IT5205 Information Systems Security

1. Introduction to Information System Security
2. Crypto systems
3. Key Management
4. **Network Security**
5. The Internet Security
6. Information Assurance

Lesson **4** and **5** cover avg. **30**% of paper.

4.1. Introduction to network security
4.2. Threats for networks
4.2. Network Security Protocols
4.3. Intruder Detection and Prevention

4.1. Introduction to network security

4.2. Threats for networks

- Denial-of-service
- Phishing and spear phishing attack
- Man-in-the-middle attack
- Drive-by attack
- Password attack
- SQL injection attack
- Cross-site scripting (XSS) attack
- Eavesdropping attack
- Birthday attack
- Malicious Code attacks

4.3. Network Security Protocols

- IP security (IPSec)
- VPN
- Kerberos
- TLS (previously SSL)
- SSH
- Wireless security

4.4. Intruder Detection and Prevention

- Preventing Malware Attacks
- Fire walls
- IDS
- HSM

4.1. Introduction to Network Security

As you have already known, network system, compared with standalone one, it is very crucial to consider security. Why? Network system has more and more security vulnerabilities due to sort of reasons like follows:

- Insure network (communication) channel
- Unknown users

Types of Threats

Threats related with networks can be classified in to two types.

Internal Threats

Network security threats originating inside a network is known as internal threats. They tend to be more serious than external threats. Here are some reasons for the severity of internal threats:

- Inside users already have knowledge of the network and its available resources.
- Inside users typically have some level of access granted to them because of the nature of their job.
- Traditional network security mechanisms such as Intrusion Prevention Systems (IPS) and firewalls are ineffective against much of the network misuse originating internally.

External Threats

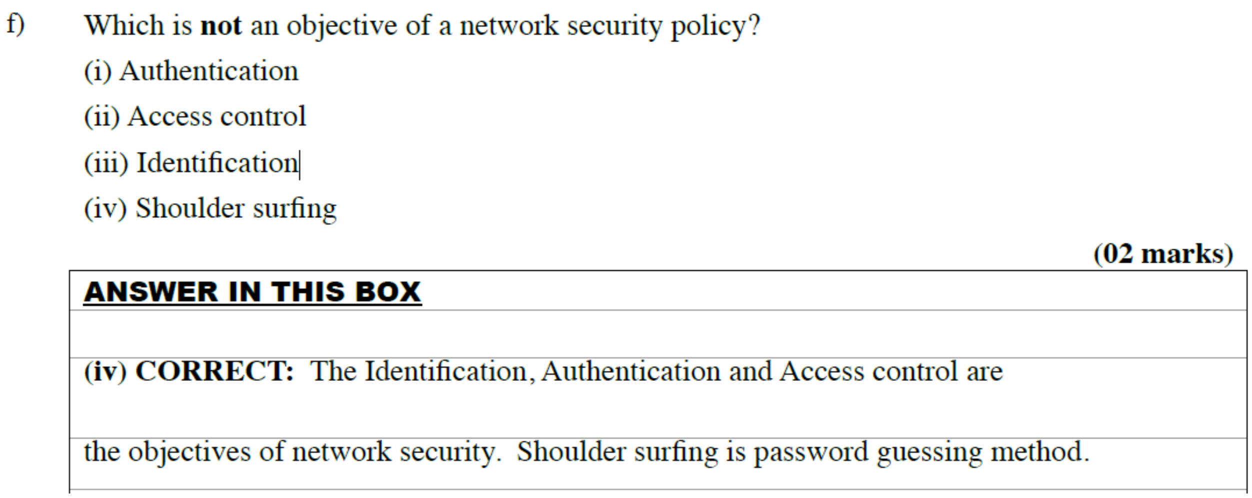
Network security threats originating outside from a network is known as external threats. Because external attackers probably do not have intimate knowledge of a network, and because they do not already possess access credentials, their attacks tend to be more technical in nature.

The Three Primary Goals of Network Security

corporate networks require network security, consider the following goals of network security:

- **Confidentiality**: implies keeping data private.
- **Integrity**: ensures that data has not been modified in transit.
- **Availability**: measure of the data’s accessibility
- **Authentication** and **Identification**: check legitimate users
- **Authorization:** determining privileges and access control

2019-2(f)



f) Which is **not** an objective of a network security policy?

(i) Authentication

(ii) Access control

(iii) Identification

(iv) Shoulder surfing

(02 marks)

ANSWER IN THIS BOX

(iv) CORRECT: The Identification, Authentication and Access control are the objectives of network security. Shoulder surfing is password guessing method.

4.2. Threats for networks

1. **Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks**

   A denial-of-service attack overwhelms a system's resources so that it cannot respond to service requests. If attacker use single computer to that, then it is known as Dos where as attacker use several networked systems to da that, it is known as DDoS attack.

