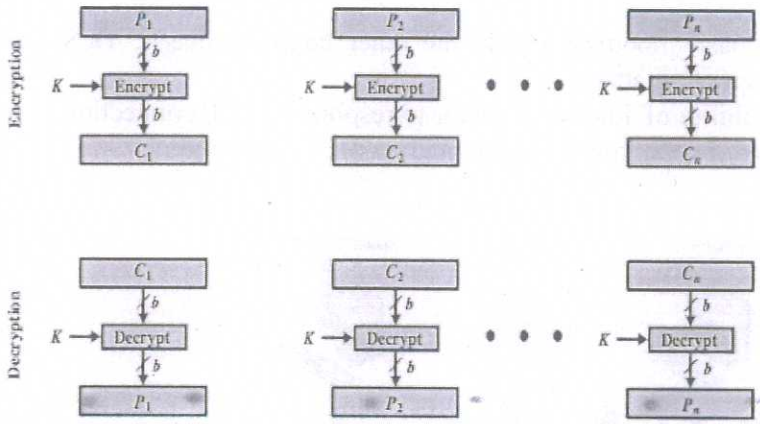
II (5)	**UNI** •All mea •An info •An cont •**Dir** cont •A d t by key e is can **ory.** •E c UNIX user is assigned a unique user identification number **(user ID).** • A user is also a member of a primary group, and possibly a number of other groups, each identified by a **group ID.**	3 3 + 3	6
II (6)	**AMPLIFIER ATTACK** •Amplification attacks are a variant of reflector attacks and also involve sending a packet with a spoofed source address for the target system to intermediaries. •They differ in generating multiple response packets for each original packet sent. This can be achieved by directing the original request to the broadcast address for some network. • As a result, all hosts on that network can potentially respond to the request, generating a flood of responses as shown in Figure • It is only necessary to use a service handled by large numbers of hosts on the intermediate network.	3	

	•A ping flood using ICMP echo request packets was a common choice, since this service is a fundamental component of TCP/IP implementations and was often allowed into networks. • The well-known smurf DoS program used this mechanism and was widely popular for some time. Another possibility is to use a suitable UDP service, such as the echo service. •  Figure 7.7 Amplification Attack	+ 3	6	
II (7)	**Sou** ➢A the spoc...g. ks is lress **SYN Spoofing** ➢Along with the basic flooding attack, the other common classic DoS attack is the SYN spoofing attack. ➢This attacks the ability of a network server to respond to TCP connection requests by overflowing the tables used to manage such connections.  Figure 7.3 TCP SYN Spoofing Attack	3 + 3	6	
	**PART (			
III (a)	**Block (** In block higher) 4 bit or a key is used for each block. Moreover, the encryption key helps to find which mathematical function to use on each block. However, using strong algorithms makes it difficult to find out the mathematical functions used on each block. Therefore, in block cipher, it might be difficult to reverse the encrypted text.	2 +		15

Stream Cipher

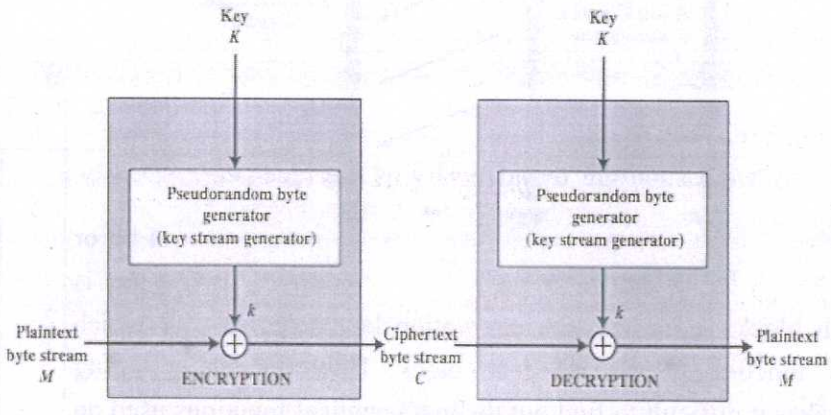
In a stream cipher, the plain text is converted into cipher text by considering one byte at a time. A stream cipher uses a pseudorandom bit generator for encryption and decryption. It is capable of generating a random stream of bits called key stream. Furthermore, the cipher performs an Exclusive OR (XOR) to create the cipher text. In other words, it performs XOR on each bit of the key with the plain text to produce the cipher text.

