Sean Gordon

CPRE 431

M08 HW

Assignments will be submitted in PDF format via Canvas.

Please submit your homework online through Canvas. Late homework will not be accepted.

Important: Your submission must be in .pdf format ONLY!

Please ensure that you support all your answers with the correct screenshots showing your solutions.

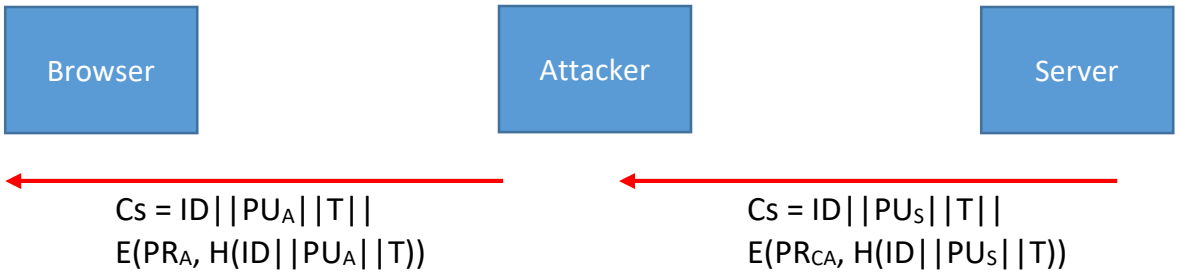
1. Consider the following threats to Web security and describe how each is countered by a particular feature of SSL.

   a. Man-in-the-middle attack: An attacker interposes during key exchange, acting asthe client to the server and as the server to the client.
   The client checks that the certificate sent from the server is valid. If not, the authentication fails.

   b. Password sniffing: Passwords in HTTP or other application traffic are eavesdropped.
   Data would be encrypted before it ever reached the password sniffer, rendering it useless to the attacker.

2. What is X.509 Certificate?
   A digital certificate using the X.509 public key infrastructure standard. They are used to verify a sender's identity for use in secure network communication.

3. Assume that a hacker was able to install a fake Certificate Authority (CA) signature on your browser. Aided with drawing (similar to the drawing in the lecture's slides), show how the Man in The Middle (MiTM) Attack can be carried out even if the server is using a certificate signed by the original CA.



Browser believes the PU_A it has stored to be a valid public key from the CA, so when the hashes match it does not question it.