Todd Leetham
GSEC Practical Assignment
Version 1.4b Option 1
January 22, 2004

Thinking Your Way In: Futures in Biometric Authentication

Abstract

As necessity is the mother of invention, it is also the enabler of the imaginative. New developments in the field of neural interfaces give rise to interesting applications beyond their intended powers of helping the disabled to move or communicate. This serves to augment not only the abilities of the physically disabled, but others of us as well.

This paper discusses the possible future use of certain Brain-Computer Interface (BCI) approaches as biometric authentication methods. The BCI methods discussed include the biofeedback method known as electroencephalogram and the much more recent motor-neural interface. It explores whether or not these methods meet the definition of a biometric device. It compares these methods to other more current biometric methods in terms of accuracy, submission and matching challenges. Also, it discusses their potential use as a solution as well as their social, health and technological impacts.

What are Brain-Computer Interfaces?

A Brain-Computer Interface in most generic terms could be defined as a mechanism by which signals from the brain are interpreted by a device that is used to control or direct a device, computer or computer program. A few technologies exist today to accomplish these goals. Two technologies in particular, electroencephalogram (EEG) and motor-neural interface (MNI) are emerging to the forefront of research and use.

An electroencephalogram-based BCI system can be described as:

> A system [that] uses oscillatory electroencephalogram (EEG) signals, recorded during specific mental activity, as input and provides a control option by its output. The obtained output signals are presently evaluated for different purposes, such as cursor control, selection of letters or words, or control of prosthetics. [3]

Typically these EEG signals are recorded mu (8-12 Hz) and beta (18-25 Hz) band signals via non-invasive sensors attached to the scalp over the areas of the brain that best reflect motor-neural activity.

A Motor-Neural Interface (MNI) BCI can be described as:

> [An] interface that consists of an internal neural signal sensor and external processors that convert neural signals into an output signal under the persons own control. [4]

The MNI method is a bit more invasive than the older EEG method. In a newly developed product from Cyberkinetics known as BrainGate™, a chip approximately 2-millimeters square with 100 electrodes is implanted by surgeons and attached to neurons in the motor cortex located in the brain just above the right ear. [5]

Are Brain-Computer Interfaces Biometric?

In order to adequately answer this question, we must define a biometric device. The National Institute of Science and Technology (NIST) defines biometrics as automated methods of recognizing a person based on a physiological or behavioral characteristic. [6] Unfortunately the line between physiological and behavioral characteristics becomes blurred when applied to these two BCI technologies.

In Lawson's paper "The New Wave 'Biometric Access & Neural Control'" biometric aspects of EEG are described:

> While it is true that a person has the ability to alter most of their own brainwave patterns, they cannot alter what is referred to as their baseline brainwave pattern. Therefore, a tentative conclusion would be that an individual's baseline brainwave pattern could feasibly meet the qualifications of a biometric and hence has the potential to be recognized as the newest biometric security solution. A solution we dubbed as an "EEG Fingerprint." [10]

The theoretical "EEG fingerprint" which is based on an individual's baseline brainwave pattern could be considered physiological, or something that is physically unique to each individual. Although this baseline brainwave pattern does not change, the brainwave pattern does depending upon activity, and therefore also serves as a potential behavioral mechanism.

Motor-neural interfaces do not seem to show similar physiological characteristics per se, but current research has not pursued that direction. It does, however, have a particularly strong behavioral characteristic. It allows subjects to control devices in real-time. Experiments with neural implants in monkeys had them moving a manipulandum (analogous to a computer mouse) that controlled a cursor in order to hit targets at arbitrary locations on a video monitor. The neural patterns associated with a variety of movements were observed. Later, based on interpreted “intentions” the monkey was able to move the cursor and hit the targets without the use of the manipulandum. [2]

The technological requirements of biometric devices go beyond the simple definition of recognition. We must determine if BCIs are capable of performing the biometric functions of identification and verification through enrollment, developing templates and accurate template matching.