2 + 8



(a) Block cipher encryption (electronic codebook mode)

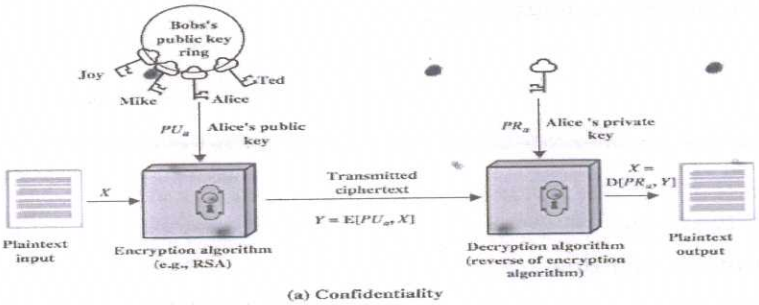
2 + 2



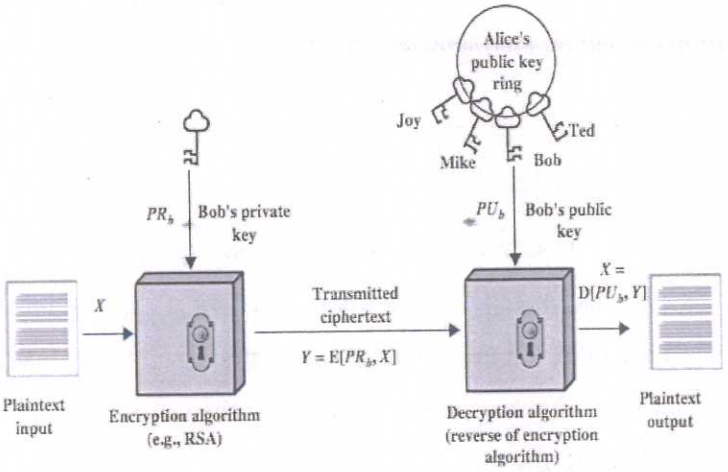
(b) Stream encryption

2

III (b)



(a) Confidentiality



(b) Authentication

4 (Any 1 fig)

7

The most important properties of public key encryption scheme are –

- Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme. +
- Each receiver possesses a unique decryption key, generally referred to as his private key. 3
- Receiver needs to publish an encryption key, referred to as his public key.
- Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver. Generally, this type of cryptosystem involves trusted third party which certifies that a particular public key belongs to a specific person or entity only.
- Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.
- Though private and public keys are related mathematically, it is not

	be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.			
IV (a)	**The OSI architecture focuses on** 1. Security attacks 2. Security services 3. Security mechanisms **Security attack**–Any action that compromises the security of information owned by an organization. **Security mechanism**–A mechanism that is designed to detect, prevent or recover from a security attack. **Security service**–A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service. **1) SECURITY SERVICES** The classification of security services are as follows: **Confidentiality:** Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. Eg., printing, displaying and other forms of disclosure. **Authentication:** Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false. **Integrity:** Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages. **Non repudiation**: Requires that neither the sender nor the receiver of a message be able to deny the transmission. **Access control**: Requires that access to information resources may be	2 + 2	8	15

	controlled by or the target system. **Availability**: Requires that computer system assets be available to authorized parties when needed. **2) SECURITY MECHANISMS** One of the most specific security mechanisms in use is cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security. Some of the mechanisms are: 1. Encipherment 2. Digital Signature 3. Access Control **3) SECURITY ATTACKS** There are four general categories of attack which are listed below. **Interruption** An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability. **Interception** An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, a program or a computer.e.g., wire tapping to capture data in the network, illicit copying of files. **Modification** An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. **Fabrication** An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity.	+ 2 + 2			
IV (b)	**M ESSAGE A UTHENTICATION C ODE** •MAC algorithm is a symmetric key cryptographic technique to provide				

message authentication.

