Tutorial 1

1. Explain the difference between Computer security, Network security, and Internet security by giving an example for each team.

Computer security\

- Hardware to operating system
- It is a generic name for the collection of tools designed to protect data and thwart挫败 hackers.
- It focuses on protecting individual computers, servers and devices from threats such as malware, unauthorized access and data breaches.
- For example, using BitLocker to encrypt a laptop's hard drive.

Network security

- LAN, WAN
- It is a measure to protect data during their transmission.
- It protects networks from unauthorized access, attacks and misuse.
- For example, a company's Wi-Fi is secured using WPA3 encryption and a firewall to block malicious traffic.

Internet security

- e.g. Secure and protect information during online transaction / purchase
- It is a measure to protect data during their transmission over a collection of interconnected networks.
- It protects against threats from the internet such as phishing, malware and DDoS attacks.
- For example, a browser warning about an untrusted website or using HTTPS for secure transactions.

2. In both X.800 and RFC4949, security attacks have been classified in terms of passive attacks and active attacks. What is the difference between the term passive attack and active attack? Give one example for each term.

Passive attack

- It attempts to learn or make use of information from the system but does not affect system resources.

- It does not affect data to be transmitted.
- The goal is to gather information covertly秘密.
- For example, eavesdropping, traffic analysis and data interception.
- The threat of unauthorised disclosure of information without changing the state of the system.

Active attack

- It attempts to alter system resources or affect their operation.
- It affects data to be transmitted.
- The goal is to modify, destruct or disrupt network communication or data.
- For example, data modification, unauthorized access, denial of service (DoS), spoofing, or injection of malicious code.
- The threat of a deliberate unauthorized change to the state of the system.

3. Briefly define FOUR (4) categories of active attack.

Masquerade

- It takes place when one entity pretend to be a different entity.
- It usually includes one of the other forms of active attack.

Replay

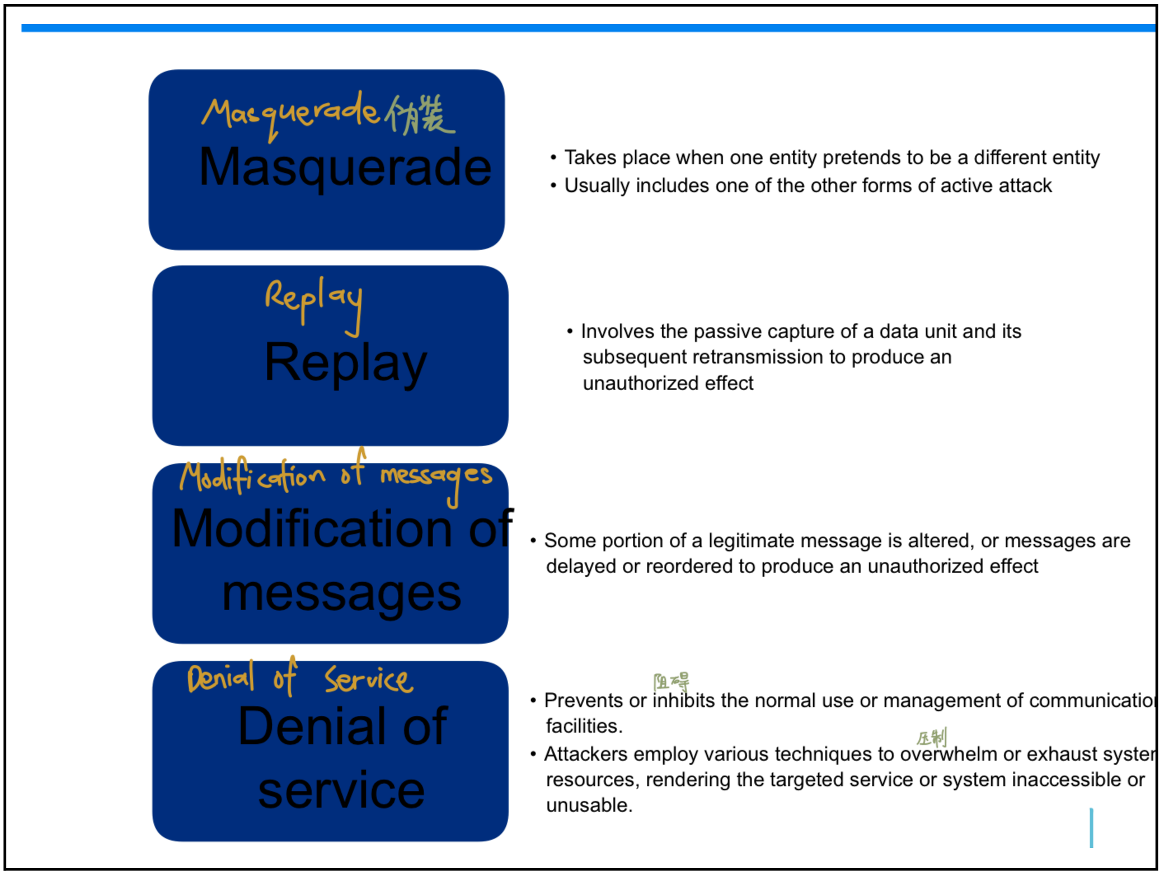
- It involves the passive capture of a data unit, then retransmit it to produce an unauthorized effect.

Modification of messages

- It alters some portion of legitimate message, or delays or reorders the messages to product an unauthorized effect.

Denial of service

- It prevents or inhibits阻碍 the normal use or management of communications facilities by sending a lot of traffic.
- Attacks employ various techniques to overwhelm or exhaust system resources, making the targeted service or system inaccessible or unusable.



Masquerade 伪装

Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Modification of messages

Modification of messages

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Denial of Service

Denial of service

- Prevents or 阻碍 inhibits the normal use or management of communicatio facilities.
- Attackers employ various techniques to 压制 overwhelm or exhaust syster resources, rendering the targeted service or system inaccessible or unusable.

4. What is the difference between the term threat and attack? Give one example for each term.

Threat

- It is a potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm.
- It is possible to happen, but not yet happen.
- For example, unstructured threats, structured threats, external threats and internal threats.

Attack

- It is an assault on system security that derives from an intelligent threat, which also means an intelligent act which deliberately attempts to evade (avoid) security services and violate the security policy of a system.
- It has already happened on the system security.
- For example, Viruses, Spyware, Phishing, Worms and DoS attacks.

5. You are the IT manager of a large e-commerce company that operates an online marketplace. Your platform connects buyers and sellers, facilitating transactions and storing sensitive customer information such as credit card details, addresses, and purchase history. Recently, there has been a rise in cyber-attacks targeting e-commerce platforms, and you have been tasked with enhancing internet security measures to protect your customers' data. Identify the three security requirements that are essential to your company.

Confidentiality

- It is the property that information is not made available or disclosed to unauthorized individuals, entities or processes.
- It can help to prevent unauthorized parties from accessing customers' sensitive information such as credit card details, addresses and purchase history.

Integrity

- It is the property that data has not been altered or destroyed in an unauthorized manner.
- It can avoid hackers from modifying or deleting customers' information without authorization.
- Can check integrity via checking whether there are changes in the hash code.

Availability

- It is the property of being accessible and useable upon demand by an authorized entity.
- It allows authorized customers to access their own information such as credit card details, addresses and purchase history.

6. On 12th May 2022, a popular online gaming platform and a streaming service experienced significant disruption in their services. Users reported that they were unable to access the gaming platform, while the streaming service suffered from severe buffering and intermittent connectivity issues. Investigations revealed that both services were targeted by a large-scale botnet-driven attack.

   (i) Name this type of attack.

Denial-of-Service (DoS) attack.

(ii) Is this attack a passive attack or an active attack? Support your answer with an explanation.

- This attack is an active attack.
- It has significantly disrupted the network communications as users were unable to access the gaming platform.
- Meanwhile, the streaming service was undergoing buffering and intermittent connectivity issues.

(iii) This type of attack usually attacks on *availability* of the websites. From the perspective of security services, describe the term *availability*.

- Availability is the property of being accessible and useable upon demand by an authorized entity.
- In this scenario, the availability of websites is affected as users were unable to access the gaming platform.

Tutorial 2

1. How many keys are required for two people to communicate via a symmetric cipher?

1 shared key
1 secret key

* Asymmetric cipher uses 2 keys.

2. What is the difference between a block cipher and a stream cipher?

Block Cipher

- Block cipher encrypts data in fixed-size blocks.
- It processes data in fixed-size blocks.
- It needs more processing power and it has lower speed as its code is larger.
- It is not suitable for real-time streams.
- Block cipher is one in which a block of plaintext is treated as whole and used to produce a ciphertext block of equal length.

Stream Cipher

- A stream cipher encrypts data one bit or one byte at a time, in a continuous stream.
- It processes data on individual bits or bytes.
- It has faster speed as it is applying a straightforward approach and lower overhead.
- It is well-suited for real-time stream encryption.
- A stream cipher is one that encrypts a digital data stream one bit or one byte at a time.

3. Describe the purposes of *Substitution* and *Transposition* in the cryptography process.

Substitution

- Substitution involves replacing elements of the plaintext with other elements according to a predefined rule or key.
- In the cryptography process, it substitutes letters or characters with other letters or characters.
- It can add an extra layer of security by encode the message.
- An operation that substitutes one value with another value.

Transposition

- Transposition involves rearranging the order of elements in the plaintext without changing the actual elements themselves.
- It does not change the original characters of the message, only their order is modified.
- It can provide security by scrambling the order of the plaintext, making it difficult to decipher without knowing the transposition key.

- An operation that exchanges one value with another value.

4. List down the strengths & drawbacks of 3DES.

Strengths

- Triple DES (3DES) has a longer key length, 168-bit key length which can overcome the vulnerability to brute-force attack of DES.
- It is also very resistant to cryptanalysis, in the sense of a longer time of period to scrutinize the algorithm.

Drawbacks

- 3DES requires three times as many rounds as DES so the additional rounds would cause the increased computational overhead and slower performance.
- Since 3DES is still using a 64-bit block size, the 64-bit block size is not large enough for efficiency and security.
- The original DES algorithm was designed in the mid-1970s when hardware implementations were the primary focus. As a result, the DES algorithm does not lend itself to efficient software implementations due to its design and structure.