2. **Phishing and spear phishing attack**

   Phishing attack is the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information.

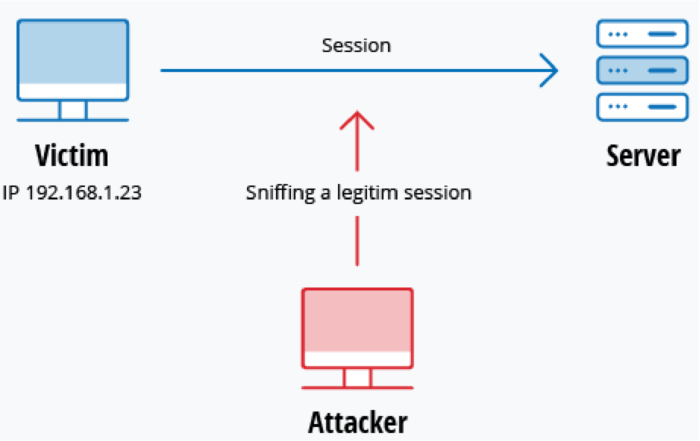
3. **Man-in-the-middle attack**

   This type of attack occurs when a hacker inserts itself between the communications of a client and a server.

   Session hijacking: attacker hijacks a session between a trusted client and network server.

   IP Spoofing: this is used by an attacker to convince a system that it is communicating with a known, trusted entity and provide the attacker with access to the system.

   Replay attack: occurs when an attacker intercepts and saves old messages and then tries to send them later, impersonating one of the participants. Timestamps can be applied to overcome this type.



4. **Drive-by attack**

Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages.

5. **Password attack**

Steal or guess someone else password by using social engineering, gaining access to a password database or outright guessing. Guessing can be done using two techniques.

Brute-force attack: password guessing using a random approach by trying different passwords and hoping that one of them may match

Dictionary attack: a dictionary of common passwords is used to attempt to gain access to a user's computer and network

6. **SQL injection attack**

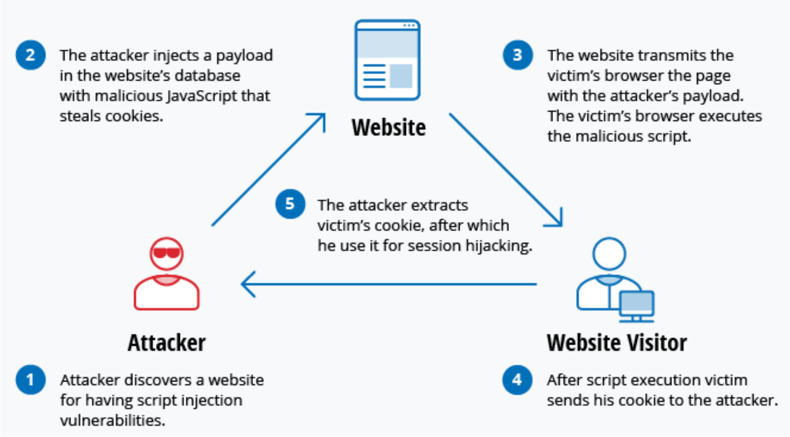
This is common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the database via the input data from the client to server.

*SELECT * FROM users WHERE account = '' or '1' = '1';"*

Because '1' = '1' always evaluates to TRUE, the database will return the data for all users instead of just a single user

7. **Cross-site scripting (XSS) attack**

This sort of attack uses third-party web resources to run scripts in the user's web browser or scriptable application.


2 The attacker injects a payload in the website's database with malicious JavaScript that steals cookies.
Website
3 The website transmits the victim's browser the page with the attacker's payload. The victim's browser executes the malicious script.
5 The attacker extracts victim's cookie, after which he use it for session hijacking.
Attacker
Website Visitor
1 Attacker discovers a website for having script injection vulnerabilities.
4 After script execution victim sends his cookie to the attacker.

8. Eavesdropping attack (Snooping or Sniffing attack)

Is a theft of information as it is transmitted over a network by a computer, smartphone, or another connected device.

9. Birthday attack

This attack can be used to abuse communication between two or more parties. They exploit the mathematics behind the birthday problem in probability theory. Simply it has a relation with message digest (MD).

10. Malicious Code attacks

- **Virus**

  Malicious program and can be replicated itself. Most of the cases, they attaches itself to a program files without the knowledge of the user.

  - **Macro viruses:** This type of viruses infect applications such as Microsoft Word or Excel. Macro viruses attach to an application's initialization sequence.
  - **File infector viruses**: usually attach themselves to executable code, such as .exe files.
  - **System or boot-record infector virus**: attaches to the master boot record on hard disks.
  - **Polymorphic viruses** — These viruses conceal themselves through varying cycles of encryption and decryption.

