Man-In-The-Middle Attack

By:
Abdulrehim Shuba
Dilnoza Saidova
Gil Rabara

Basic Overview of Man in the Middle

With Abdul

What is Man in The Middle (MiTM)?

- MiTM is a type of spoofing attack

1) An attacker pretends to be a trusted source (i.e., McDonald's wifi)
2) Data then flows through the attacker (emails, passwords, sensitive info)
3) Attacker sends "traffic" to intended location leaving the victims unaware of the attack.

Ways to Protect Yourself

With Gil

Preventative Measures

There are a lot of ways to not be the lowest hanging fruit for a MiTM attack, the ones we covered are

- SSL/TLS
- Signed Certificates
- VPN
- Knowledge

Secure Socket Layer (SSL) / Transport Layer Security (TLS)

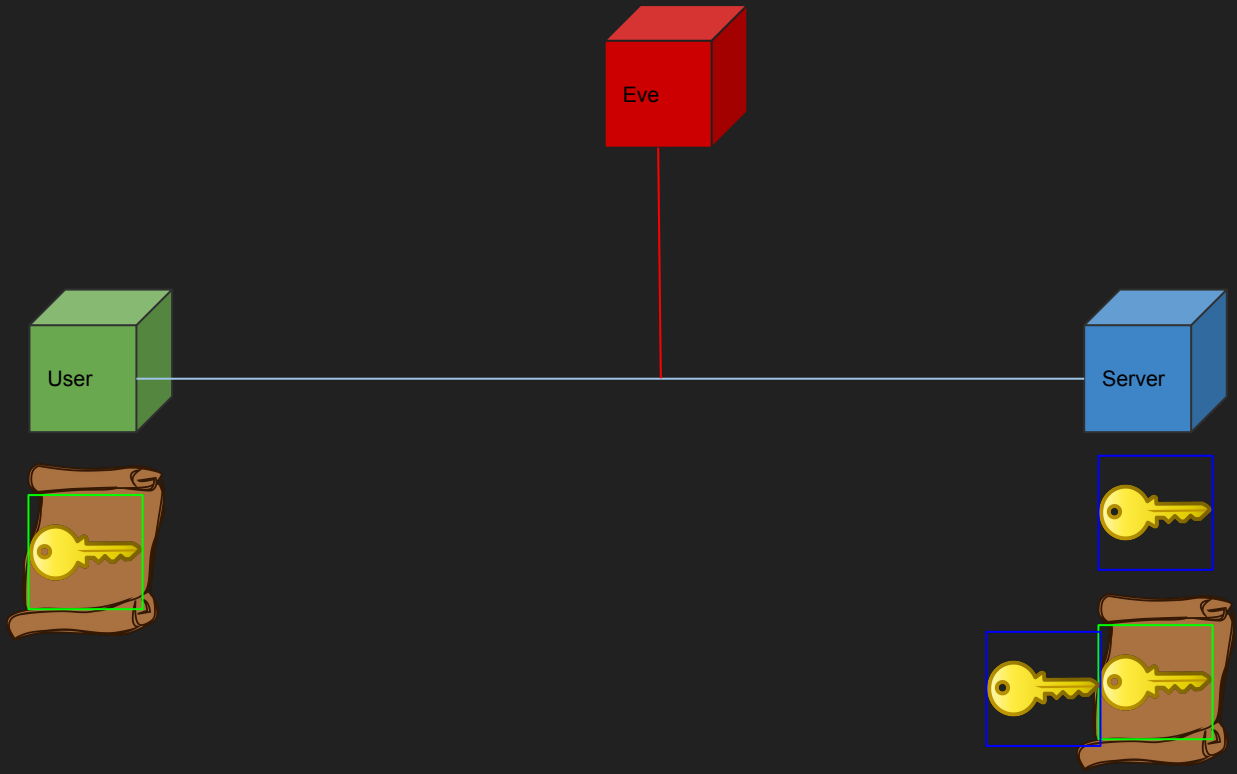
SSL provides a secure channel between two machines or devices operating over the internet or an internal network.

HTTP = does not implement SSL/TLS

HTTPS = implements SSL/TLS

1) Computer asks to speak privately with server
2) Server agrees, and sends computer a public key
3) Computer can now encrypt messages with server's public key
4) Messages can only be decrypted by server's private key