5. Explain how AES overcomes the drawbacks of 3DES.

- AES supports the key length of 128, 192 or 256 bits. It can make it more resistant to brute-force attacks as computational power increases compared to 3DES.
- AES operates on a 128-bit block size which can enhance the security compared to 3DES which is using 64-bit block size only.
- AES employs a permutation-substitution approach, which involves a series of substitution and permutation steps. Meanwhile, 3DES only uses the Feistel network which divides the block into two halves before encryption.
- A key length that can be 128, 192 or 256 bits.
- Does not use a Feistel Structure processes the entire data block in parallel during each round using substitution and permutation.

6. What is the difference between a link and end-to-end encryption?

Link encryption

- It involves a lot of encryption devices.
- It has a high level of security.
- It decrypts each packet at every switch.

End-to-end encryption

- It encrypts the source and lets the receiver decrypt it.
- The data is encrypted.
- Header is not encrypted.

7. List ways in which secret keys can be distributed to two communicating parties.

Physical delivery

- One party can select a key and physically deliver it to the other.
- A third party can select the key and physically deliver it to both parties.
- This method is suitable when there is personal contact between the recipient and key issuer.

Using Previous Keys

- If the two parties have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.

Public Key Cryptography

- A generates a public or private key pair and transmits the public key to B.
- A uses B's public key to encrypt a message to B containing an identifier of A and a nonce.
- B sends a message to A encrypted with A's public key, containing A's nonce and a new nonce generated by B.
- A returns B's nonce encrypted using B's public key.
- A selects a secret key and sends it to B, encrypted with B's public key and A's private key.
- B recovers the secret key.

For two parties A and B, key distribution can be achieved in a number of ways, as follows:

1. A can select a key and physically deliver it to B,
2. A third party can select the key and physically deliver it to A and B.
3. If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
4. If A and B each have an encrypted connection to third party C, C can deliver a key on the encrypted links to A and B.

Past Year Questions:

1. Both DES and 3DES utilize the Feistel Cipher Structure in the encryption process. Briefly explain **TWO (2)** criteria needed to increase security in Feistel Cipher Structure.

- Block size: larger block sizes can lead to greater security.
- Key size: larger key size means greater security.
- Number of rounds: multiple rounds offer increasing security.
- Subkey generation algorithm: greater complexity leads to greater difficulty of cryptanalysis, but slows cipher.
- Round function: greater complexity will make analysis harder, but slows cipher.
- Fast software encryption/decryption: the speed of execution of the algorithm becomes a concern.

2. Briefly explain **THREE (3)** examples of attacks that adopt by cryptanalysis.

Brute-force attack

- The approach involves trying and testing all possible keys in order to recover the plaintext from ciphertext.

Dictionary attack

- It is a technique for defeating a cipher text by trying to determine its decryption key by searching a large number of possibilities.

Probable-word attack

- In this attack, a guess is made as to a word that may occur in the text. For example, the guess that the words ‘fuehrerhauptquartier’ (the Fuhrer’s headquarters) exists in the encrypted document.

3. (i) Explain the function of a Key Distribution Center.

The function of the Key Distribution Center is to transmit temporary session keys to users. Each session key is transmitted in encrypted form, using a master key.

(ii) List and describe each step shown in Figure 1.

Figure 1 shows one of the key distribution options.

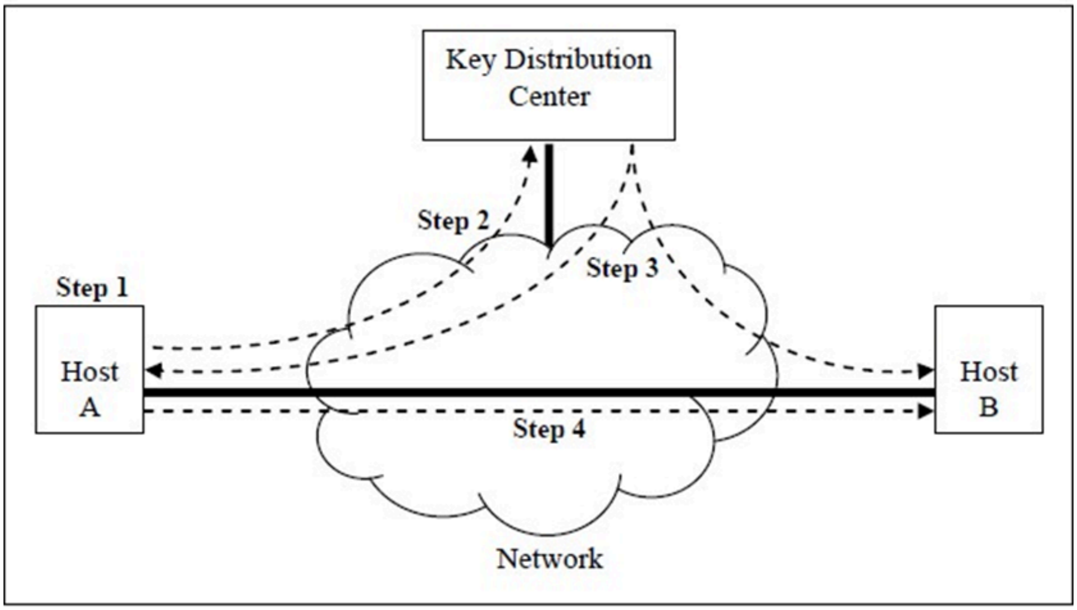


Figure 1: Key Distribution

Step 1: Host sends packet requesting connection.
Step 2: Security service buffer packet, asks KDC for session key.
Step 3: KDC distributes the session key in both hosts.
Step 4: Buffered packet transmitted.

4. (i) Identify encryption methods A and B. Explain the function of A and B in Figure 2.

A: Link encryption
Each vulnerable communications link is equipped on both ends with an encryption device.

B: End-to-end encryption
The encryption process is carried out at the two end systems. The source host or terminal encrypts the data; the data in encrypted form are then transmitted unaltered across the network to the destination terminal or host.

(ii) Do you agree that every message which passes through a packet switch is not secure? Support your opinion with a reason.

Figure 2 shows a packet-switching network with encryption devices.

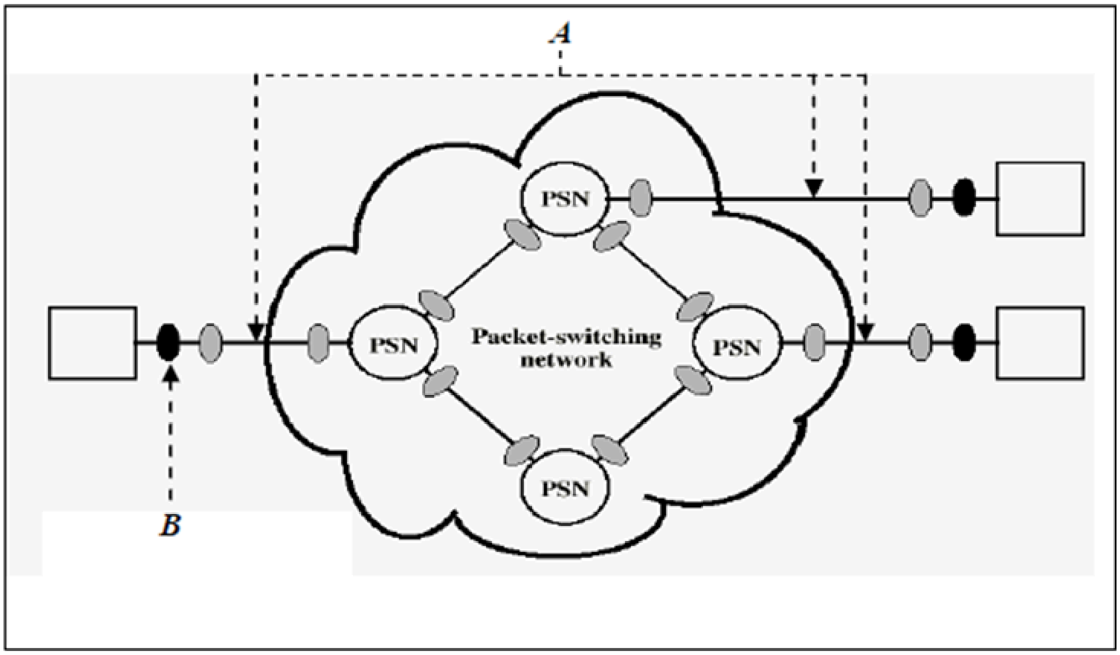


Figure 2: Packet-switching network with encryption devices

Yes
The message must be decrypted each time it enters a packet switch.
The switch must read the address (Virtual circuit number) in the packet header to route the packet. Therefore, the message is vulnerable at each switch.

Tutorial 3

1. What properties must a hash function have to be useful for message authentication?

Variable input size

- H can be applied to a block of data of any size.

Fixed output size

- H produces a fixed-length output.

Efficiency

- H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.

Preimage resistant (one-way property)

- For any given hash value h, it is computationally infeasible to find y such that H(y) = h.

Second preimage resistant (weak collision resistant)

- For any given block x, it is computationally infeasible to find y ! x with H(y) = H(x).

Collision resistant (strong collision resistant)

- It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).

Pseudorandomness

- Output of H meets standard tests for pseudorandomness.

1. Given M, easy to compute h = H(M)
2. Given h, hard to compute M such that h = H(M) → “one-way”, or “pre-image resistant”
3. Given M, hard to find M’ (different from M) such that H(M) = H(M’) → “second pre-image resistant”
4. (Not always satisfied) Hard to find M, M’ such that H(M)=H(M’) → “collision resistant”

2. What is the difference between a private key & secret key?

Private key

- It is used in public-key cryptography (asymmetric encryption) such as RSA, ECC and Diffie-Hellman.
- It is used for decryption when receiving encrypted messages.
- It acts as digital signatures to prove authenticity.

Secret key

- It is used in symmetric encryption, such as AES and DES.
- A single key is shared between parties for both encryption and decryption.
- It must remain confidential, as anyone with the secret key can decrypt messages.

