Armaan Shamsaasef

Key Exchange

Key Exchange - SY0-701 1.4

The Core Problem: How can two parties establish a shared secret key over an insecure network (like the internet) where attackers might be listening?

1. Out-of-Band Key Exchange

- Definition: The key is shared using a method outside the primary communication channel.
- Concept: The "secret" is transferred physically or via a different, presumably more secure, method.
- Example from Video:
    - You call a friend to establish a secure connection for a video call.
    - You read the encryption key to them over the phone (a different channel).
    - You then both use that key to encrypt your video call on the computer.

2. In-Band Key Exchange

- Definition: The key is established within the same communication channel. This is the primary method used on the internet and requires cryptography to be secure.

The Diffie-Hellman Key Exchange

This is the most common method for in-band key exchange. It allows two parties to create a shared secret key without ever sending the key itself over the network.

The Core Concept: It's based on the difficulty of solving the Discrete Logarithm Problem.

The Paint-Mixing Analogy (Video Example)

This analogy explains how two parties can create a shared secret (the same color of paint) while an eavesdropper cannot, even if they see all the public exchanges.

1. Common, Public Starting Point: Both you and your friend start with the same can of public paint (e.g., Yellow). This is the equivalent of the public generator and prime modulus in the mathematical algorithm.
2. Each Party Adds a Secret: You secretly mix in your private color (e.g., Red). Your friend secretly mixes in their own private color (e.g., Blue). You now have Orange, they have Green.
3. Exchange Public Mixtures: You send your Orange mixture to your friend. They send their Green mixture to you. An attacker can see these public mixtures.
4. Combine with Your Private Secret: You take your friend's public mixture (Green) and add your private color (Red) to it. Your friend takes your public mixture (Orange) and adds their private color (Blue) to it.
5. Shared Secret Created: Both of you now have the same final color: Brown. The attacker, who only saw the public Yellow, Orange, and Green, cannot easily determine the exact formula for Brown.

Key Characteristics of Diffie-Hellman

- Perfect Forward Secrecy: Even if an attacker records an encrypted session and later steals one of the private keys, they cannot decrypt the old session. This is because the shared secret was temporary and not derived from the long-term private key.
- Vulnerable to MITM: The standard Diffie-Hellman exchange does not provide authentication. An attacker in the middle can establish two separate key exchanges (one with you, one with your friend) and decrypt/relay messages.
    - Solution: Use Digital Signatures to authenticate the Diffie-Hellman public keys, ensuring you are trading keys with the right person. This is how real-world protocols like TLS implement it.

Summary

- Out-of-Band: Key is shared via a separate, secure channel (e.g., phone call).
- In-Band (Diffie-Hellman): Key is created within the session using public and private components.
    - It provides Perfect Forward Secrecy.
    - It requires an additional method (like digital signatures) for authentication to prevent Man-in-the-Middle attacks.