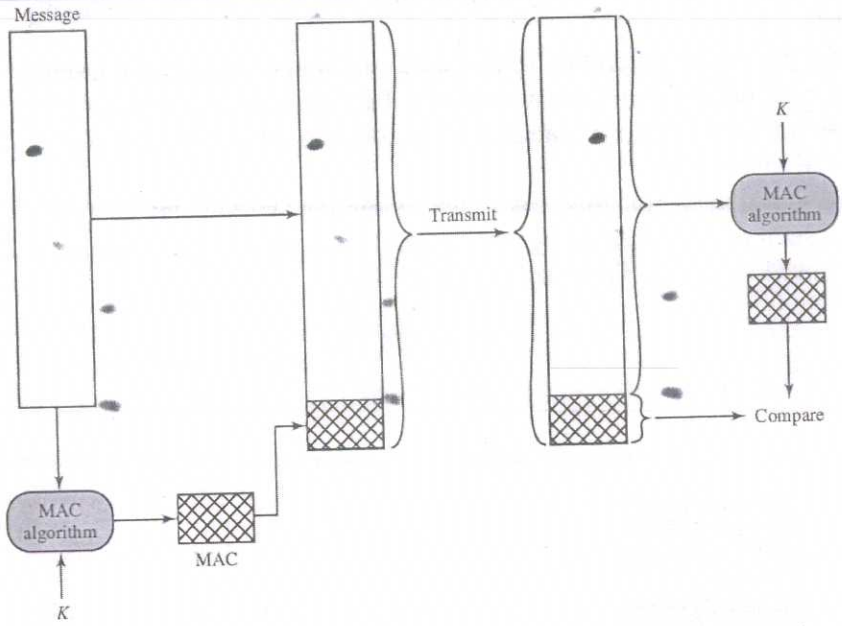
•For establishing MAC process, the sender and receiver share a symmetric key K.

•Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.

•The sender uses some publicly known MAC algorithm, inputs the message and the secret key K and produces a MAC value.

- Similar to hash, MAC function also compresses an arbitrary long input into a fixed length output.
- The major difference between hash and MAC is that MAC uses secret key during the compression.
- The sender forwards the message along with the MAC. Here, we assume that the message is sent in the clear, as we are concerned of providing message origin authentication, not confidentiality.
- If confidentiality is required then the message needs encryption.
- On receipt of the message and the MAC, the receiver feeds the received message and the shared secret key K into the MAC algorithm and re-computes the MAC value.
- The receiver now checks equality of freshly computed MAC with the MAC received from the sender. If they match, then the receiver accepts the message and assures himself that the message has been sent by the intended sender.
- If the computed MAC does not match the MAC sent by the sender, the receiver cannot determine whether it is the message that has been altered or it is the origin that has been falsified.
- As a bottom-line, a receiver safely assumes that the message is not the genuine.

4 + 7



3

Fig:Message Authentication Using a Message Authentication Code

V (a) Token based authentication

•Objects that a user possesses for the purpose of user authentication are called tokens.

•Two types of tokens that are widely used; these are cards that have the appearance and size of bank cards. 2

Table 3.3 Types of Cards Used as Tokens

Card Type	Defining Feature	Example
Embossed	Raised characters only, on front	Old credit card
Magnetic stripe	Magnetic bar on back, characters on front	Bank card
Memory	Electronic memory inside	Prepaid phone card
Smart Contact Contactless	Electronic memory and processor inside Electrical contacts exposed on surface Radio antenna embedded inside	Biometric ID card

\+ 8 = 15

Smart Cards 3

•A wide variety of devices qualify as smart tokens.