The key used in symmetric encryption is typically referred to as a secret key.
The 2 keys used for public-key encryption are referred to as the public key and private key.

3. Explain what you understand with digital signature.

- The sender “signs” a message with its private key.
- It is a cryptographic mechanism used to ensure the authenticity, integrity and non-repudiation of digital messages or documents.
- It uses asymmetric cryptography (public-key cryptography), where a private key is used to sign the data, and a public key is used to verify the signature.
- It has 3 properties:
    - Authentication: Ensures the sender is genuine since only they have the private key.
    - Integrity: Ensures that the message has not been altered during transmission.
    - Non-repudiation: The sender cannot deny having signed the message since the private key is unique to them.
- Uses Cases:
    - Secure Emails
    - Software Distribution
    - Digital Certificates
    - Legal Documents

Digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator’s private key. The signature guarantees the source and integrity of the message.

4. How can public key encryption be used to distribute a secret key?

1. Key Generation
    a. The receiver will generate a public-private key pair which are public key (shared openly) and private key (kept secret).
2. Encrypting the Secret Key
    a. The sender will generate a random secret key for symmetric encryption.
    b. Then, he will encrypt the secret key using the receiver’s public key.
    c. Thus, the encrypted secret key is safe to send over an insecure channel.
3. Decrypting the Secret Key
    a. When the receiver receives the encrypted secret key, he decrypts it using his private key.
    b. Only Bob can decrypt it since only he has the private key.
4. Secure Communication Using Symmetric Encryption
    a. Now that both sender and receiver share the secret key, they can use it for fast and efficient symmetric encryption to communicate securely.

Several different approaches are possible, involving the private key(s) of one or both parties. One approach is Diffie-Hellman key exchange. Another approach is for the sender to encrypt a secret key with the recipient’s public key.

Past Year Questions

1. Jeremy is a business manager and he is running an e-commerce website. He has very little knowledge in Internet security. Recently, his e-commerce website was hacked and data being transmitted from clients were corrupted. The website was unable to prove the data was genuine or fake.

   i. As an IT security consultant, you know that there are three types of one-way hash functions that can be used with other encryption methods and able to determine whether the date received from the clients were genuine. List THREE (3) types of one-way hash functions with its combination of other encryption methods.

HMAC (hash-based message authentication)

- The hash functions used are SHA-256, SHA-3 or MD5.
- The encryption method used is symmetric encryption such as AES.
- HMAC combines a cryptographic hash function with a secret key to create a message authentication code (MAC).
- it can ensure data integrity and authentication for preventing hackers from tampering with messages.

Digital Signatures (RSA + SHA-256)

- The hash functions used are SHA-256 or SHA-512.
- The encryption method used is asymmetric encryption such as RSA and ECDSA.
- A hash of the data is created and then encrypted using a private key to generate a digital signature.
- the receiver uses the public key to verify the signature and ensure the data is authentic and not tampered with.

Keyed Hash Function (PBKDF2, bcrypt or Argon2 with AES)

- The hash functions used are PBKDF2, bcrypt or Argon2.
- The encryption method used is AES (Advanced Encryption Standard).
- It is used mainly for password hashing and secure key derivation.
- It can prevent brute-force attacks and ensures that stored credentials remain safe.
- It can be combined with AES encryption to securely transmit sensitive information.

One-way hash function with Symmetric Encryption
One-way hash functions with Public Key Encryption
One-way hash functions with Secret Value

   ii. Provide ONE (1) difference for each of the three types of one-way hash functions

HMAC vs Digital Signatures

- HMAC uses a secret key shared between two parties while digital signatures use a private-public key pair, where only the private key can generate the signature, and the public key verifies it.

- HMAC is faster and suitable for private communications while digital signatures provide non-repudiation.

Digital Signatures vs Keyed Hash Functions

- Digital signatures are used for authenticating messages and documents, while keyed hash functions are mainly used for secure password hashing and key derivation.
- Digital signatures ensure the sender's authenticity, while keyed hash functions slow down brute-force attacks for password security.

HMAC vs Keyed Hash Functions

- HMAC is used to verify message integrity and authentication while keyed hash functions are designed for password hashing and cryptographic key stretching.
- HMAC protects data in transit, while keyed hash functions protect stored credentials by making password cracking harder.

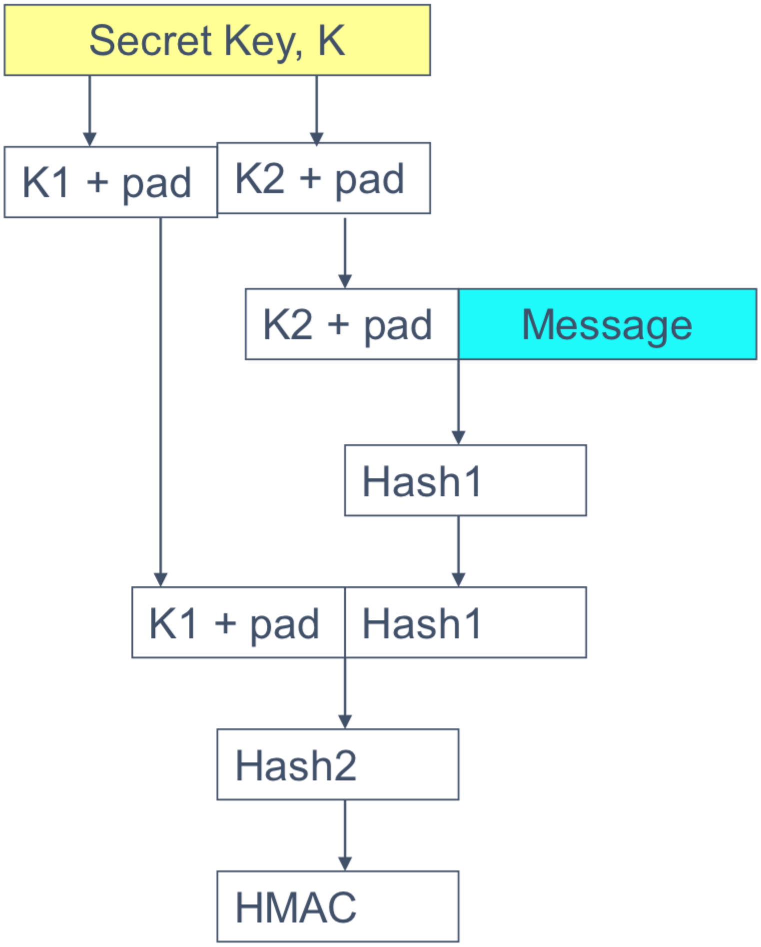
One-way hash function with Symmetric encryption
Using Hash functions and encrypt.decrypt with secret key.

One-way hash function with public key encryption
Using Hash Functions and encrypt with private key & decrypt with public key.

One-way hash functions with Secret Value
Using Hash Functions and secret value. No key involved.

iii. Among these three types of one-way hash functions, which is the most suitable to be recommended for Jeremy's e-commerce website? State ONE (1) reason and illustrate with a diagram on how the hash function can be embedded in the message from a sender to a receiver.

- HMAC (Hash-based Message Authentication Code) using SHA-256
- It can ensure data integrity and authentication to prevent attackers from modifying data transmitted between clients and the server.
- HMAC is computationally less expensive compared to digital signatures, making it ideal for high-volume transactions on an e-commerce website.
- Since it is using a shared secret key, only the sender and receiver know the key, ensuring that data is not tampered with by attackers.



Secret Key, K

K1 + pad

K2 + pad

K2 + pad

Message

Hash1

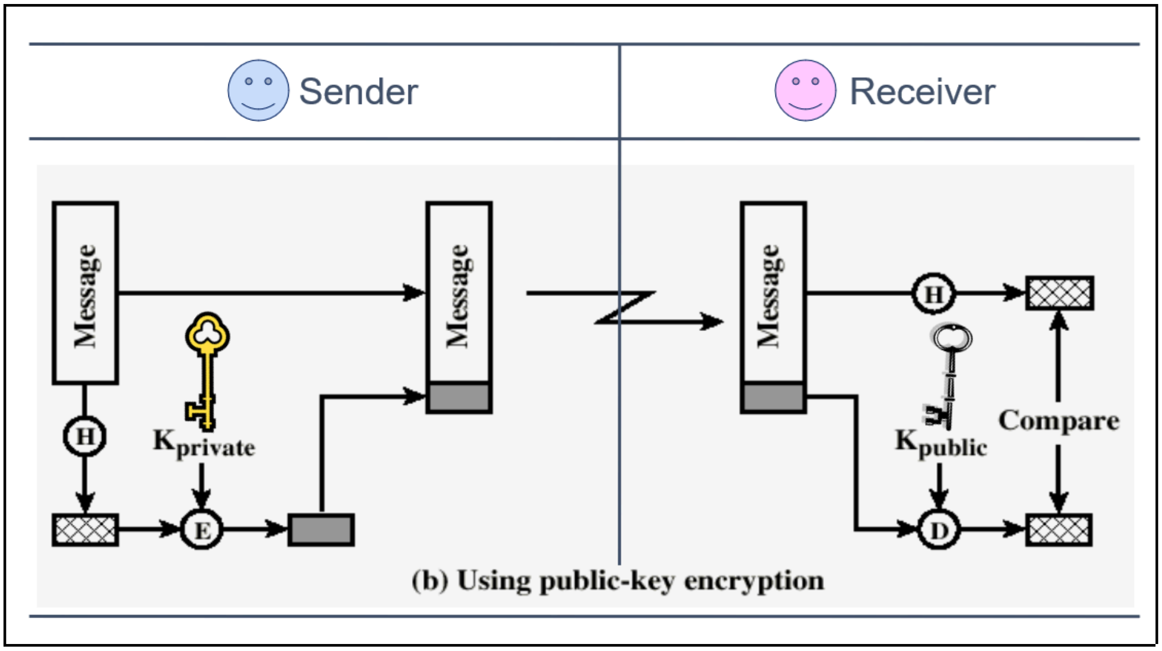
K1 + pad

Hash1

Hash2

HMAC

One-way hash function with public key encryption



(b) Using public-key encryption

2. State ONE (1) purpose of secure hash functions and provide TWO (2) examples of how the secure hash functions are being applied.

