**USC UPSTATE**

**CSCI 455: Computer Security**

**Spring 2019**

**Homework Assignment 6**

**Problem 1**

Visit the site [www.wellsfargo.com](http://www.wellsfargo.com), read its certificate and find the following information.

1. [2 Points] Which CA issued and signed the certificate? DigiCert Global CA G2
2. [2 Points] What is the subject’s identity? That is, to which company and Website is the certificate issued? [www.wellsfargo.com](http://www.wellsfargo.com) Wells Fargo & Company
3. [2 Points] Which digital signature scheme and hash function is used to sign the certificate? Signature scheme: RSA Signature hash algorithm :sha256
4. [2 Points] Which *public-key* encryption scheme is used to secure the communication between your browser and the site [www.wellsfargo.com](http://www.wellsfargo.com) and what is the length of the public key? RSA (2048 Bits)
5. [2 Points] Which *private-key* encryption scheme is used to secure the communication between your browser and the site [www.wellsfargo.com](http://www.wellsfargo.com) and what is the length of the key?
6. [30 Points] What is the certification path for [www.wellsfargo.com](http://www.wellsfargo.com), and how does your browser verify the certification path when you visit the site? Be sure to include every step of the verification. PATH: DigiCert Global Root G2🡪 DigiCert Global CA G2 🡪 [www.wellsfargo.com](http://www.wellsfargo.com)

**Problem 2**

This question refers to the key exchange protocol described on Slide 8 of the lecture on Key Exchange and Hybrid Encryption (Lecture 4, Part II). In class we showed that the given protocol is secure against *passive* attackers, i.e. attackers who can only eavesdrop and intercept the messages exchanged between Alice and Bob.

1. Show how an *active* attacker can break the protocol. Recall that an active attacker is one who can not only eavesdrop, but can also block and alter messages on the network, and inject his own messages into the network.

An active attacker can collect enough data to decrypt the messages and gain access to the keys. Several methods could be used for cracking if the user can intercept and modify the data. They could intercept all messages and send their own to trick users into sharing information or continue to study packets for frequency detection.

1. Show how to secure the protocol against active attackers if a secure PKI is available.

Use a public key encryption scheme to share the private keys so that the attacker could not find the private keys. Changing private keys each time and using public key encryption to share the private keys, makes the level of security much higher, even against active attackers.

**Problem 3**

During the discussions on PKI and SSL, we emphasized the importance of the integrity of the certificate authority (CA). What damages can an attacker cause if he is able to compromise a trusted CA? Be as comprehensive as you can in your answer, and use a good concrete example to illustrate your answer.

IF an attacker is able to compromise a trusted CA, there aren’t very many CA’s in existence, it could be catastrophic to end users under the attackers target. The attacker could use forms of phishing or other methods to route a user to untrusted sites that will show as protected in the end user’s browser. The user could be sent to a fake Amazon page that looks like the real amazon and has a trusted (lock) symbol in the left side of the URL. This could trick the end user into revealing passwords or credit card information, etc.