Homework 2

Please complete this assignment individually, each submission should be unique.

Total: 100 points

Symmetric vs Asymmetric Encryption

1. What does it mean for an encryption to be 'asymmetric'? (3 Points)
   When encryption is asymmetric, it means that it has a public key for encryption and a private key for decryption. As the name suggests, the public key is shared with everyone, while the private key is kept secret, allowing only the intended recipient to decrypt the message.
2. If I want to send a message to Hanqiu and would like only us to be able to read it, what would be the most cost-effective method to encrypt it? (7 Points)
   The most cost-effective way to encrypt the message would be symmetric encryption where both me and Hanqiu would have a shared public key for encryption and decryption. Symmetric encryption algorithms are generally faster and require less computational power than asymmetric encryption algorithms since there is only one key to encrypt and decrypt messages.
3. If I want to send all students in the class a message and cryptographically prove that the message came from me, how might I do so? (10 Points)
   If you want to send students a message and cryptographically prove the message came from you, you can use asymmetric encryption with a digital signature. The encryption needs to be asymmetric because only the person with the private key can create a naïve digital signature verifiable by anyone who knows the public key. How this works is that, as the person with the private key, you sign the message with it, and the receivers can verify the message's authenticity with their public keys to ensure the message was sent by you and not tampered with.

Chain of Trust

1. What is a certificate? (2 Points)
   A certificate is a digital document used to verify a user, organization, or website and contains a public key. Certificates are issued by trusted entities called certificate authorities (CA) and include information like subject, public key, and CA signature.
2. What is a hashing algorithm? (2 Points)
   A hashing algorithm is a function that converts data of any size into a fixed-size string of characters, typically referred to as hash values. Hashes are used to ensure data integrity and are difficult to reverse-engineer, making them useful for creating digital signatures and verifying data.
3. What is a Certificate Chain? (2 Points)

A certificate chain is a sequence of certificates where each certificate is signed by the next higher-level certificate in the hierarchy. At the top of the chain is a root certificate that is trusted by all parties and intermediate certificates link the server's certificate to the root.

4. What is a Hash Chain? (2 Points)
   A hash chain is a series of hash values where each hash value is derived from previous ones. Hash chains can be used in cryptographic protocols to ensure data integrity and protect against tampering.
5. When are Certificate Chains preferable to Hash Chains? (7 Points)
   Certificate chains are preferable when you need to establish trust in a digital identity or public key. The certificate chain allows you to verify that a certificate is valid and trusted by a root certificate authority. Hash chains are used more for ensuring data integrity rather than establishing trust in an identity.

TSL/SSL

1. What is a Man-in-the-Middle attack and how can it occur even with Asymmetric Encryption? (5 Points)
   A Man-in-the-Middle (MitM) attack occurs when an attacker intercepts and potentially alters communication between two parties. This can happen even with asymmetric encryption if the attacker can intercept the public key in the exchange process, the attacker can replace the legitimate public key with their own and decrypt and re-encrypt the communication to allow them to read or modify messages.
2. Please draw the process of a client and server authenticating each other through TLS/SSL. (7 Points)

a. • **Client Hello**: The client sends a "hello" message to the server, including supported cipher suites and a random number.
b. • **Server Hello**: The server responds with its chosen cipher suite and its own random number.
c. • **Server Certificate**: The server sends its digital certificate, which contains the public key.
d. • **Key Exchange**: The client generates a pre-master secret and encrypts it using the server's public key.
e. • **Session Keys**: Both the client and the server use the pre-master secret to generate session keys.
f. • **Authentication**: The client and server exchange messages to authenticate each other.
g. • **Secure Communication**: Once authenticated, encrypted communication begins.

MQTT

1. Why is MQTT often referred to as a 'Hub and Spoke' model? (3 Points)
   The MQTT is often referred to as a 'Hub and Spoke' model because all communication in the system is managed by a central broker (the hub). Clients (spokes) send and receive messages through the broker without directly communicating with each other.
2. Can Client A directly send a message to Client B in MQTT? (5 Points)
   No, Client A cannot directly send a message to Client B in MQTT. In MQTT, messages are published topics and clients subscribe to these topics. The broker manages the distribution of messages, ensuring that only subscribed clients receive them.
3. How might Client A get a message to Client B in MQTT? (5 Points)
   Client A can publish a message on a specific topic that Client B is subscribed to. When Client B subscribes to that topic, it will receive a message from the broker.
4. What are the two types of Man-in-the-middle Attacks possible in MQTT? (10 Points)
   The two types of MitM attacks are message interception and message injection. Message interception is when an attacker can intercept a message between the client and broker, generally what can happen if the connection is not encrypted (no TLS/SSL). Message injection is when an attacker can inject false messages into the communication stream, potentially compromising the integrity of the data being transmitted.

Closing Thoughts

1. How might Client A send a message to Client B through MQTT such that no other Client than B, even if properly subscribed to the appropriate topic can understand the content of the message? (Hint: Look to Asymmetric Encryption). (15 Points)
   A client can encrypt messages using Client B's public key before sending it. Even though other clients might be subscribed to the same topic, only client B, who has the corresponding private key, would be able to decrypt the massage.
2. Draw a system boundary for the IoT Board if deployed as an IoT Device. (15 Points)

For this question, you should draw a diagram that shows the IoT board within its system boundary. You should include:

1. **The IoT Device** (IoT board itself) as a central unit.
2. **Sensors/Actuators** connected to the IoT device.
3. **Communication Interfaces** (e.g., MQTT broker, Wi-Fi, Bluetooth).
4. **Cloud or Server** connected to the IoT device for processing or storage.
5. **User Interaction** with the IoT system (e.g., through a mobile app or web interface).