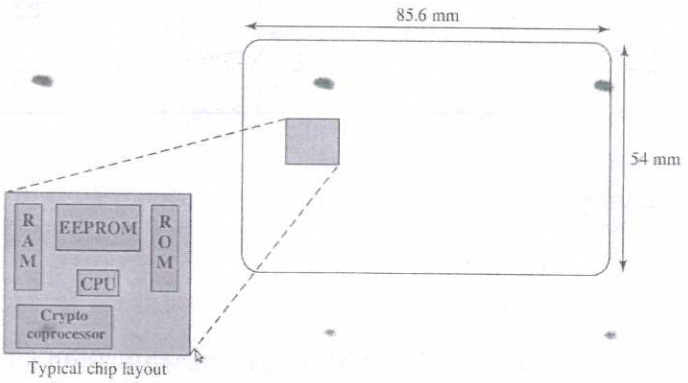
•These can be categorized along three dimensions that are not mutually exclusive:

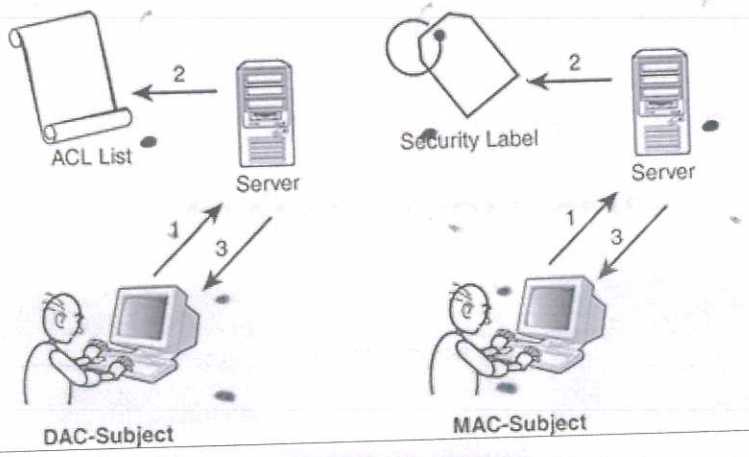
◦ Physical characteristics: Smart tokens include an embedded microprocessor. A smart token that looks like a bank card is called a smart card. Other smart tokens can look like calculators, keys, or other small portable objects.

◦ Interface: Manual interfaces include a keypad and display for human/token interaction. Smart tokens with an electronic interface communicate with a compatible reader/writer.

◦ Authentication protocol: The purpose of a smart token is to provide a means for user authentication. We can classify the authentication protocols used with smart tokens into three categories:

▪ Static: With a static protocol, the user authenticates himself or herself to

	the token and then the token authenticates the user to the computer. (password) ▪ Dynamic password generator: In this case, the token generates a unique password periodically (e.g., every minute). This password is then entered into the computer system for authentication, either manually by the user or electronically via the token. (eg otp) ▪ Challenge-response: In this case, the computer system generates a challenge, such as a random string of numbers. The smart token generates a response based on the challenge. (eg CAPTCHA)  Figure 3.3 **Smart Card Dimensions** The smart card chip is embedded into the plastic card and is not visible. The dimensions conform to ISO standard 7816-2.	+ 3		
V (b)	**Pas** •Us pri wo •Tc pas •Us ted t it ds. t a •Computer-generated passwords •Reactive password checking •Proactive password checking **1. User education** Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords. **2. Computer-generated passwords** Computer-generated passwords also have problems. If the passwords are quite random in nature, users will not be able to remember them. **3. Reactive password checking** A reactive password checking strategy is one in which the system periodically runs its own password cracker to find guessable passwords. **4. proactive password checking** A promising approach to improved password security is a proactive password checker.	1 + 1.5 each	7	
VI (a)	**Mandatory access control (MAC):** Controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources). This policy is termed mandatory because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource. Any Figure related to this concept	4 + 4	8	15



VI (b)

OBJECTS

SUBJECTS	File 1	File 2	File 3	File 4
User A	Own Read Write		Own Read Write	
User B	Read	Own Read Write	Write	Read
User C	Read Write	Read		Own Read Write

(a) Access matrix

3

Access Control Matrix or **Access Matrix** is an abstract, formal security model of protection state in computer systems, that characterizes the rights of each subject with respect to every object in the system. +

•An access matrix can be envisioned as a rectangular array of cells, with one row per subject and one column per object. The entry in a cell – that is, the entry for a particular subject-object pair – indicates the access mode that the subject is permitted to exercise on the object. Each column is equivalent to an access control list for the object; and each row is equivalent to an *access profile* for the subject. 4

