Network Security – CSE 550

Assignment 2

Total points: 35

Due: October 29, 2016 23:59 hours.

Description:

This assignment builds upon the chat server to add additional functionality of authentication and authorization to chat messages. Two users – lets say Alice and Bob who are both online could chat with one another enabling confidentiality and authentication. To do so you need to implement a KDC like functionality in the chat server. Alice communicates with the KDC to negotiate a shared secret with Bob which it uses for communicating secretly and may additionally also sign the messages (through some form of message authentication code (MAC)) to prevent against unwanted tampering. You are free to implement your own protocol to achieve the same. It may be derived from Needham Schroeder (NS) scheme or may involve more complex schemes such as those observed in Kerberos. To encrypt messages you may use openssl EVP functions (see resources below). The shared key for each user (Alice and Bob) may be derived from their passphrases by using openssl PBKDF functions (see resources below), that takes as input a passphrase and outputs a pseudo-random sequence of bytes.

To summarize:
Alice requests the KDC to communicate with Bob and a protocol ensues between Alice and the KDC that results in the derivation of the session key which Alice and Bob eventually use to communicate. Additionally the messages may involve MAC to protect these messages against unwanted tampering. The scheme works to protect online chat messages between two parties ONLY.

Some useful resources:

https://wiki.openssl.org/index.php/EVP_Symmetric_Encryption_and_Decryption

What you are supposed to submit:

1. C source code for the aforementioned chat client and sever supporting the functionalities outlined above.
2. Makefile through which one could compile these programs.
3. A write up of what your system does, what all assumptions you made, the inputs that you used to test your program and all the errors that you handled.

How you would be graded:

1. Successful compilation using Makefile –10 points.
2. Demonstration of the functionalities to encrypt the chat messages and the actual encrypted messages (must be shown using wireshark) – 20 points.
3. Description of how the system protects against atleast two kinds of attacks (particularly those involving impersonating one of the communication peers) – 5 points.