Design and Analyze Secure Networked Systems 6

Prof. Edward Chow @ Colorado Univ.

Note by waegaein@github.com

Creation and Installation of Server Certificate

1. Generate private key with passphrase.
2. Generate .pem file for Certificate Signing Request (CSR).
3. Send the CSR to a CA.
4. Receive .pem file for certificate from CA.
5. Copy the certificate file to serving directory.
6. Copy private key file to secure directory.

Creation and Installation of Client Certificate

1. Generate private key with passphrase.
2. Generate .pem file for Certificate Signing Request (CSR).
3. Send the CSR to a CA.
4. Receive .p12 file for certificate from CA.
5. Copy the certificate file to directory that browsers can access.
6. Copy private key file to secure directory.

Mutual Authentication of Client and Server

1. Client requests access to server with HTTPS protocol.
2. Server presents Server Certificate and request client to present Client Certificate.
3. Client presents Client Certificate.
4. Server responds with credential information.