- **Droppers**: A dropper is a program used to install viruses on computers. Most if the cases dropper is not infected with malicious code and, therefore might not be detected by virus-scanning software.

- **Robots** (**Bots** or **Zombie**)

  Bots are kind of malicious programs which they can be controlled remotely to perform tasks without the knowledge of computer owners. Virus can be used to install bots program in to computer.

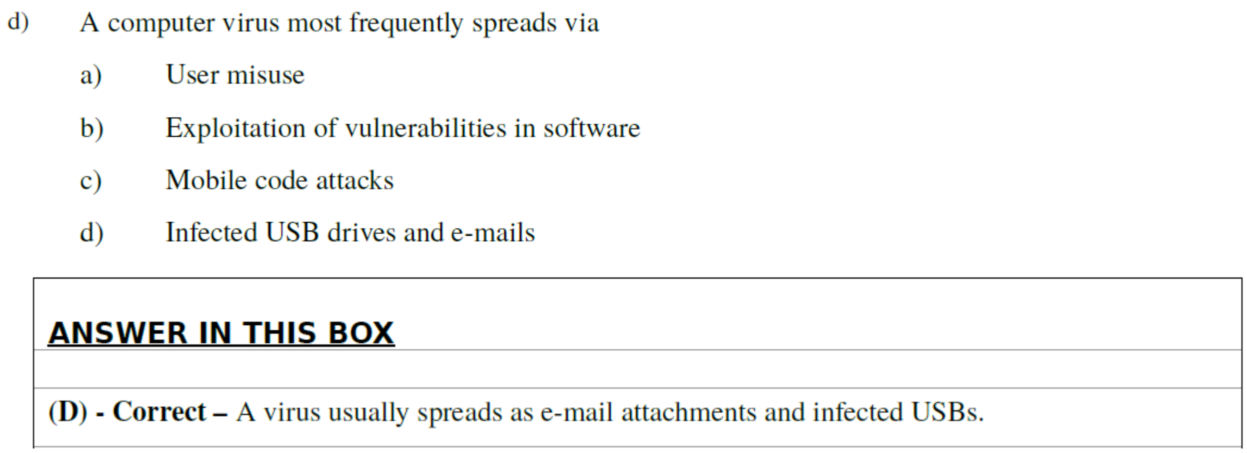
- **Worms**: self-contained programs that propagate across networks and computers. They do not attach to a host file

- **Trojan horse**: a program that hides in a useful program and usually has a malicious function. Trojans do not self-replicate.

- **Ransomware:** user's data will be encrypted and threatens to publish or delete it unless a ransom is paid

- **Logic bombs**: is a type of malicious software that is appended to an application and is triggered by a specific occurrence, such as a logical condition or a specific date and time.

2017-2(d)



