Kyle Koceski

Project Proposal

CIS 4360

11/5/2014

Submit a 1-2 page description of the project you propose to do related to computer security. You should include WHAT you are doing, HOW you propose to do it, WHY you think it is important, and a partial list of resources you expect to use for it

I propose to create a compression program which provides two-factor authentication for decryption. This program will combine a standard user-provided password and a randomly generated password, which will be texted to the appropriate user for decryption, to provide security based on the "what one knows" and "what one has" principles. I will be implementing this as a command-line software program similar to the Linux *zip* and *unzip*. In fact, I propose to use *zip* and *unzip* as the underlying compression software providing passwords via the -P argument. At compression time, the software will randomly generate an additional key to append to the user-provided password, which will both be used for encrypting the "zip" file and be sent to the decrypter's phone (the number will be provided at compression-time as an argument to the program).

I believe this is important because current compression software has not kept up with emerging trends: namely two-factor authentication. Thus, while many users encrypt zip files with a password, this password is usually passed in plain text along with the file during an email. By adding this two-factor authentication system to zip files, I hope to modernize the state of file transfer security.

Resources:

- Linux (Ubuntu) standard software packages, including the *zip* and *unzip* packages
- Textbelt (http://textbelt.com/) for messaging the recipient of the two-factor authentication password. Note: they'll still have to know the proper password.
- C++ to encapsulate the above programs and provide additional logic for implementing the two-factor authentication