- Purpose:
  - The secure hash functions can provide proof of data integrity by providing a verifiable fingerprint of the data.
  - A one-way hash function H() operates on an arbitrary length input message M, returning h=H(M).
- Examples:
  - Password storage (authentication systems)
    - Secure hash functions are used to hash passwords before storing them in databases.
    - When a user logs in, the system hashes the entered password and compares it with the stored hash to verify authenticity.
    - e.g. Websites store hashed passwords instead of plaintext passwords to prevent attackers from retrieving user credentials in case of a data breach.
  - Digital Signatures (data integrity and authentication)
    - Cryptographic hash functions are used to create a hash of a document or message, which is then encrypted with a private key to form a digital signature.
    - The recipient can verify the signature using the sender's public key to ensure the document is authentic and hasn't been tampered with.
    - e.g. Digital signatures are used in SSL/TLS certificates, ensuring secure communication between web browsers and servers.

Purposes:

Intended to provide proof of data integrity, by providing a verifiable fingerprint of the data.

Example:
Unix password: Hash user password and store into database.
Integrity of downloaded file: Use hash value to determine the integrity of downloaded file.

3. Figure 1 below shows the process of a message transmitting from a sender to a receiver by using the security of Message Authentication.

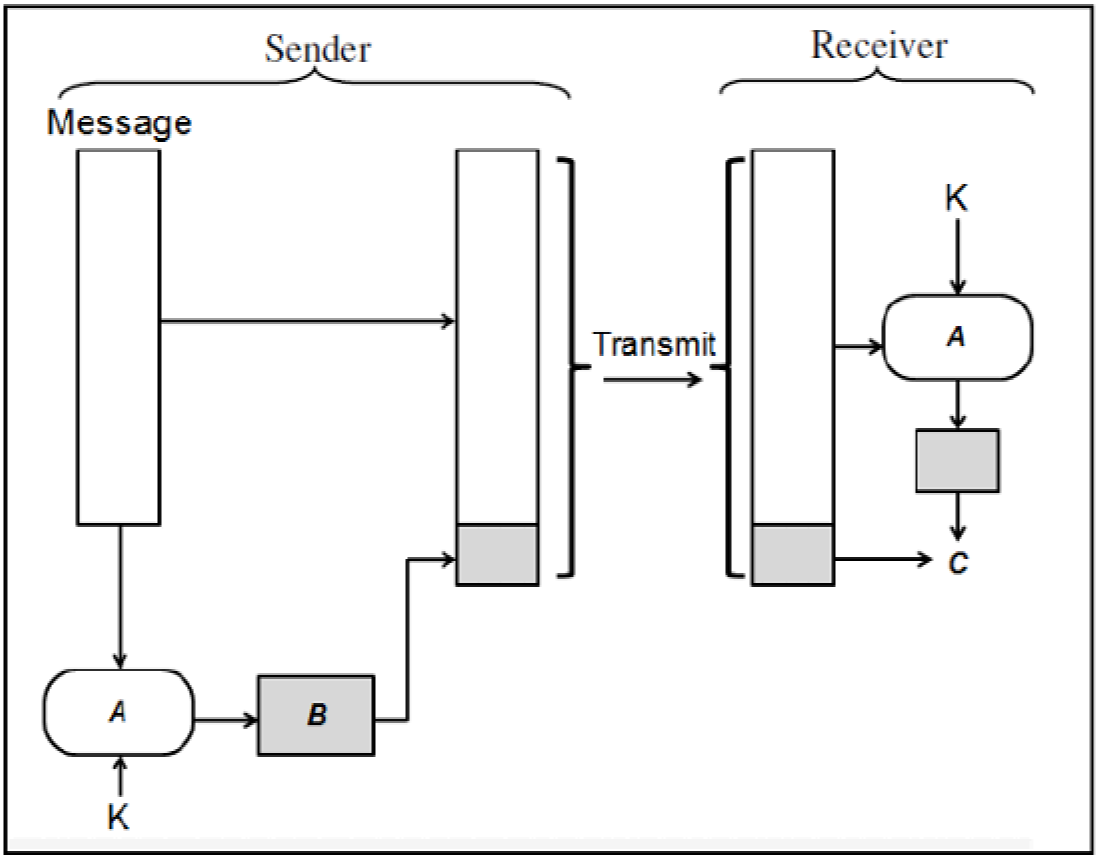


Figure 1: Message Authentication.

i. Name the component A, B, K as stated in Figure 1

- Component A: MAC (Message Authentication Code) algorithm
- Component B: MAC (Message Authentication Code)
- Component K: Secret key

ii. Component C is a process. Name the process and briefly explain the purpose of this component in Figure 1.

- The name of the process is Compare.
- It compares the MAC and the message whether they are matched.

C: Comparing process
Receiver will compare both the original MAC (Message Authentication Code) with the MAC (Message authentication Code) embedded in the message. If both MACs are the same, the message is valid and not edited by intruders, whereas if the MAC are not the same, the message is invalid and edited by intruders.

iii. With the aid of Figure 1, briefly describe the steps of the Message Authentication process from the sender to the receiver.

Step 1: Message Creation (Sender Side)

- The sender prepares a message to be transmitted to the receiver.

Step 2: Hashing with a Secret Key (HMAC Generation)

- The sender applied a hash function to the message using a secret key (K).
- This generates a Message Authentication Code (MAC), ensuring integrity and authenticity.

Step 3: MAC Attachment

- The sender attaches the MAC to the message.
- The message + MAC are then transmitted to the receiver.

Step 4: Message and MAC Reception

- The receiver receives both the message and the MAC.

Step 5: MAC Recalculation (Receiver Verification)

- The receiver applied the same hash function to the received message using the shared secret key (K).
- This generates a new MAC (C).

Step 6: MAC Comparison

- The receiver compares the newly computed MAC (C) with the received MAC.
- If they match, the message is authentic and unaltered.
- Else, the message has been tampered with or is from an untrusted sender.

Step 1: Sender shares the secret key with the receiver in advance before the message is transmitted via the Internet.
Step 2: Sender uses MAC algorithm & secret key to generate MAC.
Step 3: The MAC will be embedded into the message.
Step 4: Send the message via the Internet.
Step 5: Receiver received the message.
Step 6: Receiver uses the shared secret key and MAC algorithm to generate MAC.
Step 7: Receiver will compare the generated MAC with the embedded MAC in the message.

4. Figure 1 below shows the process of a message transmitting from a sender to a receiver by using the security of Message Authentication.

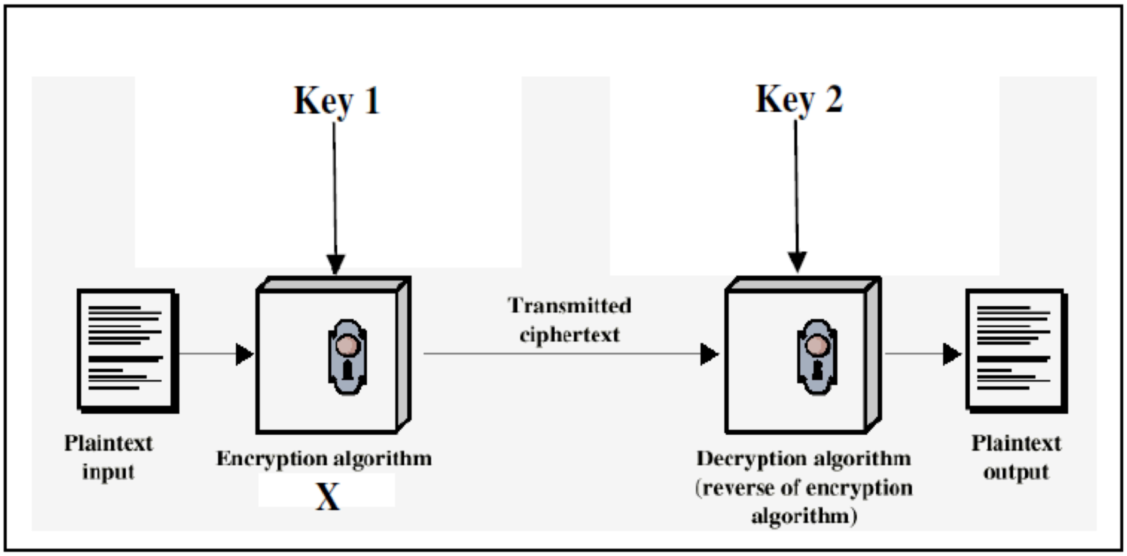


Figure 1: Encryption using Public-key cryptography.

By referring to Figure 1, answer the questions below

i. State who is the owner for Key 1 and the owner for Key 2.

Key 1’s owner: Bob
Key 2’s owner: Alice

ii. What type of key that is used in Key 1 and Key 2?

Key 1’s type: Public key
Key 2’s type: Private key

iii. By referring to X, state ONE (1) suitable example of encryption algorithm that can be used in the encryption of public-key cryptography.

X: RSA algorithm

iv. Briefly describe FIVE (5) examples that use public-key cryptography in the Internet environment.

Digital Cheque
Contract document

Credit card payment
Any confidential email or document. (e.g. Government documents / Court documents / Police investigation documents, etc)
Digital signature

Tutorial 4

1. What problems were Kerberos designed to address?

- Kerberos provides a centralized authentication server to authenticate users to servers and servers to users.
- It relies on conventional encryption, making no use of public-key encryption.

- The problem that Kerberod addresses is this: Assume an open distributed environment in which users at workstations wish to access services on servers distributed throughout the network. We would like for servers to be able to restrict access to authorized users and to be able to authenticate requests for service. In this environment, a workstation cannot be trusted to identify its users correctly to network services.

2. What are the three threats associated with user authentication over a network or Internet?

- User impersonation
  - A dishonest user may pretend to be another user from the same workstation.
- Network address impersonation
  - A dishonest user can change the network address of his or her workstation to impersonate another workstation.
- Eavesdropping, replay attack, DOS and so on
  - Attackers may try their best to access network service by mounting different attacks.