7

VII (a)

Intrusion Detection

•Detection is concerned with learning of an attack, either before or after its success. 1

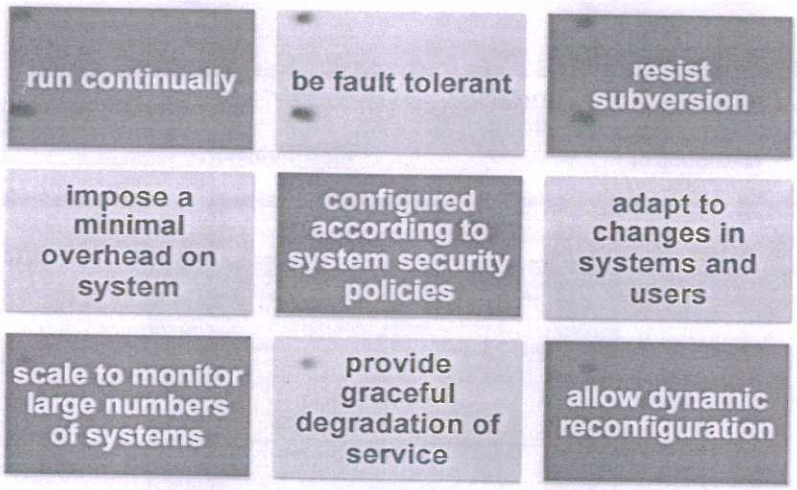
•The first one, **anomaly detection**, explores issues in intrusion +

•detection associated with deviations from normal system or user behavior. The second employs **signature detection** to discriminate between anomaly or attack patterns (signatures) and known intrusion detection signatures. Both methods have their distinct advantages and disadvantages as well as suitable application areas of intrusion detection. 2 +

•When considering the area being the source of data used for intrusion detection, another classification of intrusion detection systems can be used in terms of the type of the protected system. There is a family of IDS tools that use information derived from **a single host (system)** - host based IDS

9

15

	(**HIDS**) and those IDSs that exploit information obtained from a whole segment of **a local network** (network based IDS, i.e. **NIDS**).  	3 + 3		
VII (b)	**SNORT** • lightweight IDS –real-time packet capture and rule analysis – easily deployed on nodes – uses small amount of memory and processor time – easily configured Snort Architecture A Snort installation consists of four logical components (Figure 8.9): • **Packet decoder:** The packet decoder processes each captured packet to identify and isolate protocol headers at the data link, network, transport, and application layers. The decoder is designed to be as efficient as possible and its primary work consists of setting pointers so that the various protocol headers can be easily extracted. • **Detection engine:** The detection engine does the actual work of intrusion detection. This module analyzes each packet based on a set of rules defined for this configuration of Snort by the security administrator. •**Logger**: For each packet that matches a rule, the rule specifies what logging and alerting options are to be taken. •**Alerter:** For each detected packet, an alert can be sent. The alert option in the matching rule determines what information is included in the event notification. •A Snort implementation can be configured as a passive sensor, which monitors traffic but is not in the main transmission path of the traffic, or an inline sensor, through which all packet traffic must pass.	1 + 2	6	

