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 and applications
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 and Applications

- IP security (IPSec)
- VPN
- Kerberos
- Multifactor authentication
- 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.

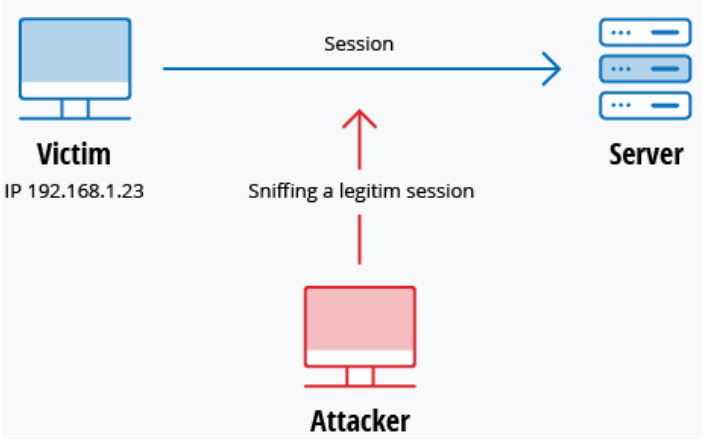
3. **Man-in-the-middle attack**

   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**

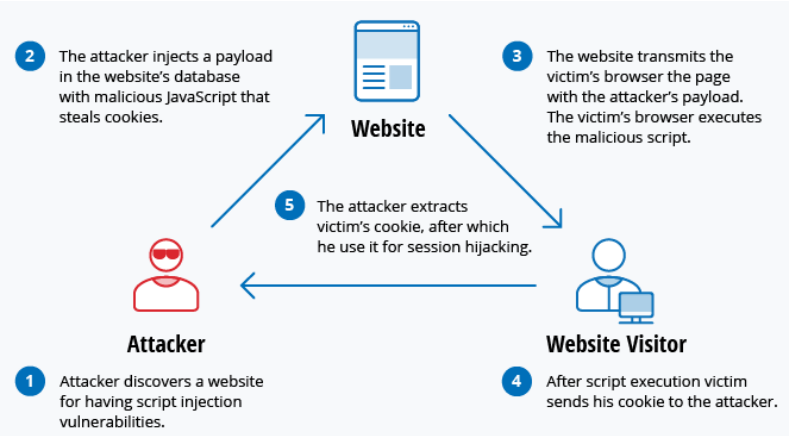
   This is common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the database via the input data from the client to server.

   *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.



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.

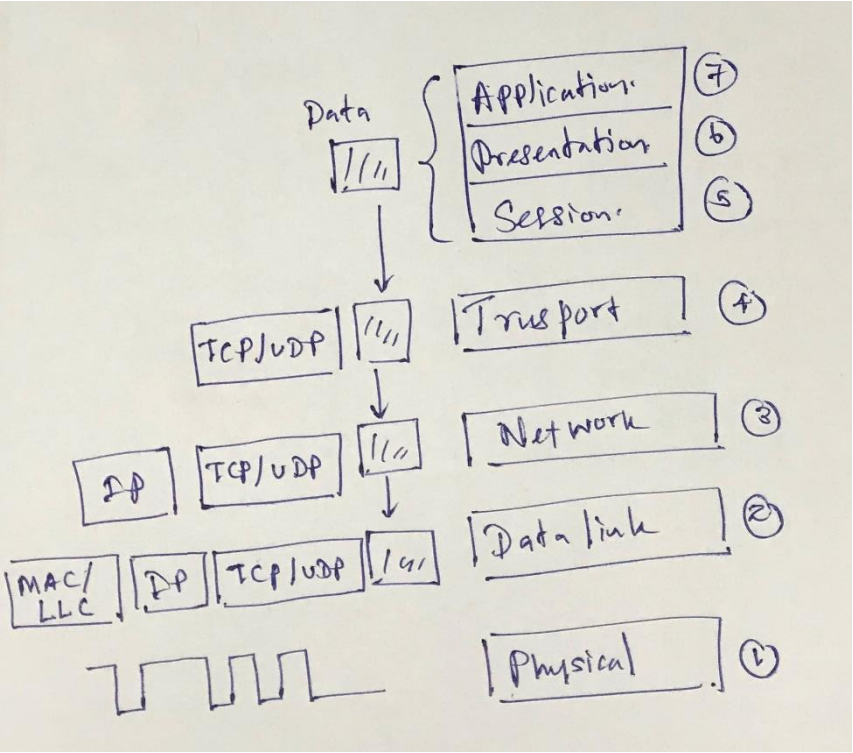
(02 marks)

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 and Applications

Internet Protocol 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

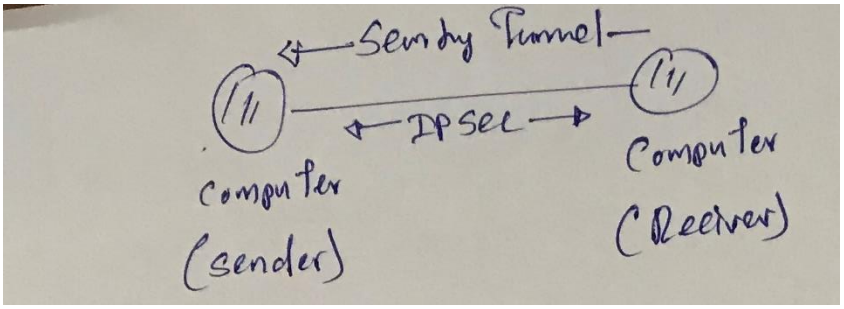
- Authentication
- Integrity
- Access control
- Confidentiality
- Replay protection (Partial)

Communication types of IPSec

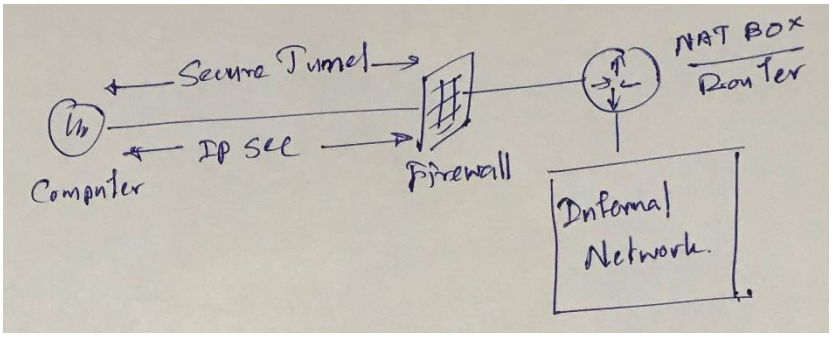
Mainly, three communication modes can be identified as follows.

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)