In biometric terms, identification happens when a biometric template or sample of the physiological or behavioral characteristics is compared against many other such biometric templates for a match. For the EEG-based BCI we can consider that the “EEG Fingerprint” would be used as the template to match against. What we don’t know is whether or not we can control or encourage someone to present a baseline brainwave pattern.

In terms of the MNI-based BCI it becomes much more difficult to perform real identification. Because it is a technology that reads motor cortex neurons in an attempt to interpret intent of movement there is not necessarily a baseline to measure. Unless the pattern that is read from the individual for the same movement (let’s say touching your nose with your right finger) is different, then we have no unique template to sample or match against.

Verification is “the process of establishing the validity of a claimed identity by comparing a verification template to an enrollment template.” [7] In the EEG-based BCI example the same questions apply. Will your one-to-one match be inaccurate due to factors that don’t allow the person to present the proper baseline brainwave pattern? The MNI-based BCI presents an even bigger question, because now a person can match a pattern of though which might correspond to a pattern of movement. This is analogous to someone typing a password in on a keyboard to enter a system. This brings up the question that it might be biometric because it is now based on motor neural firing patterns, something that is physiological in nature. The conclusion may be a bit of a stretch, but it is definitely something that forces us to re-evaluate the definition of a biometric device.

Enrollment, which is defined as “the process whereby a users’ initial biometric sample or samples are collected, assessed, processed and stored for ongoing use in a biometric system” [7], is essential to both the identification and verification biometric functions. “Key elements in choosing a biometric system include ensuring that the enrollment process is relatively simple for the user, requires a short period of time, and provides a high quality template.” [9]

Typically feature extraction is used to generate a template for enrollment, the techniques are all different depending on the biometric technology. The challenges of EEG-based BCI feature extraction are explained below:

"Current Trends in Graz Brain-Computer Interface Research" lists EEG feature extraction methods:

1) calculation of band power in predefined, subject-specific frequency bands in intervals of 250 (500) ms;
2) adaptive autoregressive (AAR) parameters estimated for each iteration with the recursive least squares algorithm;
3) calculation of common spatial filters [3]

The article goes on to also conclude on the accuracy and usefulness of those methods:

> The classification results show that all methods used, 1) bandpower, 2) AAR, and 3) CSP, result in low classification error rates after some sessions. At this time, the standard method used at our lab is AAR parameter estimation with the RLS, combined with the LDA algorithm. AAR models have the advantage that it is not necessary to specify the reactive frequency band, as it is for the bandpower method. [3]

Considering these options, it would be cumbersome to have a biometric device constantly having to retune itself to accommodate the bandpower method. By the same token, the CSP method requires a larger sensor array where particular sensors are weighted accordingly for importance is not as accommodating as the AAR method. Still enrollment would require individuals to either accept scalp sensors in order to utilize EEG-based biometric authentication devices.

The challenges of MNI-based BCI feature extraction relate primarily to its initial invasive nature. Because of this, the deployment technology would need to be highly developed and safe for humans. A major commitment to this method of biometric authentication would have to be made on some scale as well due to the fact that the somewhat delicate surgery makes contact with motor cortex neurons. Outside of those concerns, the user would likely have to go through a movement series several times in order to provide an adequate feature sample.

Another very important aspect of enrollment is the time it takes to read a template. The assumption has to be made that the sensor placing / wearing process for EEGs or the implantation surgery for MNIs would already have to have been done prior to enrollment in order for it to meet the timeliness and convenience requirements of a biometric.

For EEGs, let's make the assumption that we are using the AAR method for gathering the biometric template. In experimental trials related to measuring a baseline then detecting movement by changes in the brainwave patterns, all cues for the subject to begin thinking of movement happened at 2 seconds. We can conclude that at 2 seconds the baseline pattern was at least read and ready to interpret movement. Obviously more study would need to be conducted in the realm of how long on average it takes to get a normal baseline reading. The experiment described above concentrated more on detecting and interpreting intent of movement. It is conceivable that several attempts to enroll could take up to a minute.