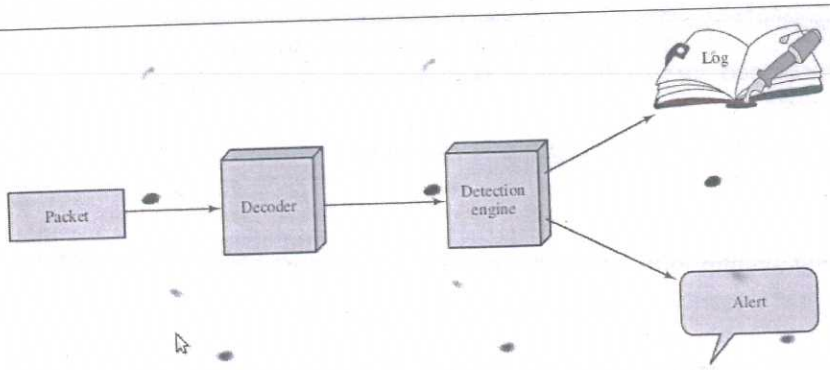
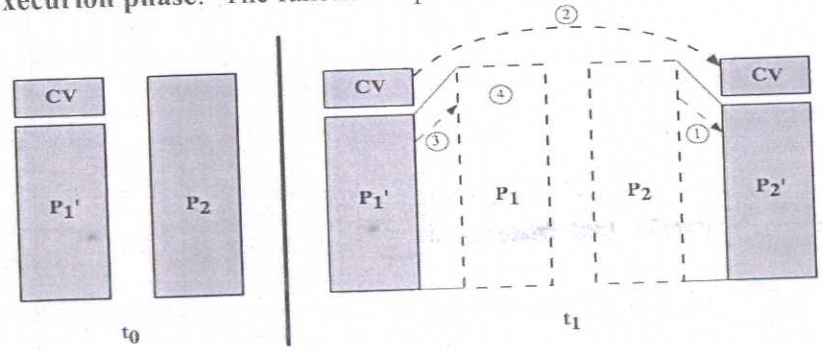