Secure Socket layer



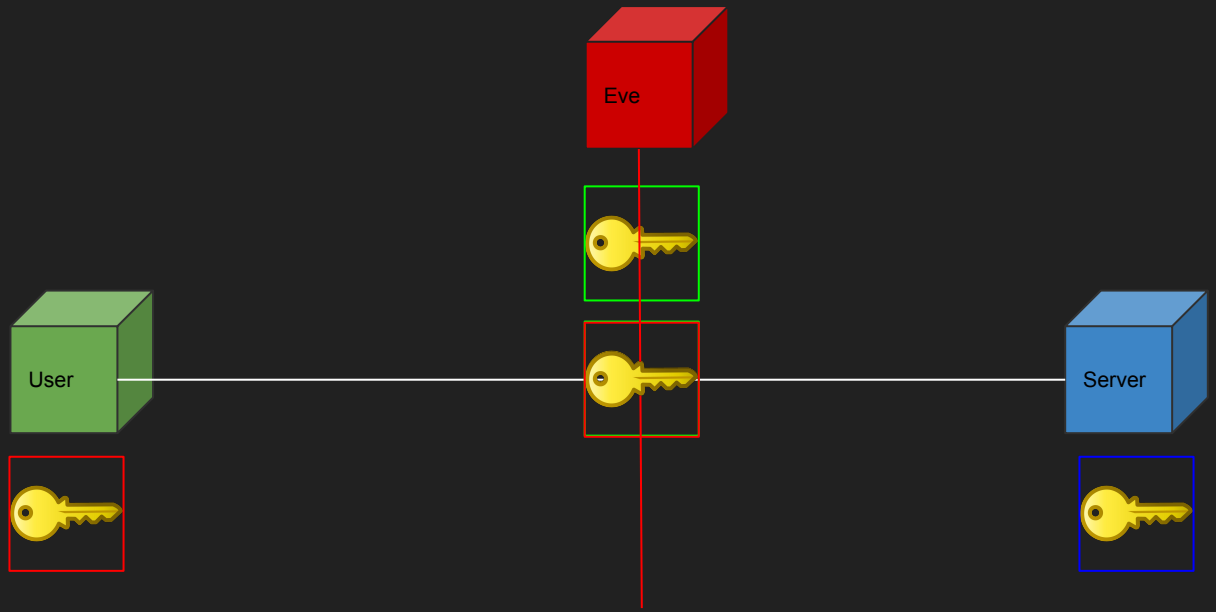
Potential Problem!!!

The initial step where the server sends the public key to the user can be intercepted. This is because way back in the day this initial message was just plain text.

1) Attacker takes the server’s public key
2) Attacker that’s pretending to be the server sends the computer their public key

Demo incoming.