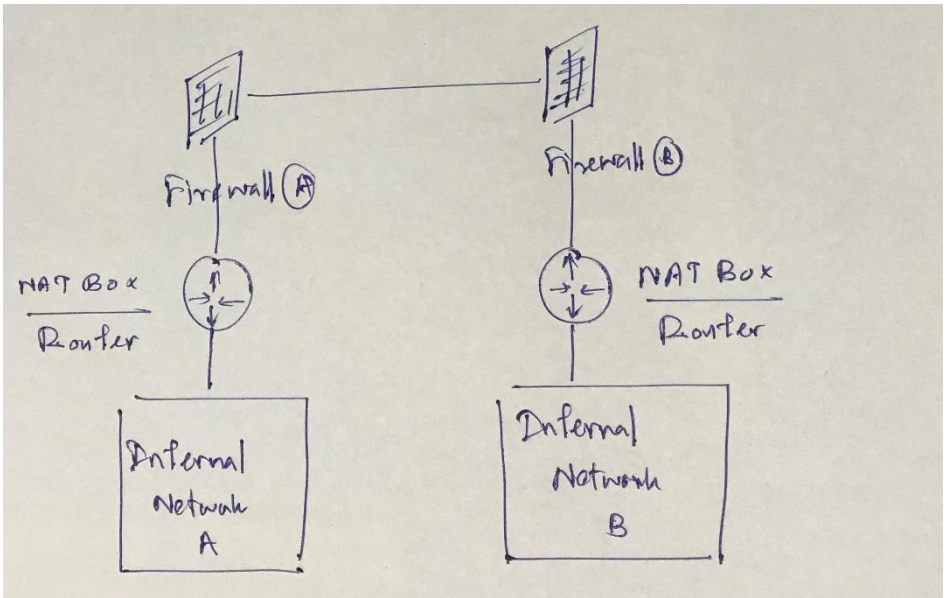
Host to Host



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

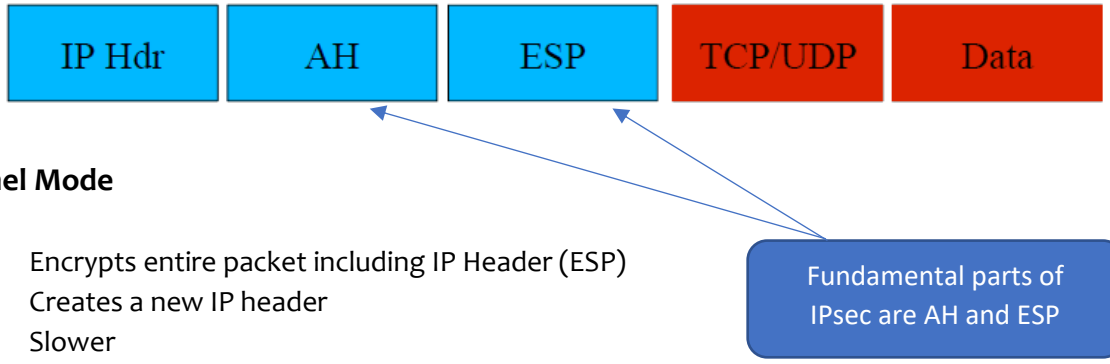
- Does not encrypt the entire packet
- Uses original IP Header
- Faster
- Works well in networks where increasing a packet's size could cause an issue
- Frequently used for remote access VPNs

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
- Frequently used in an IPsec site-to-site VPN

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

Now you can realize that additional information apart from default IP, TCP headers have to be managed in order to success the IPsec. These security properties that are recognized by communicating hosts is specified by IPsec **security association (SA)**.

Security association (SA)

- It specifies security properties from one host to another
- Another word, it is a kind of an agreement
- Typically require two SAs to communicate securely
- Particular IPsec SA specifies
  - security protocol (AH or ESP)
  - destination IP address
  - security parameter index (SPI)

An SPI is a 32-bit random number that is used to uniquely identify a particular SA for any connected device.

Those information are stored in security association database (SAD)

Various policies like above mentioned, are maintained in the **Security Policy Database (SPD)**. The sending host determines what policy is appropriate for the packet, depending on various "**Selectors**" by checking in **SPD**. Further, SPD indicates what the policy is for a particular packet.

- Source IP and Destination IP
- Name (User ID or a System Name)
- Transport Layer Protocols (TCP or UDP) or Source and Destination Ports

Major application of IPsec is **VPN**. We'll discuss in next topic.

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)

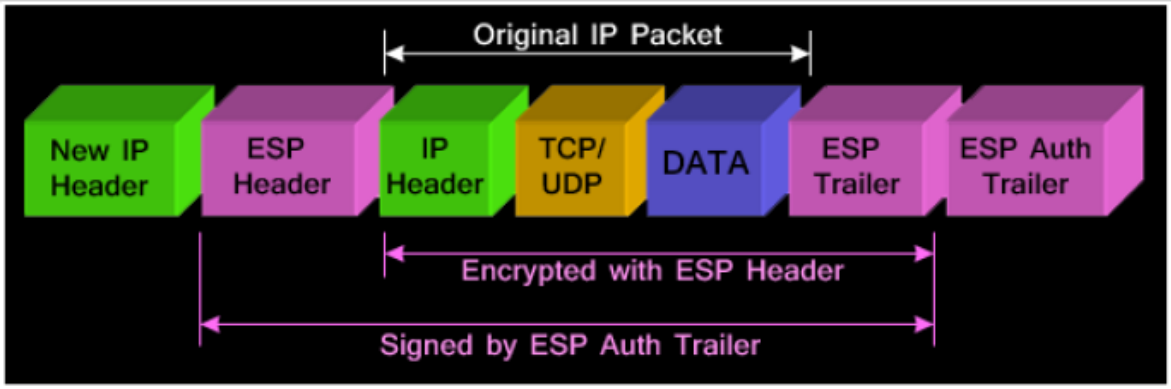
ANSWER IN THIS BOX

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:



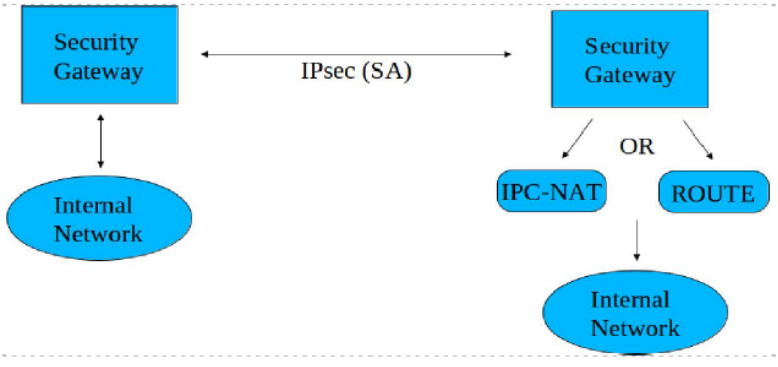
2012-4(b)

(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.