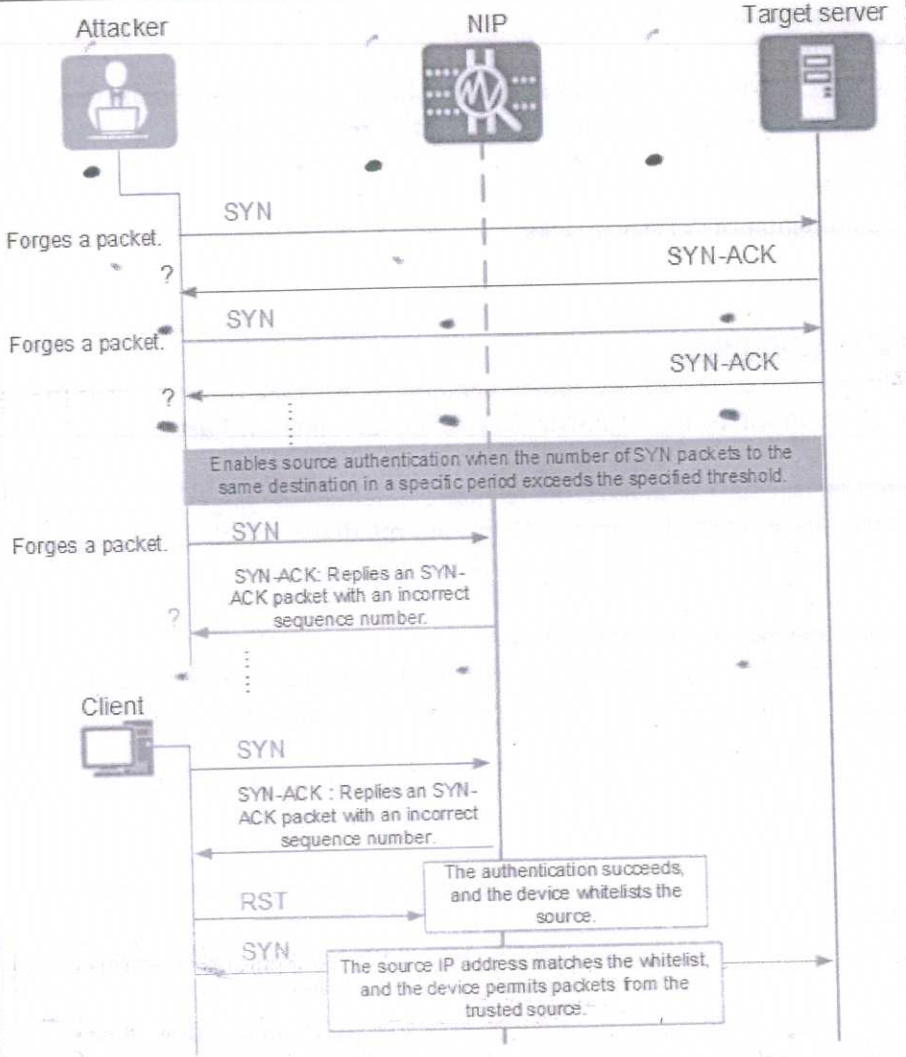
Figure 8.9 Snort Architecture

VII I (a)	**V N** •piece of software that infects programs •modifying them to include a copy of the virus •so it executes secretly when host program is run ○ specific to operating system and hardware •taking advantage of their details and weaknesses •a typical virus goes through phases of: ○ dormant ○ propagation ○ triggering ○ execution **Virus Structure:** •components: ○ infection mechanism - enables replication ○ trigger - event that makes payload activate ○ payload - what it does, malicious or benign •prepended / postpended / embedded •when infected program invoked, executes virus code then original program code •can block initial infection (difficult) •or propogation (with access controls) •**Phases of virus:** ○ **Dormant phase:** -virus is idle ○ **Propagation phase:** The virus places copy of itself into other programs or into certain system areas on the disk. ○ **Triggering phase:** - This virus is activated to perform the function for which it was intended. ○ **Execurion phase**:- The function is performed.	+ 3 2 + 2	6	15



	•When this program is invoked control passes to its virus, which performs the following steps: •For each uninfecte file P2 that is found, the virus first compresses that file to produce P2' which is shorter than the original programby the size of the virus.	+ 2	

	•A copy of the virus is prepended to the compressed program. •The compresseed virus version of the original infected program P1' is uncompressed. •The uncompressed original program is executed.			
VII I(b)	**Rootkit** A rootkit is a set of programs installed on a system to maintain covert access to that system with administrator (or root) 3 privileges, while hiding evidence of its presence to the greatest extent possible. A rootkit can be **classified** using the following characteristics: •Persistent •Memory based • User mode •Kernel mode •Virtual machine based •External mode Explanation each	3 + 6	9	
IX (a)	A **SYN** flood (half-open attack) is a type of denial-of-service (**DDoS**) attack which aims to make a server unavailable to legitimate traffic by consuming all available server resources. By repeatedly sending initial connection request (**SYN**) packets, the attacker is able to overwhelm all available ports on a targeted server machine, causing the targeted device to respond to legitimate traffic sluggishly or not at all. Packet injection (also known as forging packets or spoofing packets) in computer networking, is the process of interfering with an established network connection by means of constructing packets to appear as if they are part of the normal communication stream. The packet injection process allows an unknown third party to disrupt or intercept packets from the consenting parties that are communicating, which can lead to degradation or blockage of users' ability to utilize certain network services or protocols. Packet injection is commonly used in man-in-the-middle attacks and denial-of-service attacks.	4 + 3	7	15



IX (b)

FLOODING ATTACKS

•Flooding attacks take a variety of forms, based on which network protocol is being used to implement the attack.

•In all cases the intent is generally to overload the network capacity on some link to a server. 2

•Common flooding attacks use any of the ICMP, UDP, or TCP SYN packet types.

•ICMP Flood

◦The ping flood using ICMP echo request packets is a classic example of an ICMP flooding attack. +

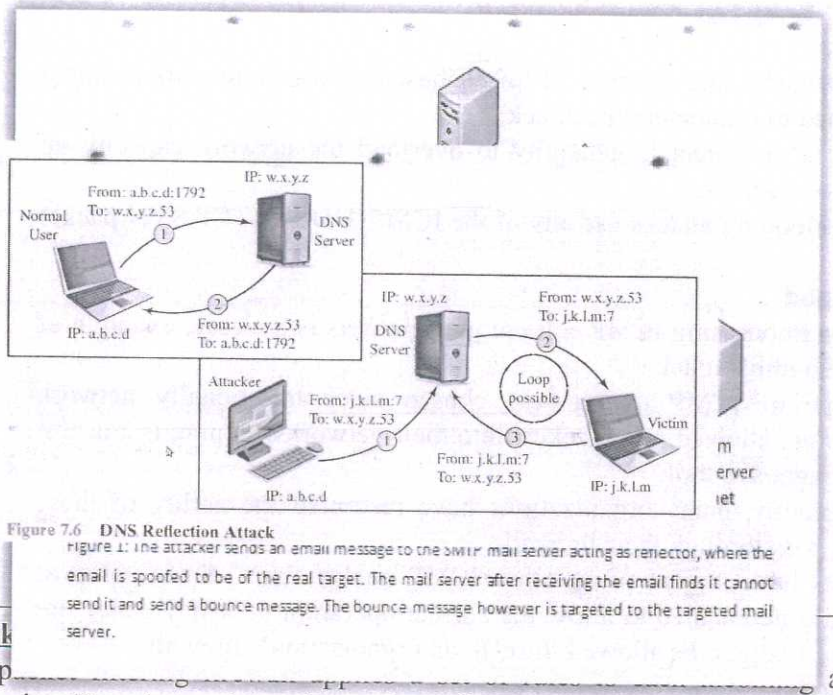
◦This type of ICMP packet was chosen since traditionally network administrators allowed such packets into their networks, as ping is a useful network diagnostic tool. 2

