# SSL/TLS: Certificates

Michael Purcell

01 June 2021

Australian National University

Software Innovation Institute

# SSL/TLS: Certificates

Man-in-the-Middle Attacks

Public Key Certificates

Certificates in SSL/TLS
- Certificate Messages
- Key Exchange Messages

References

# Secure Communications Channel

Alice and Bob want to use an asymmetric encryption scheme establish a secure communications channel.

Accordingly, both parties generate public/private key pairs and share the public keys with one another.

To send a message, the sender uses the recipient's public key to encrypt their transmission. The recipient then uses the corresponding private key to decrypt the transmission that they receive.

# An Active Adversary

Eve wants to eavesdrop on the conversation between Alice and Bob. Wee assume that Eve is an active adversary. That is, we assume that Eve can:

- intercept messages sent from Alice to Bob and vice versa.
- send messages to Alice or Bob.

If Eve can intercept the messages that Alice and Bob use to share their public keys with one another, then she can carry out a man-in-the-middle (MitM) attack.

# Man-in-the-Middle Attack

When Eve intercepts a key-exchange messages, she replaces the message with on containing a public key for which she knows the corresponding private key.

When Eve intercepts an encrypted message, she:

- decrypts the message using her private key.
- inspects and/or modifies the message.
- encrypts the message using the recipient's public key.
- sends the encrypted message to the recipient.

# SSL/TLS: Certificates

Man-in-the-Middle Attacks

Public Key Certificates

Certificates in SSL/TLS
- Certificate Messages
- Key Exchange Messages

References

# Structure

A public key certificate is an electronic document which is used to prove ownership of a public key. Each certificate contains information about:

- the subject's identity.
- the subject's public key.
- the issuer's identity.
- the issuer's digital signature.

The issuer signs the certificate using the private key associated with a public key that they own.

# Certificate Chains

By signing a public key certificate, the issuer is claiming that the subject is the rightful owner of the public key.

The issuer's public key is used to verify their signature.

Therefore, the issuer must themselves provide a public key certificate that proves that they are the rightful owner of the public key required to verify their signature.

# Root Certificate Authorities

Certificate chains terminate when they reach a certificate that has been signed by a user whose ownership of a public key has been previously established.

In most certificate ecosystems, certificate chains terminate when they reach a root certificate. Root certificates are self-signed certificates that are trusted by default.

Root certificates identify root certificate authorities which are generally vetted through some mechanism external to the certificate ecosystem.

# SSL/TLS: Certificates

Man-in-the-Middle Attacks

Public Key Certificates

Certificates in SSL/TLS
- Certificate Messages
- Key Exchange Messages

References

# The Server Certificate Message

Test

# The Client Certificate Message

Test

# The Server Key Exchange Message

Test

# The Client Key Exchange Message

Test

# SSL/TLS: Certificates

Man-in-the-Middle Attacks

Public Key Certificates

Certificates in SSL/TLS
- Certificate Messages
- Key Exchange Messages

References

# References


- The blog ”Command Line Fanatic” by Jeremy Davies
  - ”SSL Certificate Exchange”
  - ”SSL ”How Certificates Use Digital Signatures”

- RFC 5246 - ”The Transport Layer Security (TLS) Protocol Version 1.2”