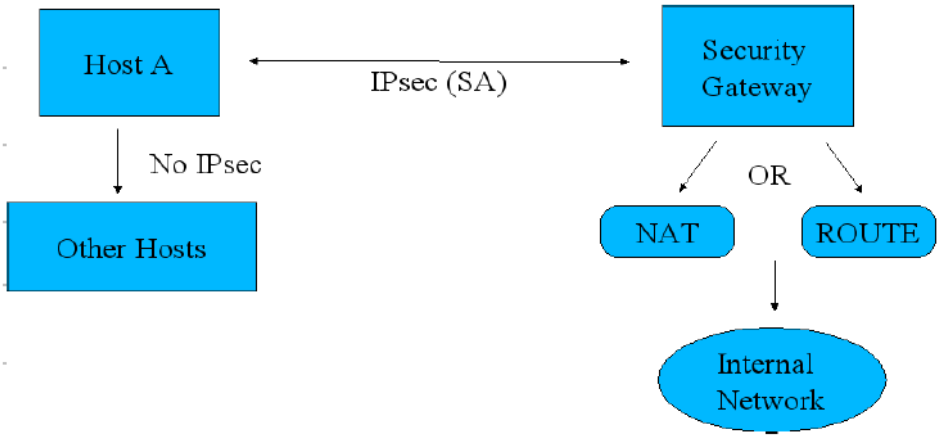
2011-4(b)

(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**

Virtual Private Network (VPN)

As you already known, we can send confidential data via public insecure links in secured way. This approach is called VPN. Which means, a VPN gives you online **privacy** and **anonymity** by creating a private network from a public internet connection. One of the best applications of IPsec is VPN. VPN create encrypted tunnel either among two computers or two networks.

Types of VPN

- Site – to – Site VPN (WAN VPN) – in between branch offices
- Remote Access VPN – among roaming users
- Extranet VPN

