Rutgers CS 419 Group Project Report

NetID1 & NetID2

October 14, 2021

1 Problem Description

What is the goal of this project? (functionality of this artifacts)

The goal of our project is to create a secure messaging system with a login system using a client-server-based connection.

Where will this program be deployed or used? (platform, users)

This program will be deployed to be used on any OS that can run python3 and its libraries and is to be implemented by users who want to confidentially send messages to one another without the possibility of a third party intercepting and interpreting the information sent between users.

2 Problem Analysis

What is the threat model? Attackers' knowledge, capability and goals?

One of the threat models is the man in the middle attack which we will soon begin testing for as well as CCA and CPA. Hopefully by making a secure login process and saving the passwords in an encrypted format as well as ensuring the RSA encryption scheme is upheld we can prevent any attackers from completely decrypting messages or learning the private keys of the users.

What is the security goal and guarantee?

The security goal is to send completely secure messages between clients and storing these encrypted messages in the server, but only fully decrypting the messages as they are passed off to the clients and by not storing any long term message data we ensure a completely secure messaging system for users who do not want information to be intercepted and encrypted by an attacker without their consent.

3 Program Design

How did you achieve your goal? functionality and security.

We plan to achieve our goal by implementing a public-private key encryption scheme through the usage of RSA encryption on the text sent and decrypted as it is recieved using python. The login system will store and encode passwords using the Sha256 encoding scheme often seen in how linux and unix secure their passwords using hash. Finally we decided to use a hmac SHA256 messages encoded by our RSA encryption.

How can it provide the security guarantee you intended?

These security protocols will be able to both send encrypted messages through the server to the client and decrypt those messages to a readable format for the clients. Hopefully as we continue to test and reapply our new security protocol we can evolve it to be completely attack proof from CPA's, CCA's, and factorization attacks

```
1 void push (int value , Stack * stp ) {
2 if ( stp - > top == stp - > size ) {
3 doubleStackSize ( stp ) ;
4 }
5 stp - > array [ stp - > top ] = value ;
6 stp - > top ++;
7 }
```

4 Evaluation

4.1 Evaluation Strategy

What and how to evaluate? platform, datasets, user study?, how to measure, effectiveness, efficiency, security

4.2 Experiments

How do you plan to do or design the experiments?

4.3 Results

What are the results?

4.4 Analysis

What do these results mean?

5 Process Description

Overall timeline.

Where are we now?

We have the RSA encoding scheme working however we still need to create a user database system and a client to server connection to actually implement and send the encoded messages to other users.

What is the plan for the next step?
The plan for the next step is to continue by testing to see if messages can be sent between clients and test to see if the RSA encoded messages are able to be encoded and decoded when sent to server and then to another client. Finally we will begin to build the user database to allow it to be open for the possibilities of multiple clients sending encrypted messages to one another.

6 Group and Artifacts

Group members and each of their contributions in %. Project repository address.

What is a proud part of this project, for each of you?

7 Questions to Answer

When do you want us to freeze the repository? 2