**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?

Answer: DigiCert Global CA G2

1. [2 Points] What is the subject’s identity? That is, to which company and Website is the certificate issued?

Answer: [www.wellsfargo.com](http://www.wellsfargo.com) Wells Fargo & Company

1. [2 Points] Which digital signature scheme and hash function is used to sign the certificate?

Answer: SRSA Signature and sha256

1. [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?

Answer: RSA (2048 Bits)

1. [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?
2. [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.

Answer: 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.

Answer: An active hacker may be able to break the encryption on the algorithm used. By gaining info or brute forcing cracking, the attacker then can alter and change files. Possibly installing malicious software to still user data or information. The attacker can sign and encrypt the files looking like Alice or Bob truly sent them.

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

Answer: By using a public key encryption, you can also encrypt the private key. Signing everything with a private key, which also changes after a given time is also key. This allows the users to once again have Integrity if the attacker somehow manages to get the private-key.

**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.

Answer: Attacking and compromising a trusted CA could possibly cause major harm. As major websites only use certain CA’s, and many websites use the same ones. If one was compromised many websites would be open to potential threats. As end users would believe they are visiting legitimate websites, they could enter their info in for hackers to take.