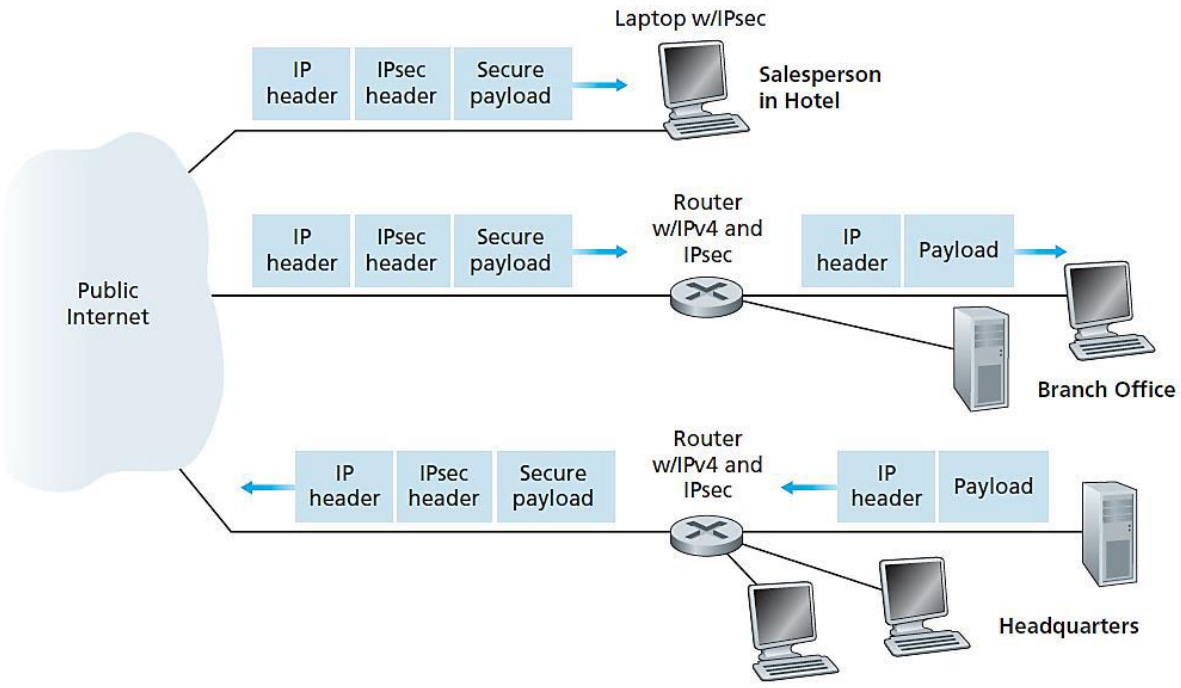
VPN suitable situation

1. If there are more locations to connect and locations are far
2. Less bandwidth required services
3. QoS is not much importance

Popular VPN protocols

1. IPSec (Internet protocol security)
2. PPTP (Point to point tunneling protocol)
3. L2TP (Layer 2 tunneling protocol) with IPSec
4. IKE (Internet Key Exchange) with IPSec
5. OpenVPN

VPN
- Provide Authentication
- Provide encryption
- Can work with certificate authorities
- Provide higher layer security of OSI model



VPN Protocol Comparison

VPN Protocol	Connection Speed	Level of Encryption	Connection Stability	Media Streaming	Torrent Downloading	Compatible With	Available in CactusVPN Client
PPTP	Very Fast	Poor	Very Stable	Good	Poor	Most OSs and devices	On Windows
L2TP/IPSec	Medium	Medium	Stable	Good	Medium	Most OSs and devices	On Windows
IKEv2/IPSec	Very Fast	Good	Very Stable	Good	Good	Most OSs and devices	On Windows, macOS, and iOS
IPSec	Medium	Good	Stable	Good	Good	Most OSs and devices	No
SSTP	Fast	Good	Very Stable	Medium	Good	Windows, Ubuntu, Android, and routers	On Windows
OpenVPN TCP	Medium	Very Good	Stable	Medium	Good	Most OSs and devices	On Windows and Android
OpenVPN UDP	Fast	Very Good	Medium	Good	Good	Most OSs and devices	On Windows and Android
SoftEther	Very Fast	Very Good	Very Stable	Good	Good	Most OSs and devices	No
Wireguard	Fast	Good	Not Yet Stable	Medium	Medium	Linux, macOS, iOS, and Android	No

2019-1(a)

(a) Suppose users in two offices would like to access each other's file servers over the Internet. Digital signature security control could provide confidentiality for such communication.
(02 marks)

ANSWER IN THIS BOX
False Virtual private network (VPN) security control would provide
confidentiality for those communications.

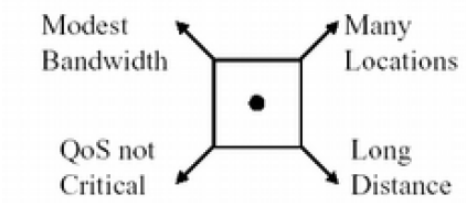
2019-4(c)

c) Provision of a Virtual Private Network (VPN) is not always justifiable in interconnecting branches of an organization. Briefly explain the deciding factors for using a VPN.

(04 marks)

ANSWER IN THIS BOX

The student should explain the following factors.



- More Locations, Longer Distances, Less Bandwidth/site, QoS less critical
  ⇒ VPN more justifiable
- Fewer Locations, Shorter Distances, More Bandwidth/site, QoS more critical
  ⇒ VPN less justifiable

2017-2(e)

e) An encrypted communications tunnel created between two systems, and used for secure communications, is called a;

a) Leased Line

b) Chinese Firewall

c) Named-pipe

d) Virtual Private Network (VPN)