d) A computer virus most frequently spreads via

a) User misuse

b) Exploitation of vulnerabilities in software

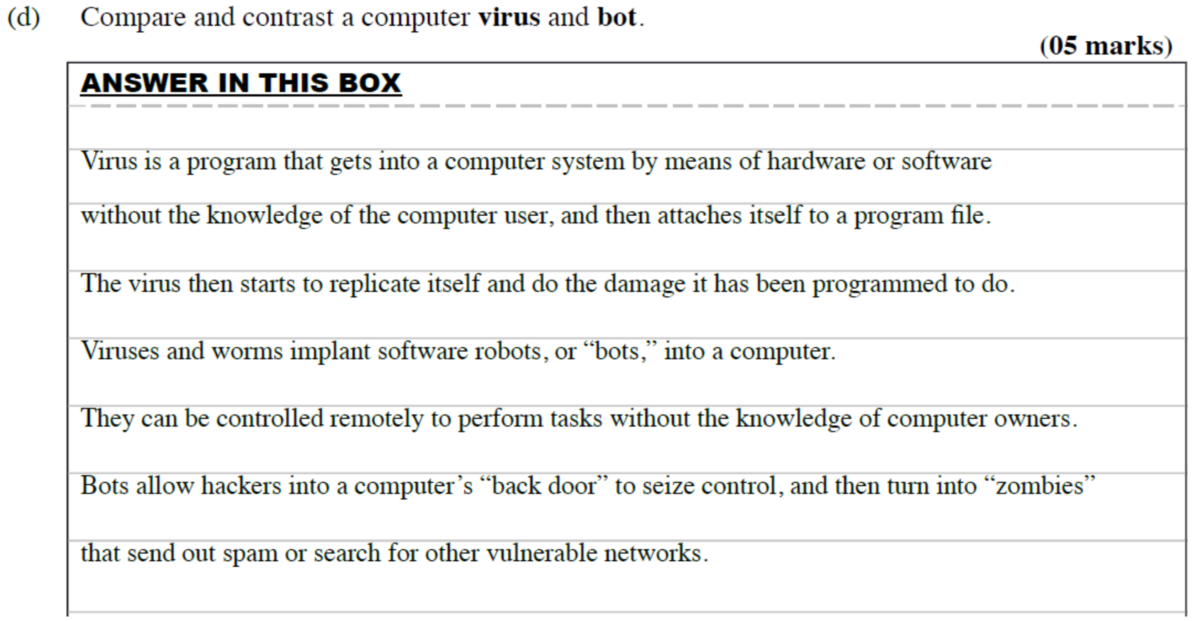
c) Mobile code attacks

d) Infected USB drives and e-mails

ANSWER IN THIS BOX

(D) - Correct – A virus usually spreads as e-mail attachments and infected USBs.

2018-3(d)



(d) Compare and contrast a computer **virus** and **bot**.

(05 marks)

ANSWER IN THIS BOX

Virus is a program that gets into a computer system by means of hardware or software without the knowledge of the computer user, and then attaches itself to a program file.

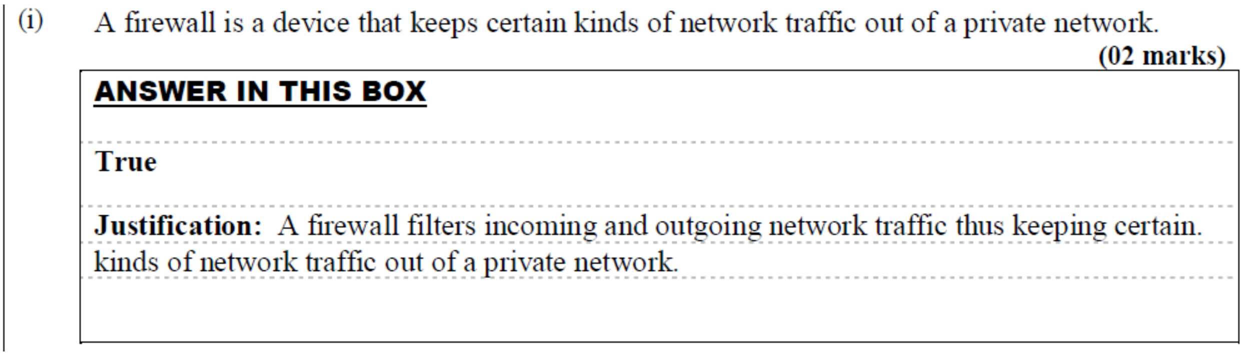
The virus then starts to replicate itself and do the damage it has been programmed to do.

Viruses and worms implant software robots, or "bots," into a computer.

They can be controlled remotely to perform tasks without the knowledge of computer owners.

Bots allow hackers into a computer's "back door" to seize control, and then turn into "zombies" that send out spam or search for other vulnerable networks.

2012-1(i)



(i) A firewall is a device that keeps certain kinds of network traffic out of a private network.

(02 marks)

ANSWER IN THIS BOX

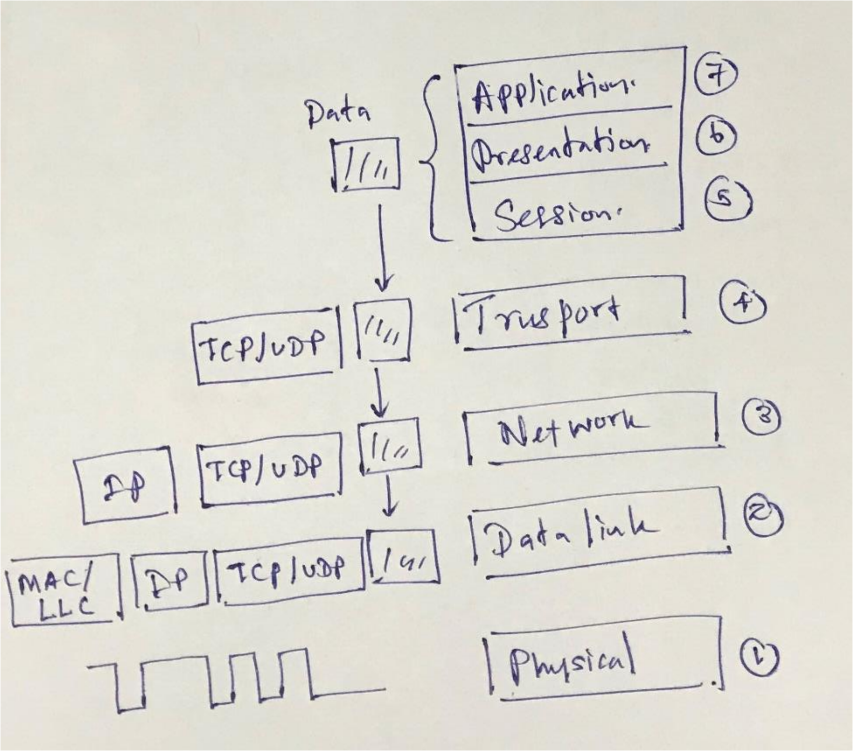
True

Justification: A firewall filters incoming and outgoing network traffic thus keeping certain kinds of network traffic out of a private network.