MNIs like BrainGate™ are designed to relay movement signals in real time. Although they are not providing a "neural fingerprint" per se, they are relaying behavioral responses of movement. The enrollment delay then becomes transferring the data from the implanted sensor to the device for interpretation and matching. A user could be asked to plug a connector into his/her implanted socket and perform the thought of the required movement series for authentication.

I have found no studies or numbers associated with the timing of this in any way. I would estimate that each enrollment sample could take between 5 and 20 seconds to collect. An alternative solution that might reduce enrollment time could be that the socket is plugged into a wireless transmitter that is also worn by the user or located above the right ear near the implantation point and the behavior data is transmitted to a reader.

Comparison to Current Biometric Methods

It is important to compare BCIs with the current biometric methods in order to understand how they fit into the biometric landscape. Different types of biometric methods lend themselves to either a physiological, behavioral or morphological set of characteristics. [1] Let us consider fingerprinting, hand geometry, iris patterns, voice patterns, and signatures in terms of submission, accuracy and matching challenges. Accuracy in biometric devices is usually measured in terms of False Acceptance Rate (FAR) and False Rejection Rate (FFR) and their function one-to-one and one-to-many for the identification and verification functions discussed above. FAR describes the number of times a template is mistakenly accepted as valid and FFR describes the number of times a valid template is rejected. [14] These terms will be used when referring to the accuracy of a biometric method.

Fingerprinting is one of the oldest and probably most widely used methods of biometric authentication. "The use of fingerprints to identify people dates from the 1800s." [1, p.249] The submission process takes place as follows:

> when prompted, the user gently places his or her finger on a postage-stamp sized optical or silicon surface. The user must generally hold the finger in place for 1-2 seconds, during which automated comparison and matching takes place…Typical verification time from "system ready"

prompt: 2-3 seconds. [7]

Problems with fingerprinting matching and submission include cold, dry or oily fingers, extreme humidity, proper placement, finger pressure, and finger disfigurement. These things can significantly slow submission. Additionally fingerprints (or fingers!) can be lifted and re-created in order to foil authentication. “Fingerprints have been shown over many years to be highly accurate. That is why they are admissible as evidence. Accuracies (1:1 FARs) in the area of .0004% are not uncommon.” [8]

Like fingerprinting, hand geometry systems examine unique characteristics of your hand and use that information to determine whether you should be allowed access. [1] In a similar method to fingerprinting above, the hand is placed on a hand-sized plate that scans the hand shape and compares the scanned data with the stored template. Scanning and verification times are comparable to fingerprint submission, 2-3 seconds. Hand geometry also suffers from the same challenges as fingerprinting matching such as cold, dry, oily, disfigured hands, swelling, rings and even nail polish. Hand geometry falls victim to potentially being lifted and duplicated to foil authentication. “Handprint systems are said to be less reliable than fingerprint systems.” [1, p.250]

Iris patterns are determined by the furrows and striations of the iris. Submission happens when the “user positions him or herself near the acquisition device (peripheral or standalone camera). User centers eye on device so he or she can see eye’s reflection. Depending upon the device, the user is between 2-18 inches away. Capture and verification are nearly immediate. Typical verification time from “system ready” prompt: 3-5 seconds.” [7] Movement of the head or eye, glasses, and colored contacts affect an accurate and timely submission. Iris patterns are extremely accurate. “Because an average iris contains 255 feature points of high entropy, this results in a theoretical false accept rate of 1 in 1078. In fact, to date no false accepts have been reported.” [8]

Voice verification systems take advantage of the unique vocal characteristics of your voice. Users typically will speak a particular phrase into a microphone or other audio sampling device for submission purposes. Depending on the phrase and nearby acoustics, submission can take from 4-6 seconds. [7] Issues with proper submission include respiratory diseases, injuries, stress, and background noise. [1] Although some algorithms can detect the sub-harmonics associated with a tape recorder, some high quality digital recordings can fool these systems. Although the method is more intuitive than others, usual speaker algorithms look at around 28 different voice characteristics. [8] I would conclude that it is generally less accurate than the other methods.

