NeuroPass

The next generation password system

Team: Anthony Nguyen, Abhejit Rajagopal, Sanjay Rai

EE113D, Fall 2013, Professor Briggs

Purpose:

Security issues in the modern day are increasingly important to preserve data and identity. Today, we move more and more commerce and transactions into the web. We sign contracts electronically. We can purchase nearly anything, from seldom-purchased high-end electronics to such daily necessities as groceries. Because of this, authenticity and reliability of credentials becomes more and more important.

Today, we use devices such as passwords, pin numbers, and personal devices as a means of verifying our identity online. Unfortunately, increases in computational power means that hackers and crackers are becoming especially adept at solving the password puzzle, reducing their security benefits to near zero. This holds true specifically for short, memorable passwords comprised of real words or phrases. As the complexity of passwords increase, their strength increases, as it requires more and more computing power to crack them. Yet, there are fundamental limits of passwords that cannot be surmounted no matter how complex the string of characters used to form them.

Going forward, it is now clear that passwords will become a relic of the past, as new authentication technologies are developed in order to protect users from malicious activity. Thus begins the development of our authentication solution, NeuroPass.

Objective:

We intend to the Emotive EPOC EEG in conjunction with the DSK board in order to prototype and develop a system that will allow the creation of a mental signature that can be used as a replacement for conventional password systems.

Benefits:

We wish to avoid fundamental issues of password security by making sure that only you with the unique credential of being yourself can log into and use personalized systems. If you leave your desk, your login session should leave with you, and when you return, you should be able to resume right where you left off. No one can learn what your password is and log in with your username and password, because no one else will have your unique mental signature. The use of this signature also prevents phishing, the practice of tricking users into giving up their passwords voluntarily. Also, you must be alive and fully conscious to access your login, so if you're drunk you can't log in. The system could also detect your

emotional state in order to prevent you from logging in under duress if you're being forced to authenticate. These are rigorous reasons why an EEG based system is more secure, fundamentally, than a password is.

Challenges

The design of this system will indeed be challenging. We anticipate that a lot of preliminary work will be required simply to begin, because we need to research and understand EEG signals. Subsequently, we need to find out what tools available to us and which ones are the most applicable to be used. Once we know what kind of processing we can do, we can begin to collect data. The proper method of collecting data, what one should think about to generate a unique and secure signature, will require development.

We hope that the data generated by this headset is sufficient to develop a password of any kind, because until we try this we do not know if the EPOC is even good enough to achieve our goals. We know that as this hardware technology becomes more and more refined, we can increase the complexity of the data processed, and perhaps come up with more and more complex ways of processing the data into a password.

There are other fundamental issues of using brain wave signals as a password. One issue is speed. A user who has memorized their ASCII encoded password is able to quickly enter the password at a prompt in under 10 seconds. We need to either match this speed at the same level of security, or have a greatly heightened level of security if we trade off speed. Certainly, a thought-password which consists of thinking of an event for 30 seconds will have more security than a thought that lasts only 10 seconds. Another issue may be that it could be difficult to get consistent readings between different days, different times of the day, different locations, how tired you are, etc etc. We want to avoid false positives and misreads, as well as make the system robust enough that you can use it at different places during the day.

Project Guidelines:

We will examine characteristics of the EEG waveforms obtained by the headset in order to seek out patterns in individual data collected under different testing environments. This is truly the core of the project – are there characteristics of the EEG waves that are a repeatable phenomenon for an individual? Our system must be able to identify the patterns of a person's thought at different times and find these specific characteristics, and only then can we turn these characteristics into a password.

Anticipated Timeline and Milestones

Week 6

Using the SDK that comes with the headset, test the accuracy of the detection that was written by the developers to determine the benchmark for our system. See if we can repeatably reproduce events. Begin work on our matching algorithm. For instance, write a function to check that can detect if the user did: “blink blink smile smile”

Week 7

Collect raw data with the headset, while at the same time watching the Emotiv Suite to make sure that the raw data matches up with the desired sequence. Begin to use EEGLAB and other Matlab based tools to process this data.

Week 8

Successfully be able to identify two actions, such as blinking and smiling from the raw data, in Matlab.

Week 9

Convert the Matlab code into C code to be used on the DSK, have it in a state that is ready to test.

Week 10

Make the system more robust, potentially ad in a third action that can be used with the password. Possibly convert the signal into an alphanumerical password so that the headset can be used with conventional password systems.