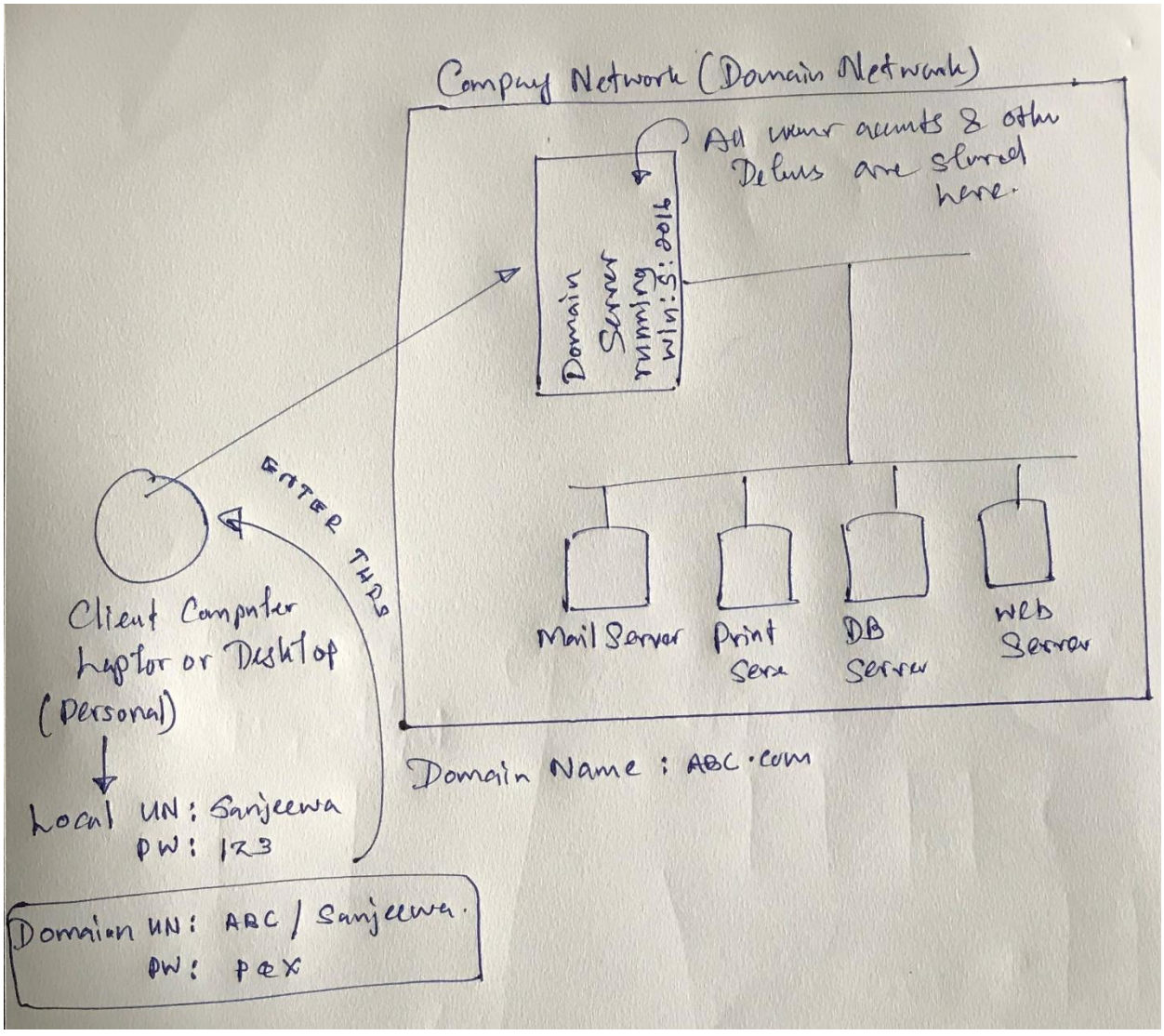
(02 marks)

ANSWER IN THIS BOX
(D)-Correct- By definition, a VPN provides a secure tunnel from one site
to another over an insecure environment such as the Internet.