Signatures are an old biometric method, comparable to fingerprinting. Who could mistake John Hancock’s signature at the bottom of the Declaration of Independence? The signature submission process is described as follows:

> With a signature verification system, you sign your name, using a biometric pen, typically attached by a cable to a workstation. The pen, or the pad on which you write converts your signature into a set of electrical signals that store the dynamics of the signing process (e.g., changes in pressure as you press down lightly on one stroke and more forcefully on another). [1, p. 251]

The verification of a captured signature scan would take between 4-6 seconds. [7] A problem with using signatures as a biometric are injuries to the arm or hand that the person uses to sign. Because of the fairly low amount of skill it takes to forge a signature, their accuracy comes into question as well when compared to the other methods. It is probably below voice recognition in terms of reliability. Unfortunately, signatures are very widely accepted as a biometric method because of their simplicity.

In comparison, I have to say that BCI submission would be similar to the iris pattern submission where the head (with sensors or implant in place) are placed into a submission area and either plugged in or scanned. Their submission times would be on par with the other methods, between 2-20 seconds. An advantage that BCIs have is that they don’t seem to suffer from many of the disadvantages of the other methods. Environmental factors like temperature or humidity, physiological effects of skin moisture, skin damage, amputation, sickness, obstructive devices like glasses or contacts. They are also not as likely to be the subject of theft or forgery. Another advantage of BCIs is that it would enable biometric authentication for the disabled in many cases where current methods do not. Quadriplegics, people with damaged eyes, missing hands, mute or paralyzed could benefit from BCI authentication. Problems with the BCI method include potential submission speed issues and those affected by stroke and other neurological diseases like Alzheimer’s.

In terms of cost, BCIs are also not as cheap or easy to implement as a voice or signature biometric method. They would more likely be on the scale of an iris or fingerprint submission method. The costs to develop BCIs as a biometric method may also prove to be prohibitive early on.

In terms of accuracy, there is no current FAR or FFR accuracy data related to BCIs, as they are not currently in wide use as biometric methods. In experiments with continuous feedback for EEG-based BCIs error rates were between 5 and 9 percent using the AAR approach. [3] However, these experiments were based on detecting movement and not on reading a baseline brainwave pattern. MNI-based BCIs have no inaccuracies from being read per se, there are mainly only variations in normal muscle control versus those detected by the motor neural sensors.

The Best Solution

So then, what is the best solution? It would depend upon what your authentication needs are as well as the cost and ease of the solution. It is still to early in development to tell what those costs might be. Perhaps until the full capabilities of the technology are explored, an early-adoptive, but multi-modal approach is required. Multi-modal approaches are useful because not only would it strengthen the authentication, it would also reduce the False Acceptance and False Rejection rates associated with biometric methods. [11]

EEG-based systems seem to perform better as biometrics individually because, like fingerprints, they potentially represent a physical characteristic. MNI-based systems could provide an alternate interface where others are not be available and might also be considered a behavioral biometric. Here are illustrations of an example of multi-modal implementation for BCIs: an EEG baseline brainwave pattern coupled with a PIN (which could also be entered via MNI), or the combination of an iris scan and an MNI-based thought of a toe wiggle and an elbow twitch.

Impact of BCIs as Biometric Devices

Movies such as ‘Johnny Mnemonic’ and ‘The Matrix’ give the public distinct impressions about the use of BCIs and their impact. There are many concerns about these types of devices potentially being harmful or controlling, something that definitely does not lend itself to adoption by people who would use biometric devices. Not just for reasons of health but it is also a privacy issue. Chaim Yudkowsky describes the comfort issue in his article “Biometrics: The passwords of the Future”:

> Despite its potential, your adoption of biometrics does require that your users be comfortable with it. Therefore ease of use is a critical component. Also, users must understand how the biometric input will be used and that the data is of limited usefulness to others. [12]

Other privacy related questions abound. Will someone be able to determine my favorite color, propensity for disease, sexual preference, or predisposition to terrorism from by baseline brainwave pattern? Will my reading give a false positive impression that I am guilty of a crime? Or about to be? Will we need to create laws that prevent the abuse of having my brainwave pattern in a database? Could we potentially be the victims of the systems that we plug into? Could they reprogram us? BCIs as biometrics could also ensure that not only are you present to use your credit card, but tell the retailer that you are in the right frame of mind to shop.

