Networks and Distributed Systems	**Homework 9: Security**
CS3700 Fall 2017	**November 16, 2017**

This homework is due at the beginning of class on November 27, 2017 and is worth 1.5% of your grade.

Name: _____

CCIS Username: _____

Problem	Possible	Score
1	20	
2	15	
Total	35	

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

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

1b. You will notice that the root certificate for this site is VeriSign Class 3 Public Primary Certification Authority - G5. What distinguishes a root certificate from other SSL certificates? (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)

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? (VeriSign Class 3 Public Primary Certification Authority - G5) Given that you are an attacker, which would you pick to download and why? (5 pts)