Nitin Nagavel

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 as the client to the server and as the server to the client.

   The main – in – the – middle attack would be countered by the certificate validation process.

   b. Password sniffing: Passwords in HTTP or other application traffic are eavesdropped.

   To counter Password sniffing, passwords are encrypted

2. What is X.509 Certificate?

   X.509 is a standardiszed set of protocols and certificates that define the public key certificates.

3. Assume that a hacker was able to install a fake Certificate Authority (CA) signature on your browser. Aided with drawing (like 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.

The man in the middle attack can indeed be carried out through HTTPS spoofing. First the attacker gets the victim to visit a website using a phishing attempt. Then, they download a fake

CA certifticate, and finally the attacker signs the certificate with a CA private key and that gets sent to the victim.

Meanwhile in the background, the attacker monitors all traffic to and from the server even if the certificate is signed by the original CA. Attached is a drawing: