Networks and Distributed Systems	**Homework 9: TLS**
CS3700 Spring 2019	**January 10, 2019**

This homework is due at the beginning of class on April 11, 2019 and is worth 2% of your grade.

Name: ____

CCIS Username: ____

Problem	**Possible**	**Score**
1	25	
2	15	
3	15	
Total	55	

1. Using your web browser, analyze the TLS certificate for `https://www.bankofamerica.com`.

1a. Who signed the certificates in this chain? How many certificates are there in the chain to the root? (5 pts)

1b. On what other domain(s) besides www.bankofamerica.com is this certificate valid (hint: look at the Subject Alternate Names field of the certificate)? (5 pts)

1c. When will this chain no longer be valid? How do you know? (5 pts)

1d. When public key encryption algorithm did Bank of America use to generate their public/private key pair? How big is the key? (5 pts)

1e. What distinguishes a root certificate from other TLS certificates? (5 pts)

2a. Suppose that using your web browser, you connect to a HTTPS web site where the root certificate in the chain is not in your browser's trust store. What should happen? (5 pts)

2b. Sometimes it is necessary to use untrusted self-signed certificates in practice. When might this be the case? What security guarantees would doing this provide? (5 pts)

2c. Suppose you are an attacker, and during a break-in, you discover that you can obtain either the private key corresponding to Bank of America's certificate, or the private key corresponding to the root CA certificate that signed Bank of America's certificate? Given that you are an attacker, which would you pick to download and why? (5 pts)

3. There are online tools that let you measure the TLS implementations used by websites. These tools tell you whether a given website's TLS implementation is vulnerable to specific security problems; whether they are following best practices; etc.

For the next set of questions, we will use the testing tool provided by Qualys that is available at `https://https://www.ssllabs.com/ssltest/`. Open the Qualys testing tool in two tabs: in one tab, analyze `www.bankofamerica.com`, in the other tab analyze `cbw.sh`.

3a. Qualys grades the security of BofA as a "B", while cbw.sh gets an "A+". Explain the primary reason why cbw.sh gets a better grade than BofA. What is the problem area, and why is it a problem? (Hint: BofA has a weakness in the "Protocol Details" section of the report) (10 pts)

3b. cbw.sh supports HSTS and HSTS preloading. What is HSTS and HSTS preloading? Why security problem is HSTS meant to address? (5 pts)