4.3. Network Security Protocols

IP Security

Before we jump in to IP security, let’s see how data passed ISO OSI model in simple.



Now you can realize that IPSec works with in IP protocol hence it is dealing with routers and layer 3 switches.

- IPSec can assure that a router or neighbor advertisement comes from an authorized router
- And a redirect message comes from the router to which the initial packet was sent (sender can be verified)
- A routing updates are coming from authorized routers

Advantages of IPSec

- Provide security for individual users
- Transparent to applications (below transport layer TCP, UDP)

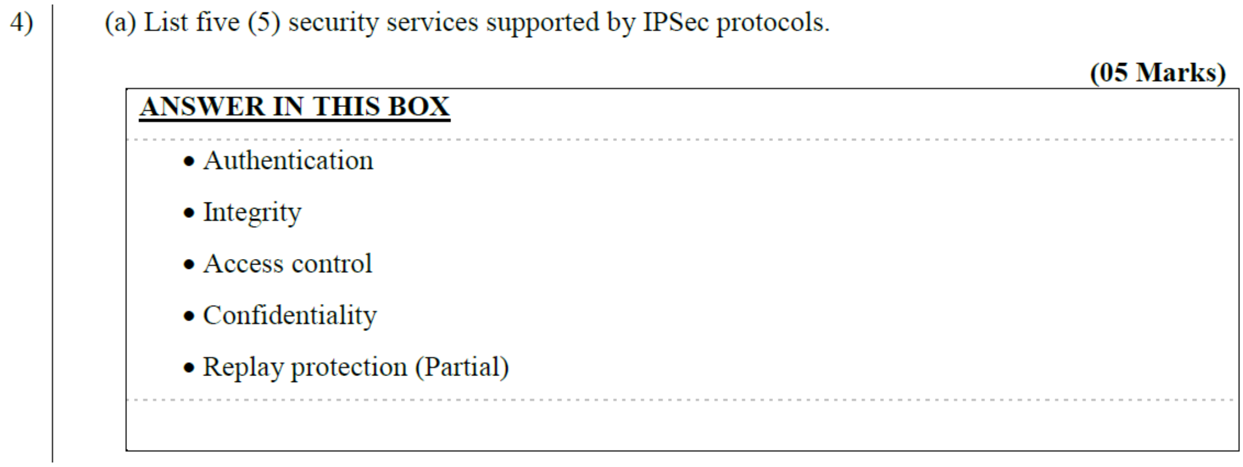
Disadvantages of IPSec

- Can be configured insecurely
- Client security is not assured
- Too complicated which means many different ways to configure
- Cannot provide document level security
- Data storage is not secure

Security services provided by IPSec

- Authentication
- Integrity
- Access control
- Confidentiality
- Replay protection (Partial)

2014-4(a)



4) (a) List five (5) security services supported by IPSec protocols.

(05 Marks)

ANSWER IN THIS BOX

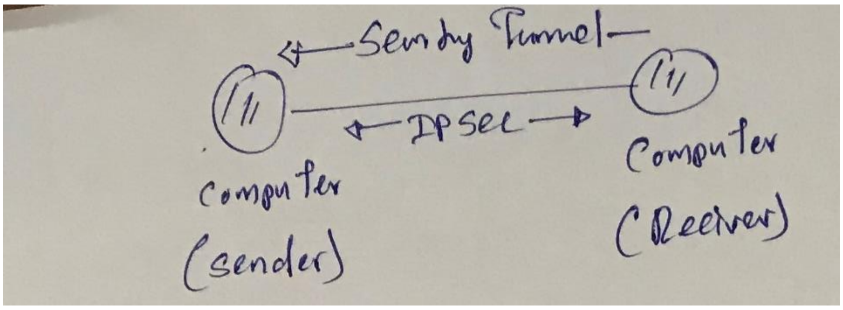
- Authentication
- Integrity
- Access control
- Confidentiality
- Replay protection (Partial)

Communication types of IPSec

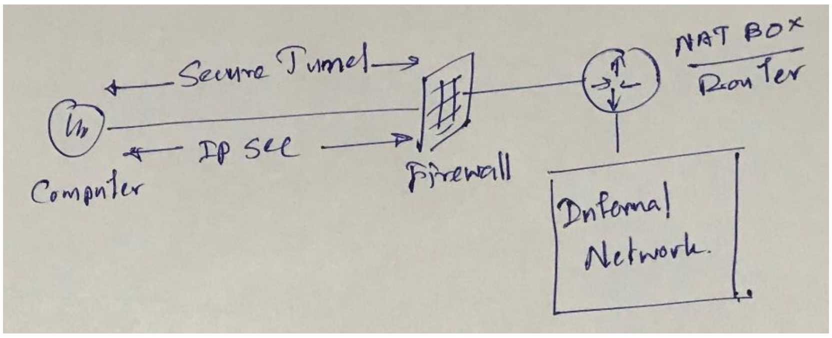
Mainly, three communication modes can be identified as follows.