- A user may gain access to a particular workstation and pretend to be another user operating from that workstation.
- A user can change the network address so that the requests sent from the altered workstation appear to come from the impersonated workstation,
- A user may eavesdrop on exchanges and use a replay attack to gain entrance to a server or to disrupt operations.

3. What entities constitute a full-service Kerberos environment?

- Kerberos authentication server (AS)
  - A centralized trusted authentication server for the whole system, who issues long lifetime tickets.
- Ticket-granting servers (TGS)
  - Issue short lifetime tickets.
- Service server (S)
  - Provide different services.
- Clients (C)
  - Users or devices that request access to services by authenticating

themselves through the Kerberos system.

- Key Distribution Center (KDC)
  - A combination of the Authentication Server (AS) and Ticket-Granting Server (TGS), responsible for issuing tickets and session keys.
- User Credentials
  - Includes user ID and password, which are used to generate encryption keys for secure communication.
- Tickets
  - Kerberos uses tickets to authenticate users without sending passwords over the network.
- Authenticators
  - Temporary credentials used to verify the authenticity of a client request when accessing a service

- A full-service kerberos environment consists of a Kerberos server, a number of clients, and a number of application servers.

4. In the context of Kerberos, what is a realm?

A realm is a logical network or administrative domain within which Kerberos authentication is managed. It defines a boundary where a single Key Distribution Center (KDC) (which includes the Authentication Server (AS) and Ticket-Granting Server (TGS)) handles authentication for users and services.

Key Aspects of a Kerberos Realm

- Unique name
  - Each realm has a unique identifier, usually written in uppercase.
- Authentication scope
  - A realm consists of users, services and servers that trust the same KDC.
- Multiple realms
  - Large organizations may use multiple realms, each managing authentication for different departments or subsidiaries.
- Inter-realm authentication
  - Kerberos supports inter-realm authentication, allowing users from one realm to authenticate and access services in another realm through trust relationships.

- A realm is an environment in which:
  - The Kerberos server must have the user ID (UID) and hashed password of all participating users in its database. All users are registered with the Kerberos server.
  - The Kerberos server must share a secret key with each server. All servers are registered with the Kerberos server.

5. What is the purpose of the X.509 standard?

- X.509 standard is used for public key infrastructure (PKI) and defines a framework for creating and managing digital certificates to enable secure authentication, encryption and digital signatures over networks.
- Public key authentication
    - X.509 certificates bind a user's or entity's public key to their identity, verified by a Certificate Authority (CA).
- Secure Communication
    - Used in SSL/TLS, S/MIME, IPSec and other protocols to ensure encrypted and authenticated data exchanges.
- Digital Signatures
    - Provides a way to verify the authenticity and integrity of messages, documents and transactions.
- Certificate Revocation
    - Defines mechanisms like Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) to revoke compromised certificates.

- X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. The directory may serve as a repository of public-key certificates. Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority. In addition, X.509 defines alternative authentication protocols based on the use of public-key certificates.

6. Give reasons why is an X.509 certificate revoked?

- Private key compromise
    - If a user's private key is compromised or stolen, the certificate is no longer secure and must be revoked.
- User no longer certified by the CA
    - If a user or entity is no longer trusted or authorized by the Certificate Authority (CA), their certificate must be revoked.
- CA's certificate is compromised
    - If the CA's private key is compromised, all certificates issued by that CA could be untrustworthy, requiring revocation.
- Incorrect or fraudulent certificate issuance
    - If a certificate was issued based on false information or an error, it must be revoked.

- The user's private key is assumed to be compromised.
- The user is no longer certified by this CA.
- The CA's certificate is assumed to be compromised.

Past Year Questions

1. What is Kerberos? State THREE (3) problems which would be encountered in Kerberos version 4.

- Kerberos is a centralized authentication system that allows users to securely access services on a distributed network.
- It uses symmetric key cryptography and relies on a trusted Authentication Server (AS) to authenticate users and services.
- Problems encountered
    - Single realm limitation
        - Kerberos Version 4 is restricted to a single realm, meaning it cannot handle authentication across multiple administrative domains.
    - Encryption system dependence (DES only)
        - Kerberos Version 4 relies on Data Encryption Standard (DES), which has become weak due to advancements in computing power.
    - Ticket lifetime issues
        - Tickets in Version 4 have fixed lifetimes, which can cause security risks.
        - If too short, users must re-authenticate frequently, leading to inconvenience.
        - If too long, attackers have more time to steal and reuse stolen tickets (replay attacks).

- Kerberos provides a centralized authentication server to authenticate users to servers and servers to users.
- 3 problems:
    - Lifetime associated with the ticket-granting ticket.
    - If time is too short -> repeatedly asking for password.
    - If time is too long -> greater opportunity to reply.

2. Explain the term Certificate Authority (CA).

- Anyone can be a CA, but must be trusted.
- It is a trusted third party, which trusted by the user community.
- CA is to proof the user/system public key that claim to be true.

- It is a trusted third party to prove the user's public key that is claimed to be True. Example, VeriSign, GTE, US. Postal Service.

3. Kerberos is an authentication service designed for use in a distributed environment. With the aid of a diagram, describe how the Kerberos operates.

Step 1: User authentication request

- The Client (C) sends a request to the Authentication Server (AS) with the user ID.

Step 2: Authentication server response

- The AS verifies the user's identity and issues a Ticket-Granting Ticket (TGT), encrypted using the user's password-derived key.

Step 3: Request for Service Ticket

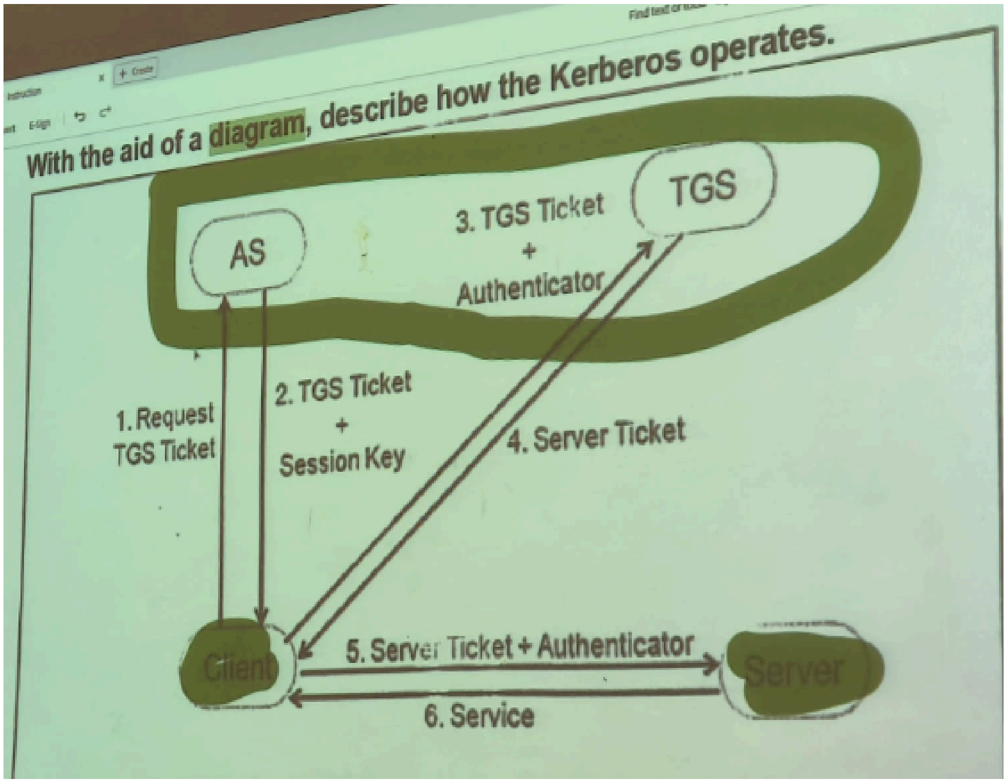
- The client sends the TGT to the Ticket-Granting Server (TGS) along with the requested service ID.

Step 4: Service Ticket Issuance

- The TGS verifies the TGT and provides a service ticket, which is encrypted with the service's secret key.

Step 5: Accessing the Service

- The client presents the service ticket to the Service Server (S).
- The service verifies the ticket and grants access.



With the aid of a diagram, describe how the Kerberos operates.

Tutorial 5

1. What is R64 conversion?

- R64 conversion is also known as Base64, it is a method of encoding binary data into a string of printable ASCII characters.
- It is commonly used in network protocols such as MIME and PGP to ensure the binary data can be transmitted over text-based systems without corruption or misinterpretation.

- R64 converts a raw 8-bit binary stream to a stream of printable ASCII characters. Each group of three octets of binary data is mapped into our ASCII characters.

2. Why is R64 conversion useful for an e-mail application?

- Compatibility and robustness
  - It allows binary data like attachments and images to be transmitted through text-only protocols to ensure the compatibility with older email systems.
- Avoiding corruption
  - It can prevent data corruption by avoiding the stripping of the 8th bit of bytes, which can occur in non-8-bit clean environments.
- Embedding images
  - It enables embedding small images directly into HTML emails using base64 data URIs, which helps avoid issues with blocked external images.

- When PGP is used, at least part of the block to be transmitted is encrypted. If only the signature service is used, then the message digest is encrypted (with the sender's private key). If the confidentiality service is used, the message plus signature (if present) are encrypted (with a one-time symmetric key). Thus, part or the entire resulting block consists of a stream of arbitrary 8-bit octets. However, many electronic mail systems only permit the use of blocks consisting of ASCII text.

3. Why is segmentation and reassembly function in PGP needed?

- E-mail facilities are restricted to a maximum message length of 50,000 octets.
- Thus, the longer messages must be broken up into segments, which are mailed separately.
- PGP will automatically subdivides a message that is too large into segments small enough to send via e-mail.
- After all other processing including radix-64 conversion, the segmentation will be executed.
- The receiver strip of all e-mail headers and reassemble the block.

- E-mail facilities often are restricted to a maximum message length.

4. What is MIME?

- MIME is a standard that extends the format of email messages to support text in character sets other than ASCII, as well as attachments of audio, video, images and application programs.
- It allows for the exchange of multimedia content over email and other internet protocols like HTTP.

