CSCI 3403 **Brennon Lee**
Homework 13 **Fall 2018, CU-Boulder**

1. **Review Question 22.4** What is DKIM

   answer

2. **Review Question 22.5** What protocols comprise SSL?

   answer

3. **Problem 22.2** 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 the server to the client.

   answer

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

   answer

   (c) IP spoofing: Uses forged IP addresses to fool a host into accepting bogus data.

   answer

   (d) IP hijacking: An active, authenticated connection between two hosts is disrupted and the attacker takes the place of one of the hosts.

   answer

   (e) SYN flooding: An attacker sends TCP SYN messages to request a connection but does not respond to the final message to establish the connection fully. The attacked TCP module typically leaves the ”half-open connection” around for a few minuts. Repeated SYN messages can clog the TCP module.

answer

4. **Review Question 23.9** What is a public key infrastructure?

5. **Problem 23.4** Using your Web browser, visit any secure Web site (i.e. one whose URL starts with “https”). Examine the details of the X.509 certificate used by that site. This is usually accessible by selecting the padlock symbol. Answer the same questions as for Problem 23.3

   (a) Identify the key elements in the certificate, including the owner’s name and public key, its validity dates, the name of the CA that signed it, and the type and value of signature.

   anwswer

   (b) State whether this is a CA or end-user certificate, and why.

   anwswer

   (c) Indicate whether the certificate is valid or not, and why.

   anwswer

   (d) State whether there are any other obvious problems with the algorithms used in this certificate.

   anwswer

6. **Problem 23.5** Now access the ”Trust Store” (list of certificates) used by your Web browser. This is usually accessed via its Preference settings. Access the list of Certificate Authority certificates used by the browser. Pick one, examine the details of its

X.509 certificate, and answer the same questions as for Problem 23.3.

(a) Identify the key elements in the certificate, including the owner's name and public key, its validity dates, the name of the CA that signed it, and the type and value of signature.

answer

(b) State whether this is a CA or end-user certificate, and why.

anwswer

(c) Indicate whether the certificate is valid or not, and why.

anwswer

(d) State whether there are any other obvious problems with the algorithms used in this certificate.

anwswer