David Im, Alper Karslioglu

Progress Report

Our team has elected to do the development project using a raspberry pi. We plan on creating a security encryption device. The device would interact with a host computer which is the computer that the user is attempting to login. A password is randomly generated from a word bank on the host, then encrypted and sent to the device. The device would then receive the message, decrypt the message, and then display the decrypted password on the screen of the device. The user would then enter the password into the host and be granted access. The device will also have a button to tell the host to generate a new password to send.

On the status of our project so far, we have acquired all the hardware needed. Because of our lack of knowledge on hardware and building a board, we have decided to focus on the software side of the project. So on the device side, it will have the basic components needed. It will use a regular monitor and a mouse. Though we understand that a real marketable device of this kind would have a smaller attached screen and a button on the device instead of a mouse, we decided against extending so far outside our range of knowledge. The board itself will be a Raspberry Pi 3 Model B Motherboard which has built in Wi-Fi capabilities and proof of purchase is attached to the submission. The host computer will be one of our personal laptops running Windows.

On the software status of the project, we have setup and installed the operating system on the device. Will be using the Raspbian operating system. On host side, we have decided to make the application for login a simple console program. It will display a simple prompt for a password. It will display a message for valid logins, invalid logins, and when the device has sent a reset password request. The software on the host device will be C++. Along with the application for login, the host software includes the random password generator using a word bank, encryption algorithm, decryption algorithm, and software for communicating with the device. So far, we have finished developing the code for the encryption and decryption algorithm. It is a steam cipher using a preset key that both the host and device will keep. The first bit of the message is XOR with the first bit of the key then second bit and so on continuing for all the bits of the message. This allows the encryption and decryption algorithm to use the same algorithm. On the device side, it uses the same algorithm but all the code for the device will be in Python because Python comes preloaded with Raspbian. The device will also need the code for communicating with the host and sending reset password requests.

On the evaluation of the project, we have decided to evaluate the limitations of the device. Specifically we want to focus on the ease of use from the user and response time. This is to evaluate how quick the user can get a password back and be able to gain access into the system as well as how quick it is to reset the password. Additionally, since the project is focusing on a security system, we thought it was appropriate to evaluate potential security flaws and how to mitigate them.