- MIME is an extension to the RFC 822 framework that is intended to address some of the problems and limitations of the use of SMTP (Simple Mail Transfer Protocol) or some other mail transfer protocol and RFC 822 for electronic mail.

5. What is S/MIME?

- S/MIME is known as Secure/Multipurpose Internet Mail Extension.
- It is a standard for encrypting and digitally signing email messages using public-key cryptography.
- It protects the content of emails from unauthorized access via encryption.
- It verifies the sender's identity and ensures message integrity using digital signatures for preventing tampering during transmission.

- S/MIME (Secure/Multipurpose internet Mail Extension) is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security.

Past Year Questions

1. Pretty Good Privacy (PGP) provides FIVE (5) services that are essential to email security. Briefly explain these FIVE (5) services and provide each with ONE (1) algorithm example.

- Authentication
  - It enables the receiver to verify the integrity of the received message via checking the message hash and hash extracted from digital signature.
  - Algorithm example: RSA / SHA
- Confidentiality
  - It allows for encrypting messages before sending and decrypting messages after received to prevent unauthorized party from accessing the messages in insecure channel.
  - Algorithm example: RSA
- Compression
  - It compresses the message after applying the signature but before encryption.
  - It can save the space for both email transmission and file storage.
  - Algorithm example: ZIP
- E-mail compatibility
  - It encode the raw binary data into printable ASCII characters since email was designed only for text.
  - Thus, most of the type of content can be sent out using email including image, audio, video attachments.
  - Algorithm example: Radix-64 algorithm
- Segmentation and Reassembly
  - It breaks the large message into segments small enough to send via e-mail since e-mail facilities often are restricted to a maximum message length of 50,000 octets.
  - Algorithm example: PGP own algorithm.

- Authentication
  - The assurance that the communicating entity is the one that it claims to be
  - Example: Digital Signature

- Confidentiality
    - The protection of data from unauthorized disclosure.
    - Example: Message encryption
- Compression
    - Compresses the message after applying the signature but before encryption. This has the benefit of saving space both for e-mail transmission & for file storage.
    - Example: Zip file
- E-mail compatibility
    - Many e-mail systems only permit the use of blocks consisting of ASCII text. To accommodate this restriction, PGP provides the service of converting its binary stream to a stream of printable ASCII characters.
    - Example: Radix-64 conversion
- Segmentation & Reassembly
    - PGP automatically subdivides a message that is too large into segments small enough to send via e-mail. This is to ease the transmitting process of the message.
    - Example: Done independently by PGP application.

2. Pretty Good Privacy (PGP) provides a confidentiality and authentication service that can be used for e-mail and file storage applications. 5 operational services such as Authentication, Confidentiality, Compression, Email-compatibility and Segmentation & Reassembly are important to PGP.

i. Give THREE (3) reasons to support the importance of Segmentation & Reassembly in Pretty Good Privacy (PGP).

- Handling e-mail length restrictions
    - E-mail facilities have maximum message length limits, often around 50,000 octets only.
    - Thus, PGP can break the large messages into smaller segments that can be sent separately to ensure all parts of the message are delivered using segmentation and reassembly.
- Efficient transmission
    - PGP can ensure that even large files can be transmitted efficiently over networks with size constraints via segmenting messages.
    - This can reduce the risk of transmission failure due to size limitations.
- Reassembly for integrity
    - At the receiving end, PGP will reassemble the segments into the original message for ensuring the message is complete and intact.
    - This is important for maintaining the integrity of encrypted and signed messages.

- E-mail facilities often are restricted to a maximum message length of 50,000 octets.
- Longer messages must be broken up into segments, which is mailed separately.
- PGP automatically subvides a message that is too large into segments small enough to send via e-mail.
- The segmentation is done after all of other processing, including the radix-64 conversion.

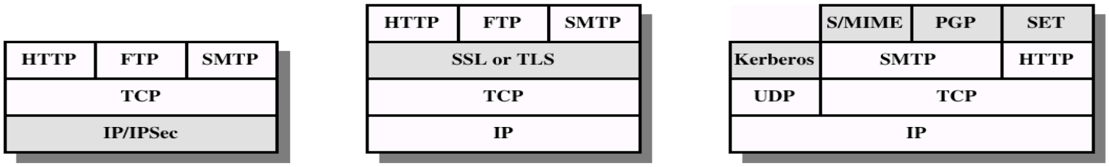
- The receiver strip of all e-mail headers and reassemble the block.

ii. Why does Pretty Good Privacy (PGP) generate a signature before applying compression?

- Storage and verification efficiency
  - PGP allows users to store only the uncompressed message along with the signature via signing the uncompressed message.
  - Thus, the message will not need to be compressed again for future verification with the signature.
- Non-deterministic compression algorithm
  - Since PGP's compression algorithm is non-deterministic, different implementations may produce different compressed outputs.
  - Signing the uncompressed message can prevent the need for all implementations to use the same compression version.
  - This can ensure the interoperability and consistent signature verification.

- The signature that embedded in the message is more secure.
- The size of the message with signature can be reduced after compression.

Tutorial 6



(a) Network Level (b) Transport Level (c) Application Level

1. What are the advantages of each of the three approaches shown in above figure?

Advantage of IPSec

- It is transparent to end users and applications and provides a general-purpose solution.

Advantage of SSL or TLS

- It is transparent to applications or embedded in specific packages.

Advantage of application-specific security services

- They are embedded within a particular application.
- The service can be tailored to the specific needs to a given application.

The advantage of using IPSec is that it is transparent to end users and applications and provides a general-purpose solution. Further, IPSec includes a filtering capability so that only selected traffic need incur the overhead of IPSec processing.

The advantage of using SSL is that it makes use of the reliability and flow control mechanisms of TCP.

The advantage of application-specific security services is that the service can be tailored to the specific needs of a given application.

2. What is the difference between an SSL connection and an SSL session?

SSL connection

- A connection is a transport that provides a suitable type of service.
- Every connection is associated with one session.
- For example, peer to peer relationship.

SSL session

- It is an association between a client and a server.
- Sessions are created by the Handshake Protocol.
- Sessions define a set of cryptographic security parameters, which can be shared among multiple connections.

- Connection: A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session.
- Session: An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

3. What services are provided by SSL Record Protocol?

Confidentiality

- The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.

Message integrity

- The Handshake Protocol also defines a shared key that is used to form a messgae authentication code (MAC).

Confidentiality

- The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.

Message integrity

- The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

4. What steps are involved in the SSL Record Protocol transmission?

Phase 1: Establish security capabilities

- Initiates a logical connection and establishes the security capabilities that will be associated with it.
- Client initiates the exchange by sending a client_hello message.

Phase 2: Server authentication and key exchange

- Server sends its certificate if it needs to be authenticated.
- The message contains one or a chain of X.509 certificates.
- The certificate message is required for any agreed-on key exchange method except anonymous Diffie-Hellman.

Phase 3: Client authentication and key exchange

- Upon receipt of the server_done message, the client verifies that the service provided a valid certificate and check that the server_hello parameters are acceptable.
- If all is satisfactory, the client sends one or more messages back to the server.

Phase 4: Finish

- Client sends a change_cipher_spec message and copies the pending CipherSpec into the current CipherSpec.
- The client will then immediately sends the finished message under the new algorithms, keys and secrets.

Fragmentation; compression; add MAC; encrypt; append SSL record header.

5. List & briefly define the principal categories of SET participants.

Cardholder

- The authorized holder of a payment card.

Merchant

- The seller offering goods or services and accepting payment cards.

Issuer

- A financial institution issuing the payment card and responsible for the cardholder's debt.

Certificate Authority

- Issues digital certificates to ensure trust and security among participants.

Acquirer

- A financial institution processing payment authorizations and facilitating funds transfer to the merchant.

Payment Gateway

- Acts as an interface between the merchant and the payment networks for authorization and payment processing.

Cardholder: A cardholder is an authorized holder of a payment card (e.g. MasterCard, Visa) that has been issued by an issuer. E.g. Customer.

Merchant: A merchant is a person or organization that has goods or services to sell to the cardholder. E.g. Amazon.com

Issuer: This is a financial institution, such as a bank, that provides the cardholder with the payment card. E.g. Maybank

Acquirer: This is a financial institution that establishes an account with a merchant and processes payment card authorizations and payments. The acquirer provides authorization to the merchant that a given card account is active and that the proposed purchase does not exceed the credit limit. the acquirer also provides electronic transfer of payments to the merchant's account. E.g. Paypal.com

Payment gateway: This is a function operated by the acquirer or a designated third party that processes merchant payment messages. The payment gateway interfaces between SET and the existing bankcard payment networks for authorization and payment functions.

Certification authority (CA): This is an entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants and payment gateways. The success of SET will depend on the existence of a CA infrastructure available for this purpose.

6. What is the dual signature and what is its purpose?

- Dual signature is a cryptographic mechanism designed to ensure both privacy and integrity during online transactions.
- It ensures that the merchant receives only the OI (details of the order) without accessing the customer's payment details.
- It also make sure the bank receives only the PI (payment details) without knowing the specifics of the order.
- Thus, both pieces of information are securely linked to prevent disputes, confirming that a specific payment is tied to a specific order.

- A dual signature is used to sign two concatenated documents each with its own hash code.
- The purpose of the dual signature is to link two messages that are intended for two different recipients. In this case, the customers want to send the order information (OI) to the merchant and the payment information (PI) to the bank. The merchant does not need to know the customer's credit card number, and the bank does not need to know the details of the customer's order.