1. Host to Host (Computer to Computer)
2. Host to Security Gateway (Computer to Firewall, Router or Network)
3. Security Gateway to Security Gateway (Firewall, Router or Network to Firewall, Router or Network)

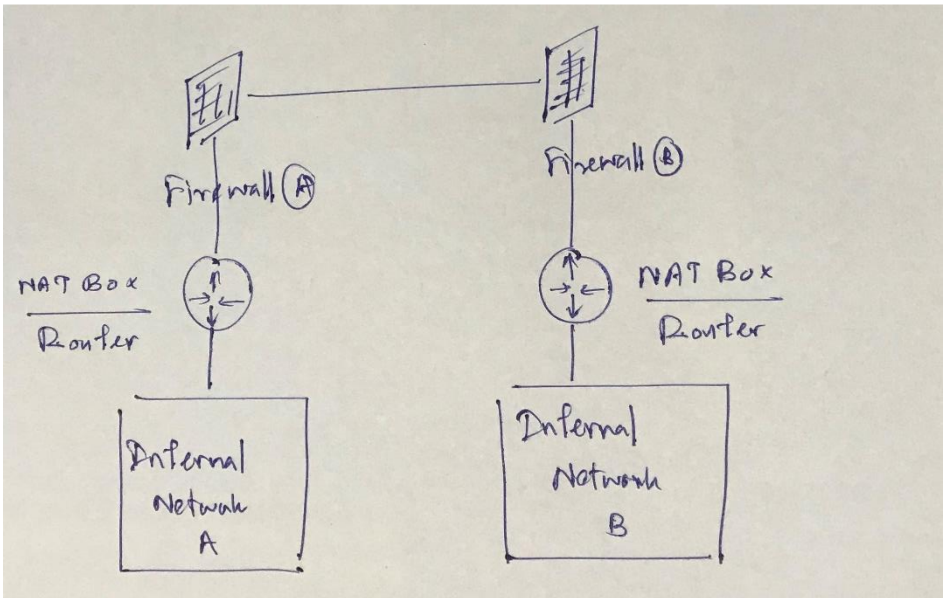
Host to Host



Host to Security Gateway



Security Gateway to Security Gateway



IPSec Connection Mode

IPSec implement two types of connection including

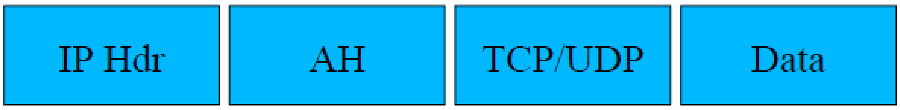
- Transport Mode
- Tunnel Mode

Transport Mode

- Does not encrypt the entire packet
- Uses original IP Header
- Faster

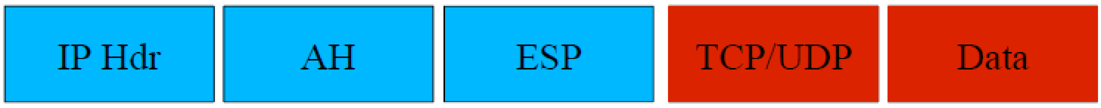
Authentication header (AH)

- IP Protocol 51
- Provides authentication of packets
- Does not encrypt the payload



Encapsulating Security Payload (ESP)

- IP Protocol 50
- Encrypts the Payload
- Provides Encryption and Authentication

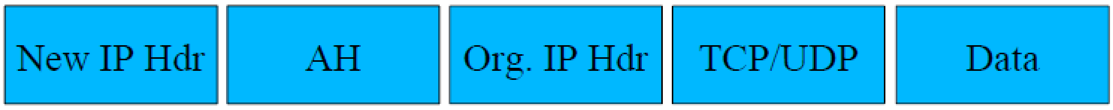


Tunnel Mode

- Encrypts entire packet including IP Header (ESP)
- Creates a new IP header
- Slower

