ITS335 – Web Security Notes

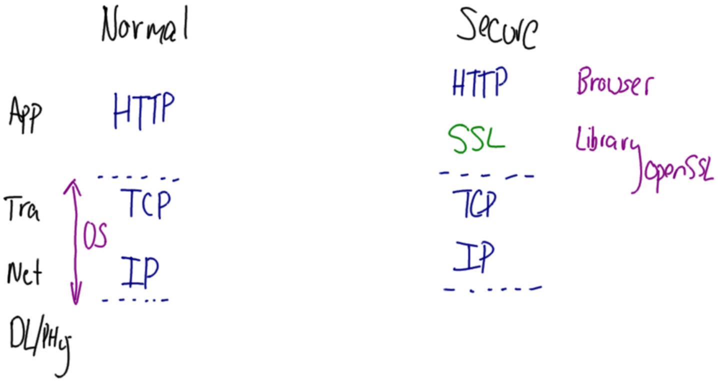

Figure 1: HTTPS Protocol Stack; Lecture 19

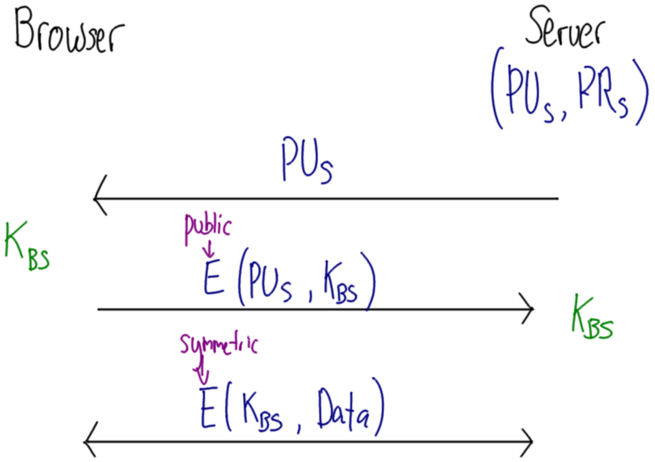

Figure 2: Exchanging a Secret Key with Public Key Crypto; Lecture 20

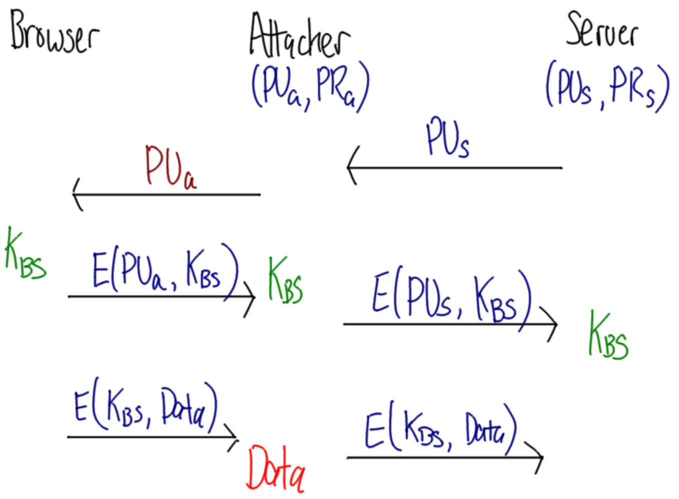

Figure 3: Man-in-the-middle attack on Key Exchange; Lecture 20

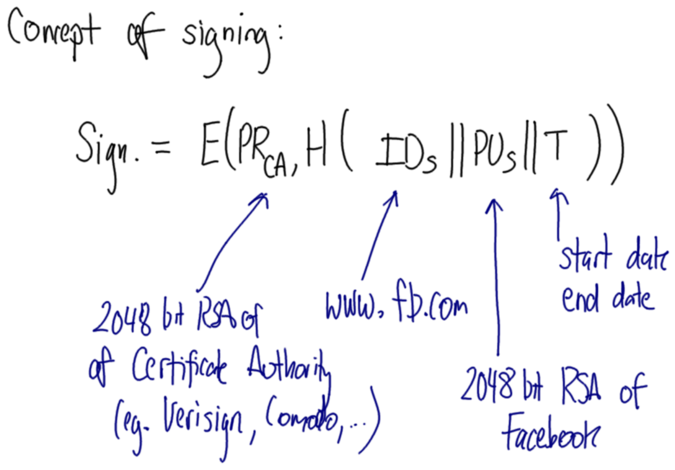
Concept of signing:
Sign. = E(PR_CA, H(ID_s || PU_s || T))
2048 bit RSA of of Certificate Authority (eg. Verisign, Comodo, ..)
www.fb.com
2048 bit RSA of Facebook
start date
end date

Figure 4: Signing a Digital Certificate; Lecture 20

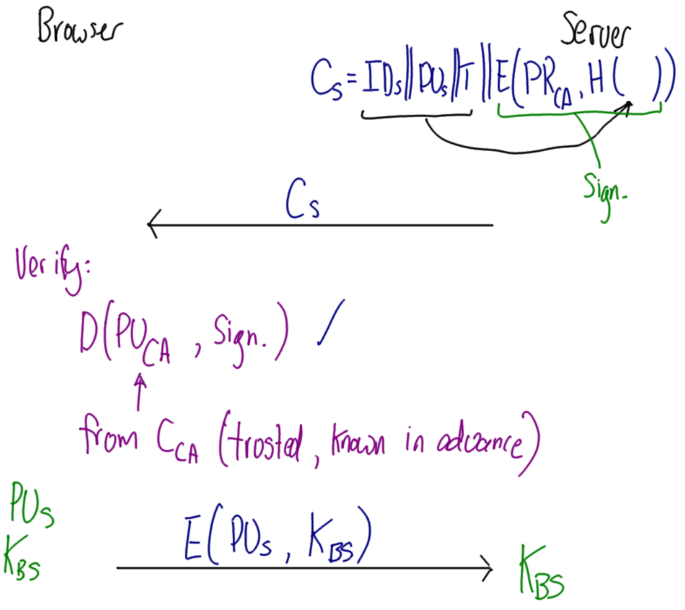
Browser
Server
Cs = IDs || PUs || T || E(PRCA, H( ))
Sign.
Cs
Verify:
D(PUCA , Sign.) ✓
from CCA (trusted, known in advance)
PUs
KBS
E(PUs , KBS)
KBS