Past Year Questions

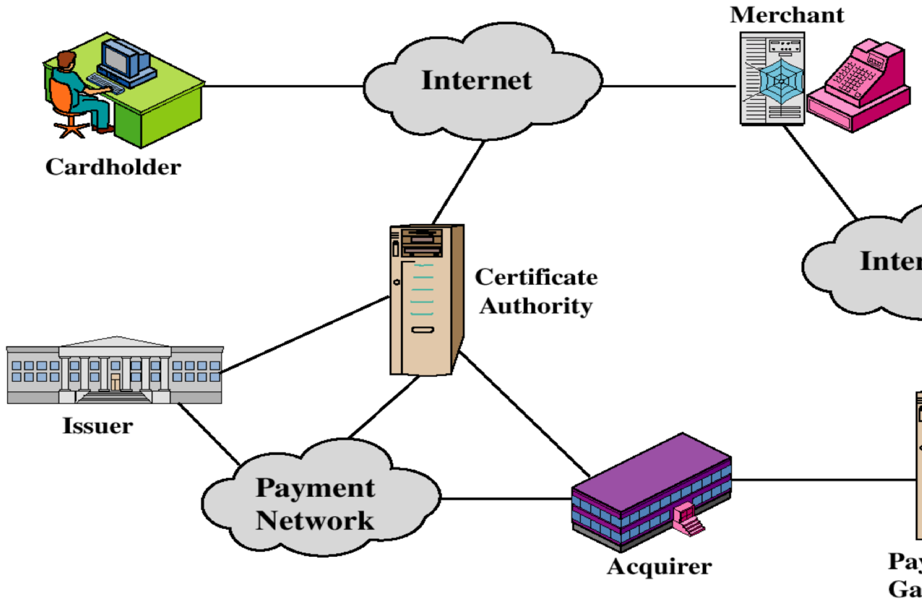
1. “Secure Electronic Transactions is a payment system.” Do you agree with the above statement? Justify your answer.

- No
- It is an open encryption and security specification to protect credit card transaction on the Internet.
- It allows users to employ the existing credit card infrastructure on an open network, such as Internet.
- It provides a framework for encrypting sensitive data, authenticating parties and ensuring confidentiality during electronic payments.
- It also uses digital certificates and signatures to secure transactions.

No. An open encryption and security specification to protect credit card transaction on the Internet, whcih provides a secure communication channel in a transaction.
Provides trust by the use of X.509v3 digital certificates.
Ensures privacy (because the information is only available to parties in a transaction when and where necessary.)

2. Secure Electronic Transactions (SET) is an open encryption and security specification to protect credit card transactions on the Internet. it provides a secure communication channel in a transaction, trusts by the use of X.509 v3 digital certificates and ensures privacy.

(i) With the aid of a diagram, illustrate Secure Electronic Transactions (SET) with its participants.



(ii) Certificate Authority (CA) is one of the Secure Electronic Transactions (SET) participants. What will happen if Certificate Authority (CA) is removed?

Loss of trust

- CAs play a crucial role to verify the identities of participants and ensure that only authorized parties can engage in transactions.
- If it is removed, the trust between these entities would be compromised, making it difficult to verify identities securely.

Non-repudiation issues

- CAs can ensure non-repudiation through digital signatures, preventing parties from denying involvement in a transaction.
- Without a CA, the proving action of the authenticity of transactions would become challenging.

Certificate Authority (CA):
CA is an entity that is trusted to issue X.509v3 public-key certificates for cardholder, merchants and payment gateways.
The success of SET will depend on the existence of a CA infrastructure available for this purpose.
Without CA, cardholder and merchant will not able to verify authenticity of each other. The same goes for transaction between Acquirer and issuer.

Tutorial 7

1. Give examples of applications of IPSec.

- Secure branch office connectivity over the network:
  - A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.
- Secure remote access over the Internet:
  - An end user whose system is equipped with IP security protocols can make a local call to an Internet service provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.
- Establishing extranet and intranet connectivity with partners:
  - IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.
- Enhancing electronic commerce security:
  - Even though some Web and electronic commerce application shave built-in security protocols, the use of IPSec enhances that security.

2. What services are provided by IPSec?

Access control; connectionless integrity; data origin authentication; rejection of replayed packets (a form of partial sequence integrity); confidentiality (encryption) and limited traffic flow confidentiality.

3. What is the difference between a transport mode and tunnel mode?

- Transport mode provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload or an IP packet.
- Tunnel mode provides protection to the entire IP packet.

4. What is a replay attack?

A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence.

5. Where are the basic approaches to bundling SAs?

- Transport adjacency:
  - Refers to applying more than one security protocol to the same IP packet, without invoking tunneling. This approach to combining AH and ESP allows for only one level of combination; further nesting yields no added benefit since the processing is performed at one IPSec instance: the (ultimate) destination.
- Iterated tunneling:
  - Refers to the application of multiple layers of security protocols effected through IP tunneling. This approach allows for multiple levels of nesting, since each tunnel can originate or terminate at a different IPSec site along the path.

6. What are the roles of the Oakley key determination protocol and ISAKMP in IPSec?

ISAKMP by itself does not dictate a specific key exchange algorithm; rather, ISAKMP consists of a set of message types that enable the use of a variety of key exchange algorithms.

Oakley is the specific key exchange algorithm mandated for use with the initial version of ISAKMP.

Past Year Questions

1. IP Security (IPSec) provides a set of security algorithms and a general framework that allows a pair of communicating entities to use whichever algorithms that provides appropriate security for the communiation.
   i. Describe TEO (2) benefits that are provided by the IPSec.

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

ii. What are the THREE (3) features that are provided by the IPSec?

- A router or neighbor advertisement comes from an authorized router.
- A redirect message comes from the router to which the initial packet was sent.
- A routing update is not forged.

iii. Give ONE (1) example of application of the IPSec.

- Secure branch office connectivity over the Internet (VPN).
- Secure remote access over the Internet.
- Establishing extranet and intranet connectivity with partners.
- Enhancing electronic commerce security.

Tutorial 8

1. What two common techniques are used to protect a password file?

- One-way encryption: The system stores only an encrypted form of the user's password. When the user presents a password, the system encrypts that password and compares it with the stored value. In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the encryption function and in which a fixed-length output is produced.
- Access control: Access to the password file is limited to one or a very few accounts.

2. What are three benefits that can be provided by an intrusion detection system?

- If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, the less the amount of damage and the more quickly that recovery can be achieved.
- An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions.
- Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

3. What is the difference between statistical anomaly detection and rule-based intrusion detection?

- Statistical anomaly detection involves the collection of data relating to the behavior of legitimate users (insider) over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.
- Rule-Based Detection involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder (inside / outsider).

4. What metrics are used for profile-based intrusion detection?

5. What is the difference between rule-based anomaly detection and rule-based penetration identification?

- With rule-based anomaly detection, historical audit records are analyzed to identify usage patterns and to generate automatically rules that describe those patterns. Rules may represent past behavior patterns of users, programs, privileges, time slots, terminals and so on. Current behavior is then observed, and each transaction is matched against the set of rules to determine if it conforms to any historically observed pattern of behavior.

- Rule-based penetration identification uses rules for identifying known penetrations or penetrations that would exploit known weaknesses. Rules can also be defined that identify suspicious behavior, even when the behavior is within the bounds of established patterns of usage. Typically, the rules used in these systems are specific to the machine and operating system. Also, such rules are generated by "experts" rather than by means of an automated analysis of audit records.

6. What is a salt in the context of UNIX password management?

The salt is combined with the password at the input to the one-way encryption routine.

Past Year Questions

1. (i) List and briefly describe THREE (3) classes of intruders.

- Masquerader - unauthorized individual who exploits legitimate user's account (outsider).
- Misfeasor - legitimate user, who misuses his or her private privileges (insider).
- Clandestine user - individual who seizes supervisory control and uses it to evade auditing or access controls (insider or outsider)

(ii) Most of the time, intruder will begin to access a protected file by adopting Password Guessing Techniques. List FOUR (4) techniques of guessing passwords.

- Try default passwords.
- Try all short words, 1 to 3 characters long.
- Try all the words in an electronic dictionary (60,000).
- Collect information about the user's hobbies, family names, birthday, etc.
- Try the user's phone number, social security number, street address.
- Try all license plate numbers (MUP103).
- Use a Trojan horse.
- Tap the line between a remote user and the host system.

(iii) In your opinion, why is it so crucial to understand the behavior of an intruder? Provide TWO (2) reasons to support your answer.

By understanding the intruder behavior:

- We can trace the intruder's activities easily.
- We can invent better security applications or technologies to countermeasures the intruder attack.

(iv) Do you agree that an internal intruder is much more dangerous than an outsider intruder? Justify your answer.

- Yes
  - Because the intruder knows very well about the company framework and architecture of the system.
  - Because the intruder is able to access into the system easily without easily trace by the organization.
- No
  - Because the intruder have better resources / technology to enter into the system organization.
  - Because the intruder cooperate with the internal staff of the organization.

(v) Based on your answer to Q3.(a)(iv), identify and describe the suitable intrusion detection approach that can counter the intruder attack. Answer depends to Q3.(a).(iv)

- Yes
  - Rule based detection
- No
  - Rule based detection
  - Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.
  - Anomaly detection (rules detect deviation in behavior pattern).
  - Penetration identification (searches for suspicious behavior).

2. i. Honeypots is a relatively recent innovation in intrusion detection technology. Describe THREE (3) objectives of Honeypots.

- Diver an attacker from accessing the critical systems.
- Collect information about the attacker's activity.
- Encourage the attacker to stay on the system long enough for.

ii. What are the TWO (2) techniques to achieve Honeypots objectives?

- Systems are filled with fabricated information designed to appear valuable but that a legitimate user will not access. Thus, any access to the honeypot is suspicious.
- Use monitoring tools and event logs in the system that detects such accesses and collects information about the attacker's activities.

Tutorial 9

1. List three design goals for a firewall.

Design goals:

a. All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall).
b. Only authorized traffic (defined by the local security policy) will be allowed to pass.
c. The firewall itself is immune to penetration (use of trusted system with a secure operating system).

2. List four techniques used by firewalls to control access and enforce a security policy.

- Service control: Determines the types of Internet services (e.g. web or email service) that can be accessed, inbound or outbound.
- Direction control: Determines the direction in which particular service requests are allowed to flow.
- User control: Controls access to a service according to which user is attempting to access it. (e.g. applied to incoming traffic from external users).
- Behavior control: Controls how particular services are used (e.g. filter e-mail to eliminate spam).

