Lab 2: Implementation and Application of HMAC-SHA1

HMAC is a keyed-hash type of message authentication code (MAC), involving a hash function and a secret key. It can simultaneously provide the data integrity and the authentication of a message. According to the different underlying hash functions MD5, SHA-1, SHA-256, etc., the algorithm is termed HMAC-MD5, HMAC-SHA1, HMAC-SHA256, etc.

Task

It is an individual work using socket programming. Client *C* and Server *S* share a password in an offline manner (e.g., a local file). Server *S* first generates a random number (64-byte), keeps it locally, and sends it to Client *C*. Then Client *C* uses this random number as the key and combines the shared password to get the HMAC value by using the HAMC-SHA1 algorithm. After that, Client *C* sends this HMAC value to Server *S* and Server *S* runs the same process and then verifies the integrity of the received message by comparing two HMAC values.

Steps

1. ***S*** and ***C*** should share a password (no more than 56 bytes). You could write it by yourself and save it in a local file.

2. ***S*** and ***C*** set up a simple chat program. (Socket)

3. ***S*** sends the random generated number (64-byte) to ***C*** and stores it locally. This number should be displayed on screen.(Hint: it's better to generate it and save it in a local file. And then the server reads it, displays it, and sends it to the client.)

4. ***S*** and ***C*** both run the HMAC algorithm to generate the HMAC value. Then ***C*** sends the HMAC value to ***S.***

5. ***S*** compares the received HMAC value and its own generated HMAC to check whether they are identical.

6. The programs on both sides should display *the shared password, the random number, the HMAC value*.

Submission

Submit a lab.zip to Canvas including two parts:

a) All the code you have for completing the task.

b) What you have learned about this lab.

c) Steps of your work (e.g., the language and library you used, problems you encountered and how you solved them, etc.). Screen captures are recommended.