Signed Certificate demo

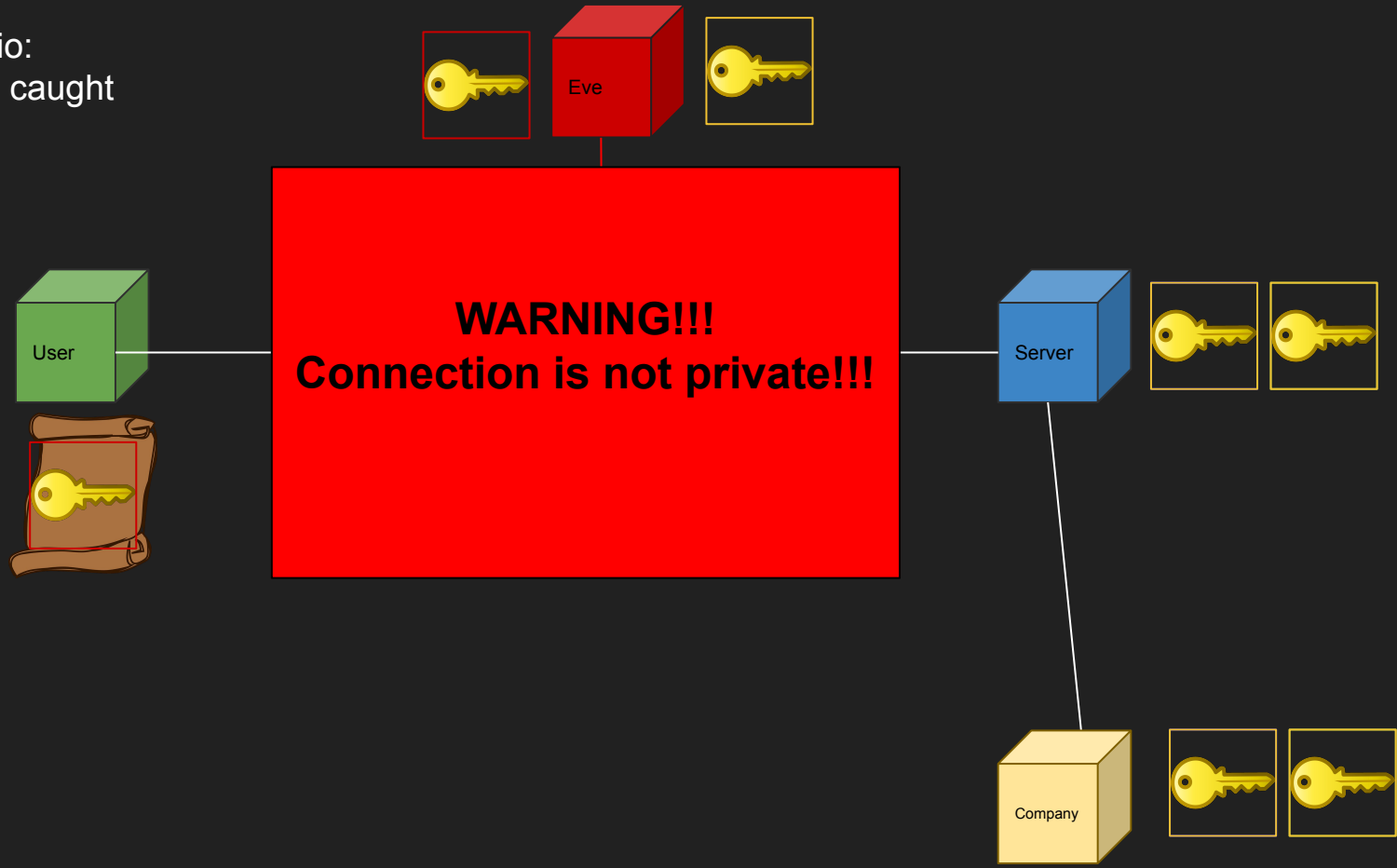


Signed Certificates

Have a trusted 3rd party validate the public keys that are being exchanged.

- 3rd party will verify if keys are from the right server
- 3rd party will now sign these keys with their own private key
- Now if the attacker changes anything the key is no longer valid

Good scenario:
Attacker gets caught



Virtual private network (VPN)

Even if a criminal manages to access your network, the encrypted data blocks them from reading your messages or knowing which websites you're going to.

- VPNs can be used within LANs to provide secure environment for sensitive data
- VPNs use key-based encryption for secure communication by creating a subnet
  - Subnet is a smaller part of large network divided into two or more networks
- Attackers wouldn't be able to decipher traffic within the VPN regardless of them being able to get into the shared network

Knowledge

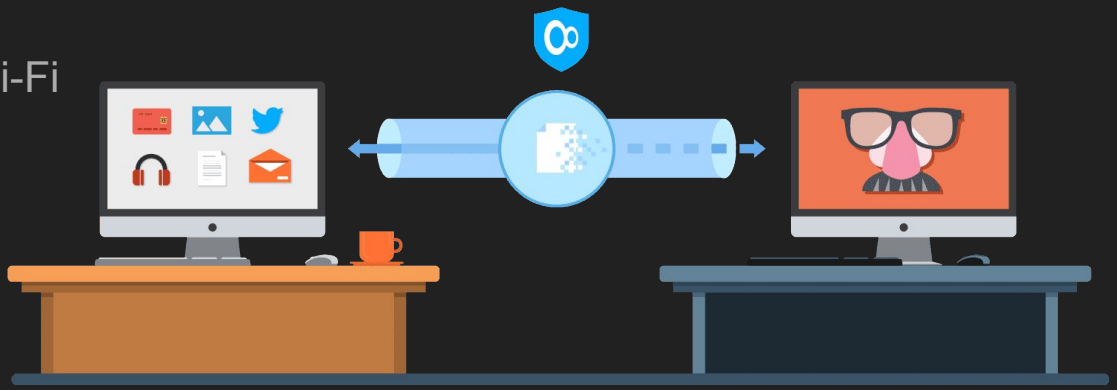
Summary &
Example of MiTM attack

With Dilnoza

Best practices to Prevent MITM Attacks - Summary

Secure Connections

- Use websites with HTTPS
- Avoid public, unsecured Wi-Fi



VPN Encryption

- VPN protects traffic between the device and VPN gateway
- Attackers wouldn’t be able to decipher traffic within VPN

Best practices to Prevent MITM Attacks - Summary Contd.

Avoid Phishing Emails

- Don’t open suspicious emails
- They could redirect to sketchy websites/force-download malware

Stay Away From…

- Suspicious certificates and promotions
- Fake websites - it’s not always safe to only look for *https*
- Pop ups (i.e., ads, urgent notifications, sketchy hyperlinks)

Real-Life Examples of MiTM Attacks

DigiNotar Hack

- In 2011, DigiNotar detected intrusion into its Certificate Authority infrastructures
- Attacker gained access to 500 certificates for well-known websites (i.e., Google)

Equifax Data Breach

- In 2017, Equifax suffered massive data breach
- Over 145.5 million Equifax customers had their financial information leaked
  - 400,000 UK, 200,000 US, 100,000 Canadian customers affected
- Equifax mobile app didn't consistently use HTTPS
  - Sensitive data was intercepted by hacker(s)

Thank you for your time