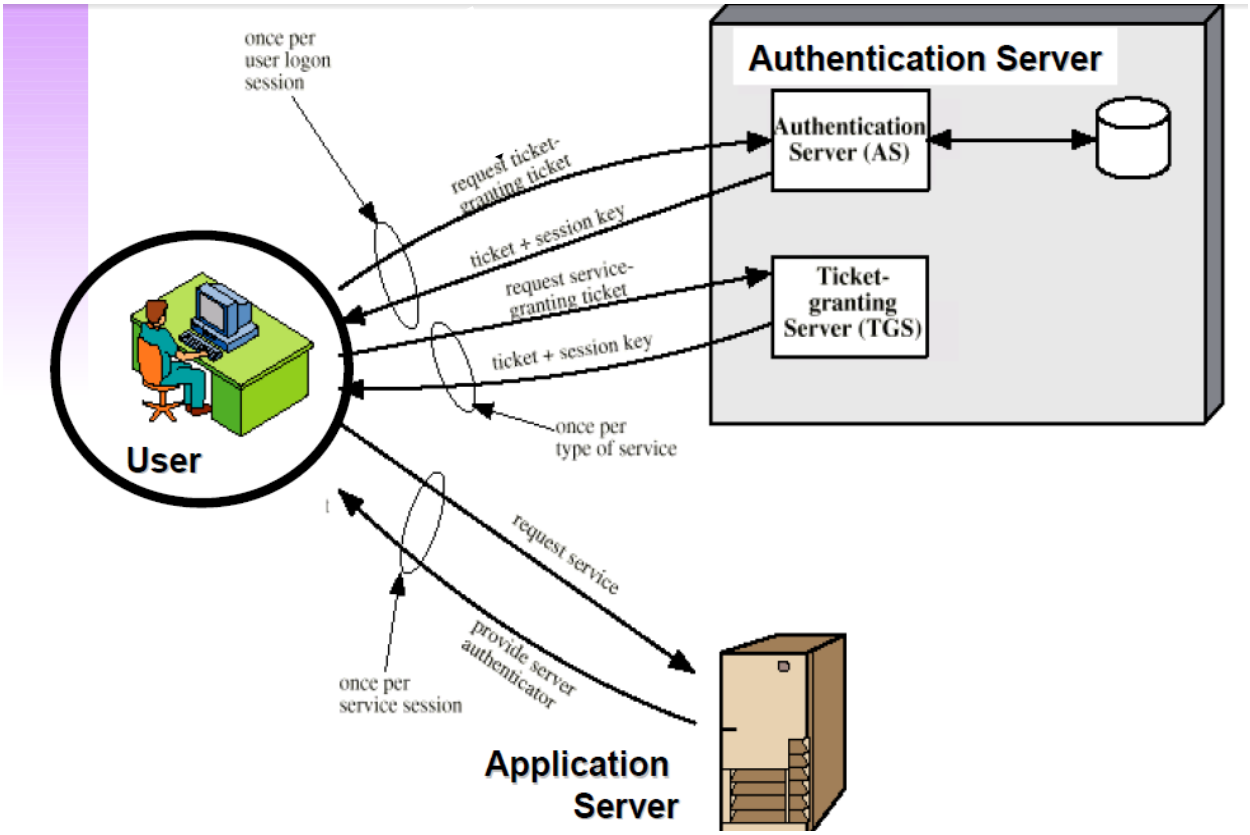
Kerberos

- Is a network authentication protocol
- Provide strong authentication for client/server applications as well as peer to peer applications
- Use private key cryptography
- Kerberos 5 Release 1.18.1 is the modern version
- Developed by Massachusetts Institute of Technology (MIT)
- It is a free standard
- But include in some commercial product (Ex: Microsoft include this for their server OSs from server 2000)

In practical, you'll experience scenario like this.



Now let's looks how this work theoretically?



Note that: at once user request particular application from application server, but that request is gone through Kerberos authentication server.

Step 1: user requiest "ticket granting ticket" from authentication server
Step 2: AS issues "ticket granting ticket" and session key to client

Step 3: user request "login ticket" from ticket granting server (TGS)
Step 4: TGS issues "login ticket" and session key to client

Step 5: user send "login ticket" to application server
Step 6: Server verifies the ticket and the authenticator and if OK, grants access to the requested server

2017-1(l)

(l) In Kerberos authentication protocol, a Ticket-Granting Server (TGS) issues a ticket granting ticket to the Kerberos client.

(02 marks)

ANSWER IN THIS BOX
False
In Kerberos authentication protocol, an Authentication Server (AS) issues
a ticket granting ticket to the Kerberos client.
Ticket-Granting Server (TGS) issues a login ticket to the Kerberos client.

2015-1(s)

(s) Kerberos is a system that supports authentication in distributed systems.

(02 mark)

ANSWER IN THIS BOX
True
Kerberos is used for authentication between intelligent processes, such as client-to-server
tasks, or a user's workstation to other hosts. Kerberos is based on the idea that a central server
provides authenticated tokens, called tickets, to requesting applications. A ticket is an
unforgeable, nonreplayable, authenticated object.

2013-1(s)

(s) In Kerberos authentication protocol, an Authentication Server (AS) issues a login ticket to the Kerberos client.

(02 marks)

ANSWER IN THIS BOX
False
Justification: In Kerberos authentication protocol, a Ticket-Granting Server (TGS) issues a login ticket to the Kerberos client.

2012-1(r)

(r) The Kerberos authentication protocol requires two systems, called the Certification Authority (CA) and the Digital Certificate (DC), which are both part of the Key Distribution Center (KDC).

