**Name: Gumisid, Reah Jane C. Section: BSIT-3127**

**PRELIMINARY WEEK 10**

**ANSWER THE FOLLOWING:**

**Preliminary Question:**What is the main difference between symmetric cryptography and public-key cryptography?

The **main difference** between symmetric cryptography and public-key (asymmetric) cryptography is how the keys are used:

* **Symmetric cryptography**:
  + Uses the **same key** for both encryption and decryption.
  + Both the sender and receiver must share this secret key securely.
  + It is **fast and efficient**, making it suitable for encrypting large amounts of data.
  + Example algorithms: AES, DES, ChaCha20.
* **Public-key (asymmetric) cryptography**:
  + Uses a **pair of keys**: a **public key** (shared openly) for encryption, and a **private key** (kept secret) for decryption.
  + Only the private key holder can decrypt what was encrypted with the matching public key.
  + It also enables **digital signatures** (verifying authenticity) in addition to encryption.
  + It is **slower and computationally heavier** than symmetric cryptography.
  + Example algorithms: RSA, ECC, Diffie-Hellman.

|  |  |
| --- | --- |
| **Analysis, Application, and Exploration for Week 10**  **Directions: Match the terms with its definition. Choose the correct answer from the given choices.** |  |
| Public-key cryptography SSL/TLS Symmetric cryptography Decryption key  Key management Mobile phone SIM card Bank card WiFi network Encryption key  Bulk data encryption |  |
| 1. Used to establish a shared secret key between two parties who have never Met before Public-key cryptography |  |
| 1. A combination of symmetric and public-key cryptography used for secure online transactions SSL/TLS |  |
| 1. Cryptography where the same key is used for both encryption and decryption Symmetric cryptography |  |
| 1. The key that is kept secret in public-key cryptography Decryption key |  |
| 1. The process of securely distributing and storing encryption keys Key management |  |
| 1. An example where symmetric cryptography is used with pre-installed keys Mobile phone SIM card |  |
| 1. An example where symmetric cryptography is used to secure financial transactions with pre-shared keys Bank card |  |
| 1. An example where the user manually establishes the symmetric key across devices WiFi network |  |
| 1. The public key can be used by anyone to encrypt, but only the holder of this key can decrypt Encryption key |  |
| 1. Typically done using symmetric cryptography for fast processing Bulk data encryption |  |

**Generalization for Week 10**

**ANSWER THE FOLLOWING:**

1. Explain how SSL/TLS combines both symmetric and public-key cryptography to provide secure communication in online transactions. Why is this approach beneficial?

**How SSL/TTLS combines symmetric and public-key cryptography:**

1. **Handshake with public-key cryptography**
   * When a client (like your browser) connects to a server (like a bank’s website), the server presents its **digital certificate**, which contains its **public key**.
   * The client uses this public key to securely exchange a **session key** (a symmetric key).
   * Because only the server has the matching **private key**, only it can decrypt this session key.
2. **Data transfer with symmetric cryptography**
   * Once both sides agree on the session key, all further communication (webpage requests, login credentials, payment details, etc.) is encrypted and decrypted using **symmetric cryptography**.
   * This makes the data exchange **fast and efficient**, while still being secure.

**Why this approach is beneficial:**

* **Best of both worlds**:
  + Public-key cryptography solves the **key exchange problem** (securely sharing a secret key over the internet).
  + Symmetric cryptography ensures **speed and efficiency** when encrypting large amounts of data.
* **Security against eavesdropping**: Even if someone intercepts the communication, they can’t decrypt the session key without the server’s private key.
* **Authentication**: The server’s certificate (signed by a trusted Certificate Authority) ensures you’re really talking to the legitimate website, not an impostor.
* **Performance**: Using asymmetric encryption for the whole session would be too slow. By limiting it to just the handshake, SSL/TLS stays secure *and* practical.

**Evaluation for Week 10**

1. What kind of cryptography does SSL/TLS use for key exchange?

a. Hash-based cryptography

b. A combination of symmetric and public-key cryptography

c. Only public-key cryptography

d. Only symmetric cryptography

1. What is the role of a public key in public-key cryptography?

a. It encrypts messages for any recipient.

b. It generates a symmetric key.

c. It signs data for authentication.

d. It decrypts messages.

1. What is the primary drawback of public-key cryptography?

a. It requires a pre-shared key.

b. It is slow due to heavy computation.

c. It cannot be used for online shopping.

d. It is prone to hacking.

1. Which of the following best describes how a bank card uses encryption?

a. It uses a pre-established symmetric key.

b. It generates a key for each transaction.

c. It encrypts data using hashing.

d. It uses public-key cryptography to encrypt the PIN.

