Brainwords: Final Report

Ernest Williams

Introduction

As the importance of cyber security becomes more apparent to society, alternatives to existing authentication methods are continually being sought after. When searching for new authentication methods, the first concern for many, is ensuring that this new method is difficult to circumvent. This idea has sparked the use of biometric authentication such as fingerprint scanning. This method of authentication is more difficult to circumvent than a typical password because it requires the presence of the user for it to work. With that being said, both passwords and fingerprint scanning can be bypassed if a malicious individual obtains their password, or forces the user to authenticate using their fingerprint. Because of this, other authentication methods are continually tested. When searching for these new authentication methods, it is important that these alternatives be both easy to use and difficult to circumvent. With that in mind we would like to assess the possibility of using a Brain Computer Interface(BCI) as a means of biometric authentication.

Brain Computer Interfaces

A BCI is a device that allows electrical signals from the brain to be read and mapped to certain commands or actions on a computer. [1] For example, these devices can allow a user to move a computer cursor by thinking a certain thought. In order for this to work, users must *train* the computer to understand when a user is thinking that they want to move a cursor. To do this, the user records this thought repeatedly until the computer is able to recognize this specific thought. These thoughts are interpreted by the computer as a pattern of electrical signals.

There are two forms of BCI devices; *invasive*, and *noninvasive*. An *invasive* BCI device requires a device to be surgically implanted into the user's brain. A *noninvasive* BCI device requires no surgery. The device is placed on the head of the user. Generally, because an invasive BCI device is surgically implanted, it is able to receive a more reliable signal than non-invasive BCI devices. Non-invasive devices depend on direct contact to the skin of the user. This can be made more difficult dependent upon the amount of hair that a user has, or the thickness of their hair.

Objective

The purpose of this research is to determine the efficacy of BCI devices as a means of authentication. More specifically, we want to assess the use of commercially available, *noninvasive* BCI devices. The decision to use these devices was made based on the idea that new methods of authentication should be easy to use. Because these devices can be purchased by anyone, it would be easy for new users to obtain these devices and use them for authentication. Also, because these devices are noninvasive, there is no risk involved in the devices use.

The devices that we decided to analyze are the EMOTIV INSIGHT, the EMOTIV EPOC+, and the MUSE. These devices were chosen because they were available in the lab. Also, each device has a different amount of sensors that could result in different levels of success in authentication. More specifically, the INSIGHT has five channels, the EPOC+ has 16 channels, and the MUSE has 5 channels. Channels are the connection points that are made between the user's head and the device. These connection points correspond to different points of the brain based on the International 10-20 standard. These points can be seen in *Figure 1*. This testing has previously been done with a single channel device which is why it is desirable to complete this testing using devices with more channels. [2]

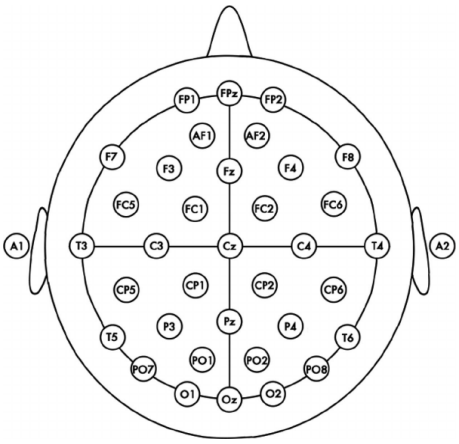

Figure 1: Connection points of the brain based on the International 10-20 Standard

Experimental Setup

During the experimentation process there were two things that were tested: practicality and authentication.

Practicality Testing

For practicality, testing was done to determine the amount of time it takes a user to set up each BCI device to be use for authentication. This was chosen as the means of determining what is practical for users because individuals will be more reluctant to adopt new methods of authentication that increase the time it takes for them to authenticate themselves for a certain device. The setup process for each device is different.

For the MUSE, the setup process requires the user to connect the device to a computer via Bluetooth. After this, the device must be placed on the user. To do this, the band of the device is placed across the user's forehead, and two sensors rest on the user's temples.

Figure 2: MUSE EEG Headset

For the INSIGHT, the setup process requires the user to connect a USB dongle to a computer. Once this is done, the INSIGHT must be connected to the dongle via Bluetooth. Once these steps are completed, the device is placed on the user's user's head. Each sensor on the device must be adjusted to make a good connection with the specific point on the user's head.

Figure 3: EMOTIV INSIGHT EEG Headset

For the EPOC+, the setup process requires the user to connect a USB dongle to a computer. Once this is done, the EPOC+ must be connected to the dongle via Bluetooth. The next step to settings up the EPOC+ is to wet each sensor on the device by placing the felt sensors in a saline solution. Then each sensor is placed back into the headset. Once this is done, the headset is placed on the user's head, then each sensor is adjusted until the desired level of connection is reached.

Figure 4: EMOTIV EPOC+ EEG Headset

For the EPOC+ and the INSIGHT, the desired level of connection is determined using the EMOTIV Control Panel software which shows the level of connection for each sensor. This can be seen in *Figure 5*. For the MUSE, the device was simply placed on the user's head as securely as possible.