Figure 5: Certificate for Secret Key Exchange; Lecture 20

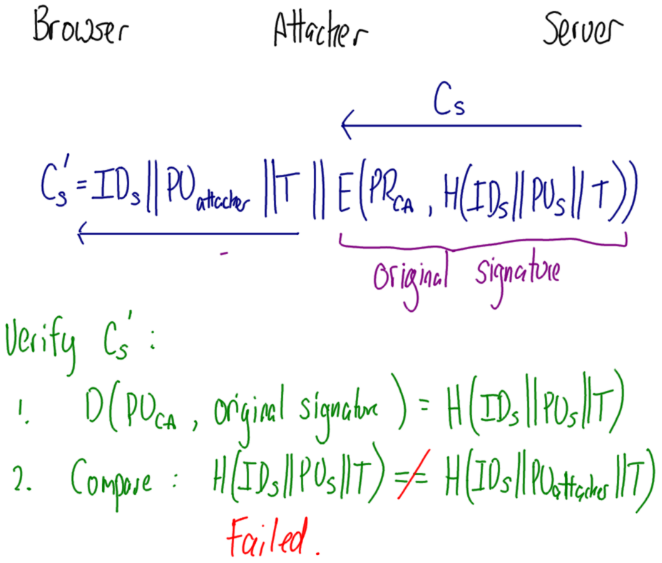
Browser
Attacker
Server
Cs
Cs' = IDs || PUattacker || T || E(PRCA , H(IDs || PUs || T))
original signature
Verify Cs' :
1. D(PUCA , original signature) = H(IDs || PUs || T)
2. Compare : H(IDs || PUs || T) ≠ H(IDs || PUattacker || T)
Failed.

Figure 6: Attack on Certificate - Changed Public Key; Lecture 21

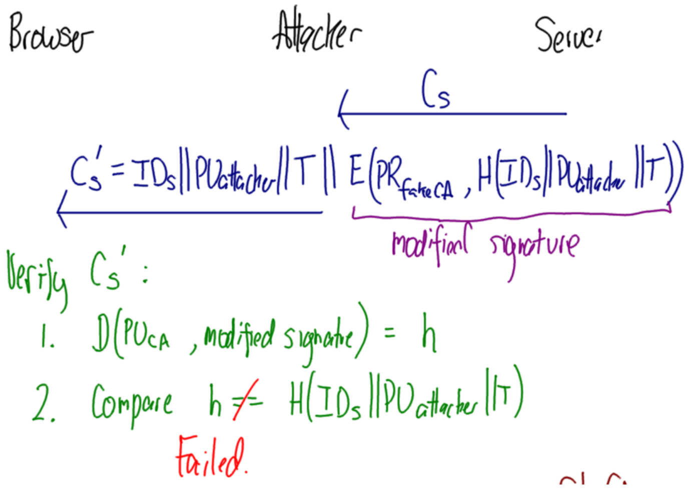
Browser
Attacker
Server
C_s
$C_s' = ID_s || PU_{attacker} || T || E(PR_{fakeCA}, H(ID_s || PU_{attacker} || T))$
modified signature
Verify C_s':
1. $D(PU_{CA}$, modified signature$) = h$
2. Compare $h \neq H(ID_s || PU_{attacker} || T)$
Failed.

Figure 7: Attack on Certificate - Changed Signature; Lecture 21

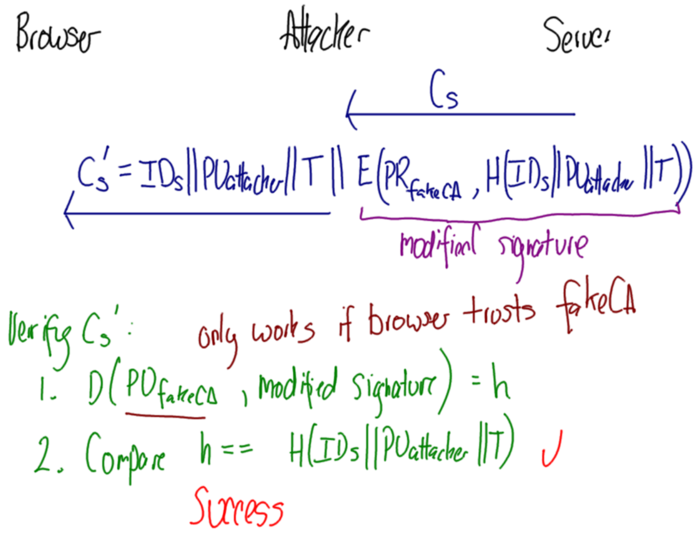
Browser
Attacker
Server
C_s
$C_s' = ID_s || PU_{attacker} || T || E(PR_{fakeCA}, H(ID_s || PU_{attacker} || T))$
modified signature
Verify C_s':
only works if browser trusts fakeCA
1. $D(\underline{PU_{fakeCA}}$, modified signature$) = h$
2. Compare $h == H(ID_s || PU_{attacker} || T)$ ✓
Success

Figure 8: Attack on Certificate - Fake CA; Lecture 21