S/Key Protocol ReadMe

@author Adriene Cuenco
CS460 Secure Communication

Brief instruction of how to use the program.

The program begins with the main menu where one can log in,register or exit. A new user must register first before logging in. During registration the user must provide a personal ID, the number of authentications(n) and a random seed. The random seed is then ran through a secret cryptographic hash function n times and produces a password chain n-1 in length,salting. After the user registers, the user will have n-1 successful logins before the user must re-register. During login, the user must input an ID and the server responds with i. The user must then provide Password i. If cryptoHashFunct(password i) is equal to password i-1 then user is authenticated and server will replace password i-1 with password i.

Introduction of database file(s): purpose, name, location, record format

The record format of the database used is Java's Hashtable<key,value>, where key and value are strings. The key is ID and the value is the current password in the password chain. The name of the database is *database* and is located in global variables. The purpose of this database is to hash ID and current password together.

Explanations of any cryptographic functions used: where and why.

I created a method named secretHashAlgo(string) using Java's *java.security.messageDigest* library. The method encrypts passwords using SHA-256. It is used in registration to encrypt the user's provided secret seed, n times. It is also used in authentication where it encrypts the user's provided password i. If secretHashAlgo(password i) is equal to password i-1, which is the password stored in the database,then user is authenticated and password i-1 is replaced with password i.

Security analysis on the current system. (What attacks may be possible and how to defend against them)

This system can help deter password sniffing attacks. If an attacker gets a hold of the user's password that has already been used, that password is useless in this system. An attacker can also look into the database and grab password i. The attacker would need to reverse the cryptographic hash function which is known to only be one way and very difficult to do.

Other attacks involve man-in-the-middle attacks, but this can be avoided using Ipsec tunneling like SSH and SSL. Also, if the attacker knows the seed and cryptographic algorithm, the attacker may generate the password chain compromising the system. SKey is also vulnerable to collisions which has a complexity of 2^{32}. The system I built is using SHA-256, created by the NSA and is computed with 32 bit words. The reason I did not use SHA-512 which is computed with 64 bit words is because it is unfeasible to have a 64 bit encrypted hex string as a login password.SHA-256 ,which is part of the SHA-2 family, is not perfect and has its flaws. It is known to fail in preimage resistance in 52 rounds and fails in collision resistance in 46 rounds.