◦More recently, many organizations have restricted the ability of these packets to pass through their firewalls.

◦Attackers have started using other ICMP packet types. Since some of these should be handled to allow the correct operation of TCP/IP, they are much more likely to be allowed through an organization's firewall.

•UDP Flood

◦to use UDP packets directed to some port number, and hence potential +

	service, on the target system. •**TCP SYN Flood** ○ to send TCP packets to the target system. Most likely these would be normal TCP connection requests, with either real or spoofed source addresses. ○ Indirect attack types that utilize multiple systems include ▪ Distributed denial-of-service attacks ▪ Reflector attacks ▪ Amplifier attacks	2 + 2	8	
X (a)	**REFLECTOR ATTACK** •The reflection attack is a direct implementation of this type of attack. The attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system. •When the intermediary responds, the response is sent to the target. •Effectively this reflects the attack off the intermediary, which is termed the reflector, and is why this is called a reflection attack. •Ideally the attacker would like to use a service that created a larger response packet than the original request. •This allows the attacker to convert a lower volume stream of packets from the originating system into a higher volume of packet data from the intermediary directed at the target. •Common UDP services are often used for this purpose. Originally the echo service was a favored choice, although it does not create a larger response packet. • However, any generally accessible UDP service could be used for this type of attack. •Another variant of reflection attack uses TCP SYN packets and exploits the •normal three-way handshake used to establish a TCP connection. The attacker sends a number of SYN packets with spoofed source addresses to the chosen intermediaries.  Figure 7.6 **DNS Reflection Attack** Figure 1: The attacker sends an email message to the SMTP mail server acting as reflector, where the email is spoofed to be of the real target. The mail server after receiving the email finds it cannot send it and send a bounce message. The bounce message however is targeted to the targeted mail server.	+ 4 (an y one fig)	8	15
X (b)	**Pack** •A p… and outgoing IP packet and then forwards or discards the packet .	4	7	

•The firewall is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet:

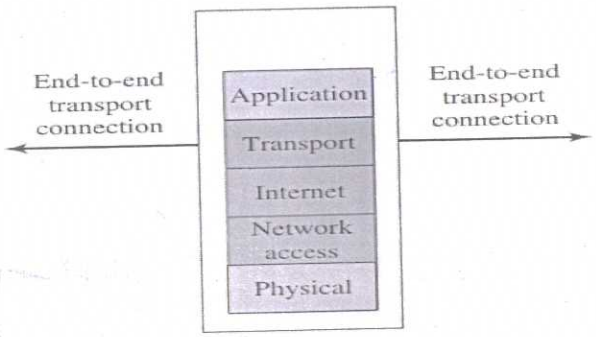
- **Source IP address:** The IP address of the system that originated the IP packet (e.g., 192.178.1.1)
- **Destination IP address:** The IP address of the system the IP packet is trying to reach (e.g., 192.168.1.2)
- **Source and destination transport-level address:** The transport-level (e.g., TCP or UDP) 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 is destined for

The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.

Two default policies are possible:

• Default ϭ discard: That which is not expressly permitted is prohibited.

• Default ϭ forward: That which is not expressly prohibited is permitted.



(b) Packet filtering firewall

only 10 papers found in master copy
wrong page numbers total