1. How does SSL/TLS achieve both security and speed in encrypting data?

a. By using only symmetric cryptography

b. By using only public-key cryptography

c. By combining public-key cryptography for key exchange and symmetric

cryptography for bulk data encryption

d. By using dynamic key exchange

1. Why is symmetric cryptography suitable for mobile phone communications?

a. It requires no key management.

b. The key is pre-installed by the mobile operator.

c. It uses less data than public-key cryptography.

d. The user generates the key.

1. In what situation is symmetric cryptography commonly used?

a. For encrypting emails to strangers

b. When sending data to an unknown party

c. In online banking transactions where a key is pre-establish

d. For securing large-scale public websites

1. In public-key cryptography, what is the key that must be kept secret?

a. Symmetric key

b. Public key

c. Decryption key

d. Encryption key

1. Which of the following scenarios would public-key cryptography be most appropriate for?

a. Securing communication between two pre-established devices

b. Securing online transactions between strangers

c. Encrypting communication within a private network

d. Encrypting WiFi traffic

1. How is the symmetric key shared between a browser and an online store during a transaction?

a. It is emailed to the user.

b. It is automatically stored on the user's device.

c. The online store generates the key and sends it to the browser.

d. The browser generates the key and encrypts it using the store's public key.

**Assignment for Week 10**

Instructions: Read each sentence or phrase carefully. Choose TRUE if the statement is correct and FALSE if the statement is incorrect.

* + - 1. Symmetric cryptography uses different keys for encryption and decryption.

**FALSE**

* + - 1. Public-key cryptography is slower than symmetric cryptography due to more complex computations.

**TRUE**

* + - 1. SSL/TLS combines both symmetric and public-key cryptography for secure online transactions.

**TRUE**

* + - 1. In a WiFi network at home, the symmetric key is automatically generated by the devices connected to the network.

**FALSE**

* + - 1. Public-key cryptography is used to encrypt the bulk of the data traffic in online shopping transactions.

**FALSE**

**NAME: Gumisid, Reah Jane C. SECTION: BSIT-3127**

**Preliminary Activity for Week 11**

**ANSWER THE FOLLOWING**

**What are the two main categories of computer networks based on how the connection is established?**

A computer network enables computer systems, and their applications, to exchange information. Computer networks can be grouped in two categories depending whether the connection is established through a physical cable or not.

Wired networks refer to those networks where nodes are connected using a physical link (cable). There are many different wired network technologies. Most desktop computers can connect to wired networks using an Ethernet connection. Ethernet connections are governed by the IEEE 802.3 standard. An Ethernet cable consists of 4 pairs of copper cable and can be used to transmit voice or data as frames containing protocol information and data. Desktop workstations are generally connected to their organization network using an Ethernet connection. This kind of network is also called Local Area Networks (LAN). In order to eavesdrop an Ethernet connection, the attacker requires physical access to the Ethernet cable or the devices that are connected to the device (routers and Ethernet switches).

In a wireless (or non-wired) network, the nodes connect to each other by transmitting radio waves through the air. Most well known wireless technologies are Bluetooth, WiFi, and the various cell phone networks.

Bluetooth networks uses UHF radio waves from 2.4 to 2.485 Ghz to connect devices from just a few meters away up to 100 meters away depending on the version used. The Bluetooth Special Interest Group (SIG) at the IEEE (Institute of Electrical and Electronic Engineers) develops the Bluetooth standard. Bluetooth and similar range networks are considered Personal Area Networks (PAN) or Personal Wireless Area Networks (PWAN).

WiFi networks are specified by the IEEE 802.11 standard and operate in the 2.4GHz or 5GHz spectrum. This standard has evolved like Bluetooth, improving its range and maximum data rate over the years so that the latest standards potentially provide Gbps performance and can have a range of 100's or in some cases 1000's of meters. WiFi networks are considered within the category of Wireless LAN (WLAN) networks. They are generally present in households, public spaces and organizations to provide network and Internet access to mobile devices (laptops, smartphones, etc.).

Cellular networks are a kind of Wide Area Network (WAN) that splits the geographical space into cells. Inside each cell, at least one base station provides wireless connectivity to the nodes (cell phones and other devices) using standards based protocols typically referred to as 3G and 4G services. Base stations in different cells are connected to each other through a backhaul network, being able to provide network access to wide geographic areas. A variety of standards are available and deployed worldwide and can provide voice, data and multimedia communications over a variety of data rates and distances

**Analysis, Application, and Exploration for Week 11**

**Instruction: Read each sentence or phrase carefully, select the best answer among the choices.**

1. A category of harmful software design to infiltrate or damage systems

MALWARE

1. Used to prevent unauthorized access to or from a private network

FIREWALL

1. A wired network technology used to connect desktop computers

ETHERNET

1. Wireless network standard with ranges up to 1000 meters

WI-FI

1. A method of disguising malware as legitimate software

TROJAN HORSE

1. A form of cyberattack aimed at stealing sensitive data through deception

PHISHING

1. Wide Area Network used in cellular communication

4G

1. Protects privacy by encrypting internet connections

VPN

1. Network standard commonly used for local area network (LAN) connectivity

LAN

1. Personal Area Network technology with a range of up

to 100 meters

BLUETOOTH

**Generalization for Week 11**

**1.** Discuss the importance of employee training in maintaining network security. How can training programs help mitigate the risk of insider threats?