3. What is the difference between a packet-filtering router and a stateful inspection firewall?

- A traditional packet filter makes filtering decisions on an individual packet basis and does not take into consideration any higher layer context.
- A stateful inspection packet filter tightens up the rules for TCP traffic by creating a directory of outbound TCP connections. There is an entry for each currently established connection. The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.

4. What is an application-level gateway and circuit-level gateway?

- An application-level gateway, also called a proxy server, acts as a relay of application-level traffic.
- A circuit-level gateway does not permit an end-to-end TCP connection; other without examining the contents. The security function consists of determining which connections will be allowed.

5. In the context of access control, what is the difference between subject and an object?

- A subject is an entity capable of accessing objects. Generally, the concept of subject equates with that of process. Any user or application actually gains access to an object by means of a process that represents that user or application.
- An object is anything to which access is controlled. Examples include files, portions of files, programs and segments of memory.

6. What is the difference between an access control list and a capability ticket?

- For each object, an access control list lists users and their permitted access rights.
- A capability ticket specifies authorized objects and operations for a user.

7. What are two rules that a reference monitor enforces?

The monitor enforces the security rules (no read up, no write down).

8. What properties are required of a reference monitor?

Properties of the Reference Monitor:

- Complete mediation: Security rules are enforced on every access.
- Isolation: The reference monitor and database are protected from unauthorized modification.
- Verifiability: The reference monitor's correctness must be provable (mathematically).

<u>Past Year Questions</u>

1. What are the THREE (3) general limitations that are faced in a firewall?

- Firewalls cannot protect against attacks that bypass the firewall.
    - Internal systems may have dial-out capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters.
- The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
- The firewall cannot protect against transfer of virus-infected programs or files.

2. Figure 4 shows one of the firewall types.

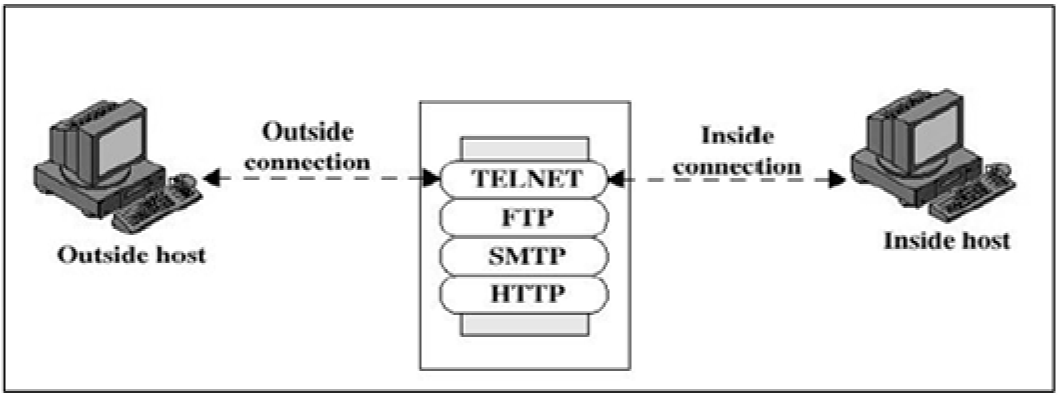


Figure 4: Firewall

i. Identify and briefly describe what type of firewall is shown in Fig 4.

- Application-level Gateway
- Also called proxy server
- Acts as a relay of application-level traffic

ii. Give (2) advantages and (1) disadvantage for this type of firewall.

Advantages [Any 3 answers below]

- Higher security than packet filters
- Only need to scrutinize a few allowable applications
- Easy to log and audit all incoming traffic

Disadvantage

- Additional processing overhead on each connection (gateway as splice point) - gateway must examine and forward all traffic in both directions.

Tutorial 10

1. What are the differences between virus and malicious programs? Provide each with an example.

> - Computer "Viruses: and related programs have the ability to replicate themselves on an ever increasing number of computers. They originally spread by people sharing floppy disks. Now they spread primarily over the Internet (a "Worm").
> - Other "Malicious Programs" may be installed by hand on a single machine. They may also be built into widely distributed commercial software packages. These are very hard to detect before the payload activates (Trojan Horses, Trap Door, and Logic Bombs).

2. What is the role of compression in the operation of a virus?

> A virus will perform compression to make the infected program have same size as the original program.

3. What is the role of encryption in the operation of a virus?

> A portion of the virus, generally called a mutation engine, creates a random encryption key to encrypt the remainder of the virus. The key is stored with the virus, and the mutation engine itself is altered. When an infected program is invoked, the virus uses the stored random key to decrypt the virus. When the virus replicates, a different random key is selected.

4. What are typical phase's operations of a virus or worm?

> A dormant phase, a propagation phase, a triggering phase, and an execution phase.

5. In general terms, how does a worm propagate?

> Step 1 - Search for other systems to infect by examining host tables or similar repositories of remote system addresses.
> Step 2 - Establish a connection with a remote system.
> Step 3 - Copy itself to the remote system and cause the copy to be run.

6. What is a digital immune system?

> - The system provides a general-purpose emulation and virus-detection system.
> - The objective is to provide rapid response time so that viruses can be stamped

out almost as soon as they are introduced.

- When a new virus enters an organization, the immune system automatically captures it, analyzes it, adds detection and shielding for it, removes it, and passes information about that virus to systems running a general antivirus program so that it can be detected before it is allowed to run elsewhere.

7. How does behavior-blocking software work?

Behavior-blocking software integrates with the operating system of a host computer and monitors program behavior in real-time for malicious actions. The behavior blocking software then blocks potentially malicious actions before they have a chance to affect the system.

Past Year Questions

1. The basic transformation stages of computer viruses are exactly similar to biological viruses. State and briefly explain each phase.

   1. Dominant phase - the virus is idle.
   2. Propagation phase - the virus places an identical copy of itself into other programs.
   3. Triggering phase - the virus is activated to perform the function for which it was intended.
   4. Execution phase - the function is performed.

2. List THREE (3) Advanced Antivirus Techniques. Among these techniques, which technique is the best countermeasure against malwares for an operating system in a computer? Provide ONE (1) explanation to support your answer.

   - Generic Decryption (GD)
   - Digital Immune System
   - Behavior-blocking software
   - Behavior-blocking software is the best countermeasure for an operating system in a computer because it monitors program behavior in real-time for malicious actions and blocks potentially malicious actions before they have a chance to affect the system.

3. Macro viruses are the common type of viruses that attack Microsoft Office. Briefly describe how Macro virus invades Microsoft Office files.

   The macro could run whenever the document is opened, or when a certain command is selected (Save File).

4. Briefly define each type of the malware shown below:
    a. Compression virus:

A virus will perform compression to make the infected program have the same size as the original program.

    b. Email virus:

A virus that manipulates marco virus and embedded in attachment. The email virus will send itself to everyone on the mailing list in the user's email address list.

    c. Trojan horse:

A computer program with an apparently or actually useful function that contains additional (hidden) functions that, when invoked, performs some unwanted or harmful function.

    d. Trap door:

Also known as back-door. Undocumented entry point written into a program, used to grant access without normal methods of access authentication.

Tutorial 11

1. List and describe TWO (2) widely recognised standards for managing and improving information security.

    - NIST framework provides guidelines for identifying, detecting and responding to cyberattacks.
    - ISO 27001 is a standard for establishing, implementing, maintaining and continually improving an information security management system (ISMS).

2. Describe the consequences of non-compliance with the Personal Data Protection Act (PDPA) in Malaysia.

    Non-compliance with PDPA can lead to significant legal penalties, including fines and imprisonment, loss of reputation, decreased customer trust, and potential financial losses due to litigation and settlement costs.

3. Propose improvements to an existing security policy to better address current cybersecurity threats.

    Enhancing the existing security policy could include updating acceptable use policies to cover recent technological advances such as cloud storage and IoT devices, increasing awareness training frequency, and incorporating advanced threat detection and response strategies.

4. Define "Risk Management" in the context of cybersecurity.

    Risk management in cybersecurity involves identifying, assessing and prioritizing risks followed by coordinated efforts to minimize, monitor and control the probability or impact of unfortunate events or to maximize the realization of opportunities.

5. Explain the difference between qualitative and quantitative risk assessments.

    Qualitative risk assessment uses non-numeric descriptions or categories to assess and prioritize risks, often based on expert opinions, whereas quantitative risk assessment calculates numerical probabilities and impacts, using data to estimate the frequency and costs of potential losses.

6. Describe Single Loss Expectancy (SLE), Annualised Rate of Occurrence (ARO) and Annualised Loss Expectancy (ALE) used in risk assessment. Calculate ALE if a company estimated LSE is RM1 million due to data breach and ARO is 3.

- Single Loss Expectancy (SLE) calculates the expected monetary loss every time a risk occurs.
- Annualised Risk of Occurrence (ARO) is used to determine the likelihood of a risk occurring within a year based on historical data or industry standards.
- Annualised Loss Expectancy (ALE) calculates the expected monetary loss over a one-year period.

ALE
= SLE x ARO
= RM1 million x 3
= RM3 million

7. Evaluate the effectiveness of using a risk register in managing organizational risks.

A risk register is effective as it provides a centralized document to record identified risks, their severity, and the actions to be taken. It helps in tracking the progress of risk mitigation and is crucial for communication within the organization about potential risks.

8. Compare and contrast the roles of deterrent and preventative controls in risk management.

Deterrent controls are intended to discourage potential attackers through the implication of consequences, while preventative controls aim to stop threats from occurring by directly addressing vulnerabilities.

9. Suggest THREE (3) methods to enhance data privacy by organisations to protect customers' data.

Any 3 methods:

- conducting regular data privacy impact assessments
- privacy notice to inform users about data collection and usage
- implementing stringent access controls
- regular privacy training for employees
- data minimization
- data masking using encryption techniques
- data tokenization
- and establishing a clear protocol for responding to data breaches
- understand country-specific government regulations, especially regarding data sovereignty, which dictates where data must be stored and processed

10. Justify the need for implementing strong data destruction policies at the end of the data lifecycle.

Strong data destruction policies are necessary to ensure that sensitive information is irretrievably destroyed, preventing unauthorized access and compliance issues, and protecting against identity theft and breaches, which could have legal and reputational consequences.