

ITS335 – Web Security Notes

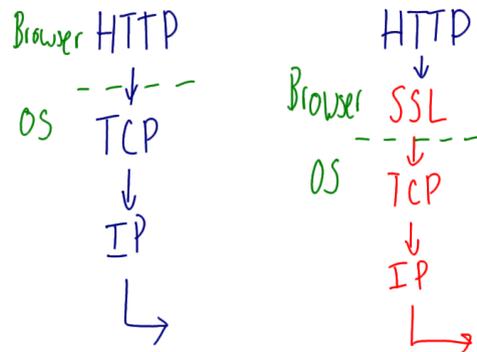


Figure 1: HTTP vs HTTPS; Lecture 20

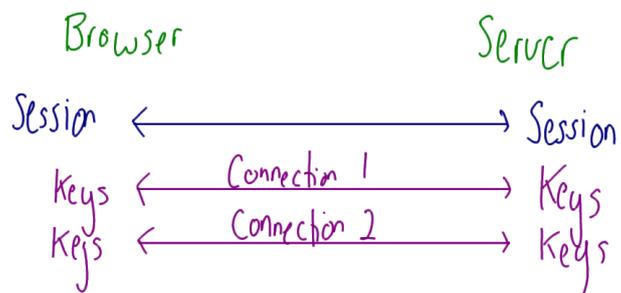


Figure 2: SSL Session and Connection; Lecture 20

Symmetric :

$$C = E(K_{ab}, P) \quad P = D(K_{ab}, C)$$

\xrightarrow{C}

Public Key :

$$C_1 = E_{RSA}(PU_b, K_{ab}) \quad K_{ab} = D_{RSA}(PR_b, C_1)$$

$\xrightarrow{C_1}$

Figure 3: Exchange Symmetric Key using Public Key Crypto; Lecture 20

Browser

$$C_1 = E_{RSA}(PU_m, K_{ab}) \quad K_{ab} = D_{RSA}(PR_b, C_2)$$

$\xrightarrow{C_1}$

$$K_{ab} = D_{RSA}(PR_m, C_1)$$

$$C_2 = E_{RSA}(PU_b, K_{ab})$$

Figure 4: Man-in-the-Middle Attack on Public Key Exchange; Lecture 20

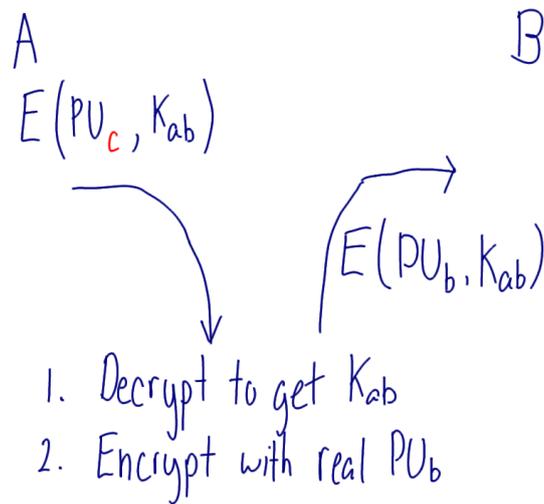


Figure 5: Man-in-the-Middle Attack on Public Key Exchange (2); Lecture 21

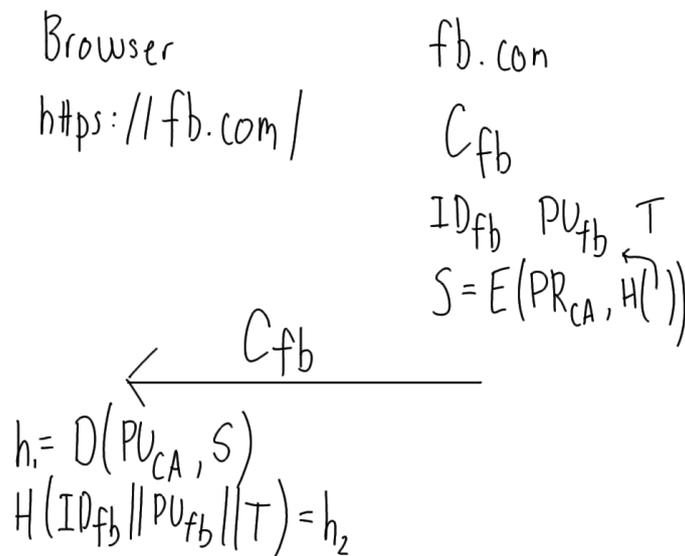


Figure 6: Server sending Certificate to Browser; Lecture 21

C_{eff.org} issued by
StartCom Class 2

C_{startcom class 2} issued by
StartCom

C_{startcom} issued by
(self-signed) StartCom

Figure 7: Certificate Hierarchy; Lecture 21