CS 5490/6490: Network Security – Spring 2020
Programming Assignment 3
Due by 11:59:59 PM MDT on February 26th 2020

Important:

- **No late submissions will be allowed so please plan well ahead of the due date.**
- **No cheating will be tolerated. No copying from the Internet is allowed.**
- **Total Points for this Programming Assignment: 100**

The goal of your programming assignment is to build the expanded Needham Schroeder Mediated-Authentication Scheme (Figure 11-19 from the Perlman book). You need to write socket programs that run on three nodes (can be three processes on the same machine), Alice, Bob, and the KDC. You must use one of Python, or Java for your programs.

Assume that Alice initiates the authentication exchange. Please ensure the following.

- The challenges are at 64 bits long.
- The secret key encryption scheme is 3DES.
- You need to set up shared keys for each 3DES based secure communication between two parties (Alice and KDC, Bob and KDC, and, Alice and Bob).
- Use a unique number for identifying a user instead of IP addresses and port numbers.
- Read sections 11.5 and 11.6 from the book before choosing values of the various N's in Figure 11-19.

When the initial two-message handshake is not used, and when N_B is removed from the ticket, the extended version of Needham Schroeder reduces to the original version (Figure 11-18). For the original version of Needham Schroeder scheme first use the Electronic Code Book (ECB) for encrypting multiple blocks and demonstrate how Trudy is successful in impersonating Alice by causing a *reflection attack.* Remove this vulnerability by using Cipher Block Chaining (CBC) instead of ECB. In creating the reflection attack, you can assume that the information that Trudy needs to eavesdrop is available to her (i.e., you can make that information available to Trudy in your program, you do not need to sniff that information in real time).

Include print commands in your code to show

- one successful authentication (extended Needham Schroeder),
- the reflection attack (original Needham Schroeder), and
- the difference in CBC vs ECB outputs for the last two messages (original Needham Schroeder).

Using the *handin* utility (directory PA1-20), electronically turn in your code along with the output files, and a readme file. The readme file should explain how the code is organized. Your code should be well commented. *5 points* will be deducted for lack of comments. For this assignment you could take the help of existing tools such as *Openssl* for 3DES related functions. In addition to submitting your code, you will be required to give a demo of your programming assignment to the TA. You can use any computer/laptop to work on your programming assignment.

Grading Rubric:

40 points: Extended Needham Schroeder implementation
35 points: Reflection Attack implementation
15 points: CBC instead of ECB
5 points: Exception handling in your code
5 points: Detailed comments in your code