Pistachio

Deliverable: Proposal
Team: Pistachio
Members: Cameron Dziurgot, Luke Brodowski, Travis Moretz
Due Date: 20 September 2015
Submission Date: 20 September 2015

Pistachio

Mobile Authentication Proposal

With the ever increasing number of users of smartphones, tablets, and touch screen device, users are concerned of safely securing their data. Having a passkey to open a device is only one level of security. Many devices only allow for a four digit passkey which only offers a unique 10,000 different passcodes. If an unsuspecting user is not careful when unlocking their device, the passkey can easily be seen by onlookers. After watching someone enter a passkey into a device, it isn't too hard to guess the numeric passkey by watching the sequence of taps on the screen. The general motion of the hand and finger can give away where the user tapped, and by mimicking the hand and finger motion the device passkey can be guessed with relative ease.

If a passkey was more complex by adding not just the numbers tapped, but the duration of the press, the duration of the gaps between presses, and the area of the screen that one's finger contacts when pressing the screen, an unauthorized user would have difficulty accessing a device. By recording all of these variables and storing them as attributes of a vector, the degree of complexity of a passkey would give a much more secure device. This would make every passkey unique to the given user, adding another level of security.

We would like to start developing an Android application that can detect the time interval of a user's unique presses and authenticate the user based on the accuracy of those time intervals to some stored data. To start the application would be simple, allowing the user to save a passkey that was a sequence of taps or presses, as well as keeping track of the duration of each press, the duration of time between presses, and the area of the screen that was contacted by the finger. The application would then need to

compare the sequence that was re-entered against the original saved sequence and compare the two to within a degree of certainty. If the second sequence is outside the variance of acceptance, the sequence was not a match and should be logged as such. If the second sequence is within the variance of acceptance then it should be logged as a successful attempt. By performing and logging a series of attempts by different users and different stored passkeys, we will be able to collect statistics on false acceptance and false rejection of the system. Gathering these statistics will better improve the acceptance rate, and demonstrate the reliability of the security feature..

The application will need a user interface, to start a rectangle on the screen for the user to perform the sequence. A way to start and stop the recording of the sequence like a start / stop button. The system will need a way to store the saved sequence as well as all attempted re-entries of the sequence for analysis. There will have to be the main vector comparison method that will compare the re-entries to the stored “passkey”, or sequence. The comparison should indicate acceptance or rejection and the degree of certainty of it. This will help to set and adjust the parameters on the degree of certainty to make this system feasibly to use as authentication system.