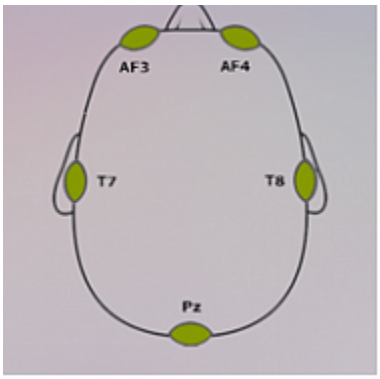

Figure 5: EMOTIV Control Panel showing desired connections

Authentication Testing

For authentication testing, the goal was to determine if the electrical signals received from two different users will correlate for the same stimulus. The motivation behind this was to determine how safe this method of authentication would be if a malicious individual knew what the user was thinking when trying to authenticate themselves. To test this, subjects were sat in front of a screen. The subjects were instructed to focus on the screen and countdown from 10 to 1 following a countdown on the screen. While the user did this, the electrical signals were being recorded into MATLAB. This recording was done for three days, with a recording being taken from each subject in the morning, afternoon, and evening. The motivation behind testing as different points in the day was to determine if the signals from a subject would differ between different times of the day, different days, or both.

Due to the time available to complete this testing, the INSIGHT was chosen to be used for authentication. This choice was made because the EMOTIV line of devices has an existing developer's suite that allows individuals to more easily access and manipulate data received from these devices. The INSIGHT specifically was chosen due to the small number of channels which makes the setup time significantly less than that of the EPOC+.

Results

Practicality Testing Results

Device	Prepare BCI Device	Desired connection	Total
EMOTIV EPOC+	20s	1560s	26.3 min
EMOTIV INSIGHT	5s	135s	2.33 min
MUSE	7s	75s	1.36 min

Table 1:Average time values for setup of each BCI device

The results in the table above correspond to the overall time it takes to set up each BCI device. The "Prepare BCI Device" column refers to the steps taken before placing the device on the subject's head. The "Desired Connection" refers to the amount of time that it takes to adjust the device on the subject's head to a point where a consistent successful connection is shown as seen in *Figure 5.*

Authentication Testing Results

	U1T1	U1T2	U1T3	U2T1	U2T2	U2T3
U1T1	1	-0.0168	.1143	-.0636	.2700	.0301
U1T2	-0.0168	1	-.2216	.0383	-.1190	.6088
U1T3	.1143	-.2216	1	-.0884	-.0298	-.0816
U2T1	-.0636	.0383	-.0884	1	-.0361	.01768
U2T2	.2700	-.1190	-.0298	-.0361	1	-.0097
U2T3	.0301	.6088	-.0816	.01768	-.0097	1

Table 2: Correlation values for two subjects

The table above shows the correlation values for data recorded. In this table, U corresponds to user, and T corresponds to trial. The correlation was calculated using the Pearson Product Moment formula for correlation which measures the linear relationship between two sets of data from -1 to 1. This equation can be seen in *Equation 1.*

$$r_{XY} = \frac{\sum (X - \bar{X})(Y - \bar{Y})}{\sqrt{\sum (X - \bar{X})^2 \sum (Y - \bar{Y})}}$$

Equation 1: Pearson Product Moment Correlation Formu

Conclusions

Based on the data gathered, we must conclude that commercially available BCIs are not currently an efficient means of user authentication. This conclusion is based majorly on the inconsistency in the correlation values shown in *Table 2.* When calculating correlation values, the desire was for there to be a high level of correlation when comparing two trials taken from a single subject. Furthermore, it was desired that the correlation value be low when comparing trials between users. With the data we were able to gather, there are multiple times where there is a higher value of correlation between two different subjects. With that being said, from a statement of practicality, BCI devices could be used for authentication. Devices such as the MUSE or INSIGHT that have a small number of channels will be more desirable because they take minimal time to setup.

Future Work

In the future the practices used to conduct this research could be improved upon. While analyzing the data that was collected, there were differences in the amount of data points collected during each recording session. This may have been caused to the device disconnecting during the recording. Also, there were different spikes in the data on certain recordings that would not occur in other. To address these concerns, it may be desirable to do longer recording session. This would allow the researchers to determine if certain moments in a user's recordings are spikes, or if it is normal for that user. Also, the MUSE and EPOC+ should be tested for authentication purposes to determine if they provide data that can be used for authentication.

References

[1]"Brain-Computer Interface (BCI)". *ALSA.org*. N.p., 2016. Web. 1 Aug. 2016.

[2]Cook, Ian et al. "Figure 2. Electrode Montage. We Used A Standard Extension Of The...".*Researchgate.net*. N.p., 2016. Web. 1 Aug. 2016.

[3]Chuang, Nguyen, Wang, and Johnson. "I Think, Therefor I Am: Usability and Security of Authentication Using Brainwaves". *1-16*

[4]"What Does Muse Measure? - Muse: The Brain Sensing Headband". *Muse: the brain sensing headband*. N.p., 2016. Web. 1 Aug. 2016.

[5]Pete, Sailor et al. "Emotivinsight Update". *3D FilaPrint*. N.p., 2014. Web. 1 Aug. 2016.

[6]"EMOTIV - Brainwear® Wireless EEG Technology". *Emotiv*. N.p., 2016. Web. 1 Aug. 2016.

[7] Panel, EMOTIV. "EMOTIV Control Panel - Emotiv". *Emotiv*. N.p., 2016. Web. 1 Aug. 2016.