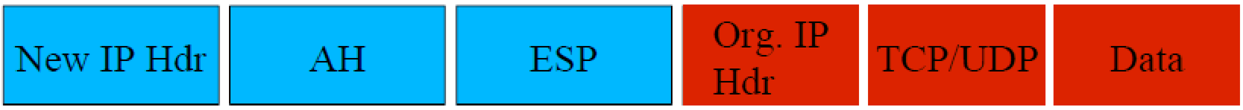
Authentication header (AH)

- IP Protocol 51
- Provides authentication of packets
- Does not encrypt the payload



Encapsulating Security Payload (ESP)

- IP Protocol 50
- Encrypts the Payload
- Provides Encryption and Authentication



2017-4(a)

4) a) IPSec is a framework for securing IP packets sent through the public Internet. Depending on the amount of security we need, it is possible to configure IPSec in different ways. IPSec ESP (Encapsulating Security Payload) Tunnel Mode is such a configuration. Using a suitable diagram,explain how IPSec ESP Tunnel Mode works to protect an IP datagram with a TCP payload.

(07 marks)

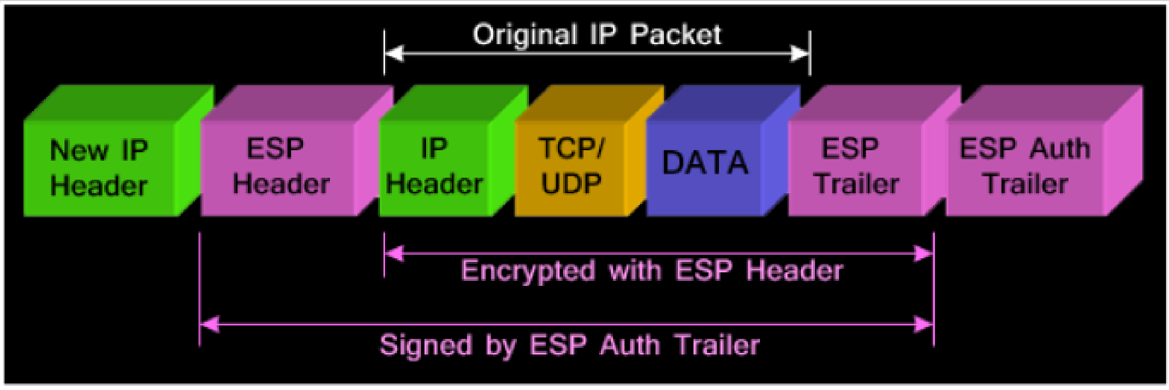
ANSWER IN THIS BOX

Tunnel mode is used to encrypt traffic between secure IPSec Gateways,

In tunnel mode, an IPSec header (AH or ESP header) is inserted between

the IP header and the upper layer protocol.

The packet diagram below illustrates IPSec Tunnel mode with ESP header:



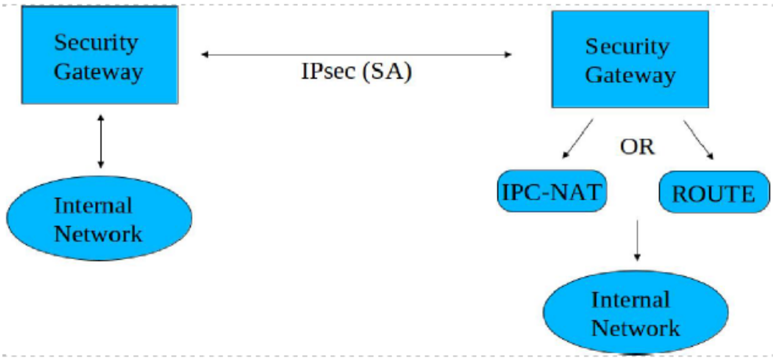
2012-4(b)

(b) Explain the security gateway to security gateway network configuration scenario that is used by the IPSec protocol use a simple diagram.

(06 marks)

ANSWER IN THIS BOX

Student should explain the following diagram.



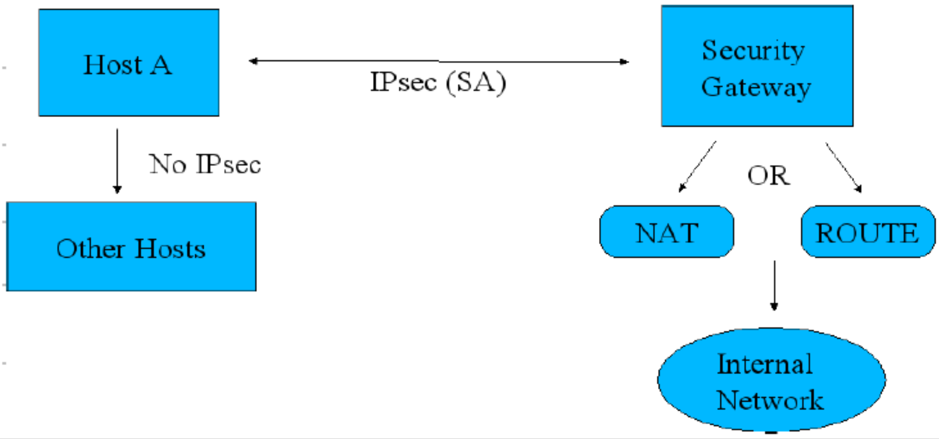
2011-4(b)

(b) Briefly describe a typical "Host to Security Gateway" IPSec configuration method referring to an example.