**Employee Training**

Sometimes external threats are successful because of an insider threat. The weakest link in data protection can be your own employees.

Ensure your employees understand network security. Your employees should be able to identify threats. They should also know who to contact to avoid a security breach.

Provide security training throughout the year, and be sure to update it. There are new security risks every day.

**1. Why employee training is important in network security**

* **Humans are the weakest link**: Even with strong firewalls, encryption, and intrusion detection, a single careless click on a phishing email can compromise the entire network.
* **Awareness of threats**: Training makes employees recognize common attacks such as phishing, social engineering, malware, and password theft.
* **Policy compliance**: Employees learn why following security policies (e.g., strong passwords, multi-factor authentication, data classification rules) is essential.
* **Incident response**: Proper training ensures employees know how to report suspicious activity quickly, reducing damage from a breach.

**2. How training mitigates insider threats**

Insider threats can be **malicious** (an employee intentionally causing harm) or **accidental** (an employee making a mistake). Training helps address both:

* **For accidental threats**:
  + Teaches safe email and web browsing practices.
  + Reinforces correct handling of sensitive data.
  + Encourages use of secure authentication methods.
  + Reduces errors like misconfigurations or unauthorized sharing.
* **For malicious threats**:
  + Helps employees understand monitoring and accountability measures, reducing the likelihood of intentional misuse.
  + Fosters a **security-first culture**, making it harder for a disgruntled insider to gain support or hide malicious activity.
  + Encourages employees to report suspicious behavior among peers.

**3. Elements of an effective training program**

* **Regular sessions** (not just one-time onboarding).
* **Interactive learning** (simulated phishing attacks, role-playing social engineering scenarios).
* **Clear communication of policies** and the reasons behind them.
* **Role-based training** (technical staff, managers, and general employees get tailored content).
* **Continuous updates** to adapt to evolving cyber threats.

**Evaluation for Week 11**

1. What type of data is referred to as "credentials" when sent over a network?

a. Documents

b. Multimedia files.

**c. Usernames and passwords**

d. Chat messages

1. Which of the following is NOT a common network security threat?

a. Phishing

**b. Network segmentation**

c. Spyware

d. Viruses

1. What is the weakest link in data protection in most organizations?

**a. Employees**

b. Router settings

c. VPN configurations

d. Firewalls

1. What does updating software help to fix?

a. Chat message errors

b. Software installation errors

**c. Security vulnerabilities**

d. Network segmentation issues

1. Why is it important to standardize software across a network?

a. To improve internet speed

b. To limit the number of devices on the network

c. To prevent users from accessing the network

**d. To ensure consistent security updates**

1. What is the main purpose of using a VPN (Virtual Private Network)?

**a. Securing network traffic over the internet**

b. Encrypting passwords only

c. Blocking unauthorized users from website

d. Speeding up data transfer

1. Which of the following is a wireless technology used to connect devices over a short distance?

a. Cable modem

b. Ethernet

**c. Bluetooth**

d. Fiber optics

1. What is malware?

**a. Malicious software designed to harm or exploit system**

b. An antivirus program

c. A type of network security

d. A network protocol

1. What frequency range does Bluetooth use?

**a. 2.4 GHz to 2.485 GHz**

b. 5 GHz to 6 GHz

c. 10 GHz to 11 GHz

d. 1 GHz to 1.5 GHz

1. What standard is commonly used for cellular networks?

a. Ethernet

**b. 4G**

c. LAN

d. VPN

**Assignment for Week 11**

**Instructions: Read each sentence or phrase carefully. Choose TRUE if the statement is correct and FALSE if the statement is incorrect.**

* 1. Wi-Fi networks operate in both the 2.4 GHz and 5 GHz spectrum.

**TRUE**

* 1. A firewall is used to encrypt data during transmission over a network.

**FALSE**

* 1. Phishing attacks are specifically aimed at deceiving users into giving up personal information.

**TRUE**

* 1. Bluetooth networks have a longer range than Wi-Fi networks.

**FALSE**

* 1. A customer list requires stronger security controls than a publicly available marketing brochure.

**TRUE**