(02 mark)

ANSWER IN THIS BOX
False
Justification: Kerberos authentication protocol requires two systems, called the Authentication Server (AS) and the Ticket-Granting Server (TGS), which are both part of the Key Distribution Center (KDC).

Multifactor authentication

Following things, we used to authenticate in day to day life: password, debit card, PIN number, finger mark, face of user self, voice pattern and etc.... Those are belonging to following categories

1. **User has** (Debit card)
2. **User knows** (PIN number, Password)
3. **User is** (finger mark, face id)

In some case, in order to strength the security level, we approach to use more than one factor with access control system at the same time. This is known as multifactor authentication

2018-1(j)

(j) A One Time Password (OTP) protocol which sends a random password via SMS to your mobile phone provides two-factor authentication.

(02 marks)

ANSWER IN THIS BOX
True
In using a this protocol, a user needs to access his mobile phone and enter the OTP.
Thus it provides two factor authentication.

2018-2(a)

a) Which one of the following security controls can be used to increase the authentication strength of an access control system?

(i) Key-pad door lock

(ii) Two Factor dongle

(iii) PIN number

(iv) Password

(02 marks)

ANSWER IN THIS BOX
(ii) CORRECT: Using two of the three factors
(something you know, something you have, and something you are)
increase the strength of authentication.

2017-1(j)

(j) An ATM cards provides three-factor authentication.

(02 marks)

ANSWER IN THIS BOX
False
An ATM cards, a user needs to enters the PIN and put the finger.
Thus it provides two factor authentication.

2017-2(f)

f) Which one of the following can be used to increase the authentication strength of an access control system?

a) Multi-party

b) Two Factor

c) Mandatory

d) Discretionary

(02 marks)

ANSWER IN THIS BOX
(B) – Correct - Using two of the three factors (something you know,
something you have, and something you are) increase the strength of authentication.

2016-1(j)

(j) An ATM card provides two-factor authentication.

(02 marks)

ANSWER IN THIS BOX
True
In the ATM card system, user needs to present the card and enters
the PIN so it provides two factor authentication.

2013-1(j)

(j) A fingerprint based attendance system provides two-factor authentication.

(02 marks)

ANSWER IN THIS BOX
True
Justification: In the fingerprint based attendance system, a user needs to enters the PIN and put the finger so it provides two factor authentication.

2012-3(a)

3) (a) Describe "two factor authentication" mechanism by using an example.

(05 mark)

ANSWER IN THIS BOX

A two factor authentication mechanism combines two authentication mechanisms that list under the following authentication principles.

1. Something the user knows
2. Something the user has
3. Something the user is

Automatic Teller Machine (ATM) card is the best example for two factor authentication. It uses a plastic card with the magnetic script (Something the user has) and Personal Identification Number (PIN) (Something the user knows) for authentication of a banking user.

2011-3(c)

(c) Authentication mechanisms use three(3) basic principles to confirm a user's identity. Briefly describe these three(3) basic principles.

(06 mark)

ANSWER IN THIS BOX

1. Something the user knows. Passwords, PIN numbers, passphrases, a secret handshake, and mother's maiden name are examples of what a user may know.

2. Something the user has. Identity badges, physical keys, a driver's license, or a uniform are common examples of things people have that make them recognizable.

3. Something the user is. These authenticators, called biometrics, are based on a physical characteristic of the user, such as a fingerprint, the pattern of a person's voice, or a face (picture).

2010-1(k)

(k) A banking card (ATM card) provides two-factor authentication.

(02 marks)

ANSWER IN THIS BOX

True

Justification: In the ATM card system, user needs to present the card and enters the PIN so it provides two factor authentication.

2009-1(k)

(k) A smart card provides the so called "two-factor authentication".

(02 marks)

ANSWER IN THIS BOX

True

Justification: In the smart card system, a user is required to present the card and the enter the PIN so it that provides two factor authentication.

2008-2(f)

(f) Typically, a password should be relatively long enough to provide enhanced security. However, PINs (Personal Identification Numbers) used with ATM cards to draw money out of a cash machine have only four decimal digits. Why is it safe to have PINs of only four digits even though we would normally recommend that passwords be longer than this?

(05 marks)

ANSWER IN THIS BOX

ATM cards use two factor authentication (in addition to the PIN, a valid card must be presented at the ATM machine).

At the ATM machine an intruder can try the PIN only a maximum of 3 times.

To be continued