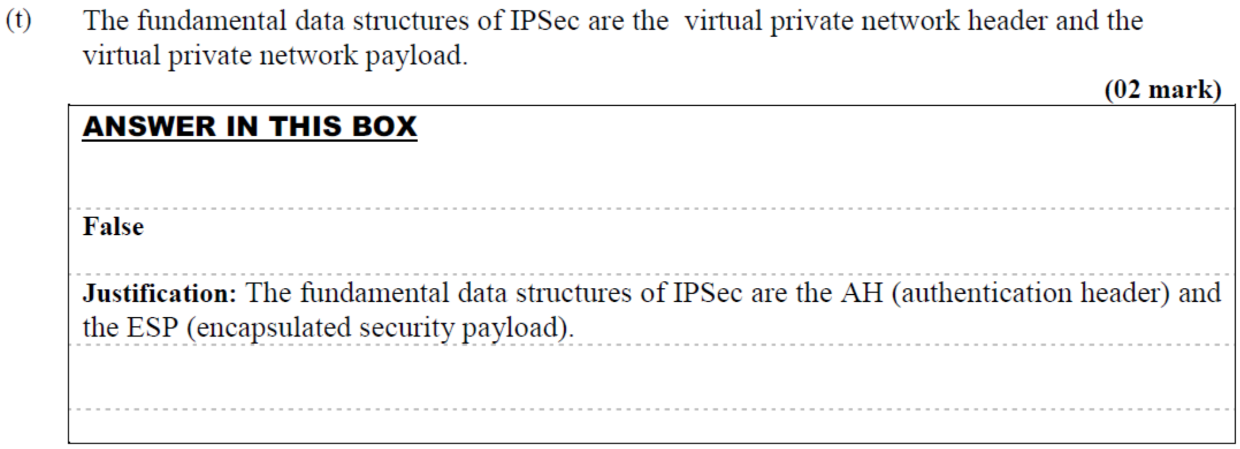
(05 marks)

ANSWER IN THIS BOX

(*Student should explain the following digram by using a practical example such as as roaming user connectivity*)



2011-1(t)



(t) The fundamental data structures of IPSec are the virtual private network header and the virtual private network payload.

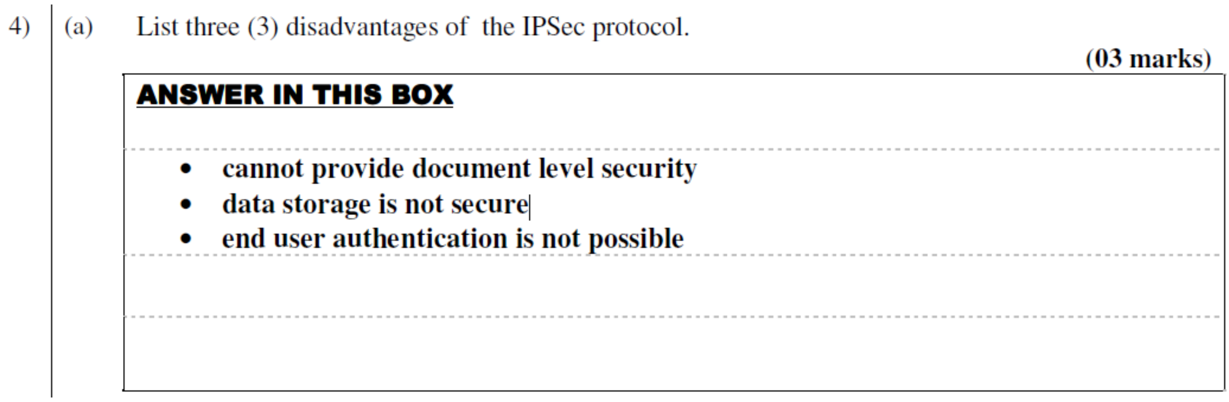
(02 mark)

ANSWER IN THIS BOX

False

Justification: The fundamental data structures of IPSec are the AH (authentication header) and the ESP (encapsulated security payload).

2009-4(a)



4) (a) List three (3) disadvantages of the IPSec protocol.

(03 marks)

ANSWER IN THIS BOX

- **cannot provide document level security**
- **data storage is not secure**
- **end user authentication is not possible**