Outside of privacy there are other social impacts. Are there religious concerns about the use of BCIs? Do they violate any tenets? Will some religions consider it an abomination along the lines of human cloning? Will the cost of their development keep them in the hands of the wealthy? When would they be truly accessible to the public? When is it acceptable to implant MNIs in people? Only at the time where they require biometric access? Or perhaps eventually it will become widely accepted to implant sensors in children or babies.

Of course there are the health concerns. What are the health risks associated with the long-term use of EEG sensors or MNI implants? Are there risks of infection? Can EEG-based BCI sensors be adequate when they are worn over the hair rather than attached directly to the scalp? How many times over a person's lifetime would they have to go through a maintenance or re-implantation process for an MNI sensor?

Will we just show up to work and sit down with no keyboard? I imagine that it will go beyond that. People will not necessarily go into an office. Users could work through a console without peripherals or perhaps a semi-opaque HUD where signals transmitted directly to their visual and auditory cortexes give an interface without physical properties and are authenticated by thought alone.

How soon can we expect the future of BCIs to unfold? EEG-based BCI research has been going on for several years and continues to develop. MNI-based research has also developed dramatically over the last couple of years. Cyberkinetics has asked the Food and Drug Administration for permission to test the device on humans. Clinical trials for BrainGate™ are estimated to begin this year. Cyberkinetics also says they expect researchers will be plugging in 5 people by then end of 2004. If trials go well, they expect that they will have a product on the market by 2007. [5]

Although there are many unanswered questions concerning BCIs, I believe in the need to explore their applications. I will continue to watch their development closely. This could very well be the future of biometric authentication, as we know it.

References

[1] Russell, Deborah & Gangemi Sr. G.T. Computer Security Basics O'Reilly & Associates, Inc. 1991. 246-252.

[2] Serruya, MD et al. "Instant neural control of a movement signal." Nature Vol. 416 14 Mar 2000 (2000): 141-142

[3] Pfurtscheller, G. et al. "Current Trends in Graz Brain-Computer Interface Research." Jun 2000. URL: http://icat.snu.ac.kr/review_paper/11.pdf (17 Jan 2004).

[4] Cyberkinetics, Inc. "Cyberkinetics Presents Innovative Direct Brain-Computer Interface For Clinical Use In Motor-Impaired Human Patients." 10 Nov 2003. URL: http://www.cyberkineticsinc.com/CKI-SFN-FINAL-11.10.pdf (16 Jan 2004).

[5] Philipkoski, Kristen. "Transforming Thoughts Into Deeds" Wired 14 Jan 2004. URL: http://www.wired.com/news/medtech/0,1286,61889,00.html (15 Jan. 2004).

[6] NIST, ITL. "About Biometrics." URL: http://www.itl.nist.gov/div895/biometrics/about.html (19 Jan 2004).

[7] "Biometrics." URL: http://www.biometricsinfo.org/biometrics.htm (19 Jan 2004).

[8] "Biometric Applications" URL: http://www.rofin.com.au/pr_bssfaq.html (20 Jan 2004).

[9] Palmgren, Keith "Biometric Authentication, An Introduction" Apr 2000 URL: http://www.netip.com/articles/keith/biometric_authentication.htm (19 Jan 2004).

[10] Lawson, WJ. "The New Wave 'Biometric Access & Neural Control'" 24 Apr 2002. URL: http://inet2002.org/CD-ROM/lu65rw2n/papers/t10-a.pdf (16 Jan. 2004).

[11] Lawson, WJ. et al. "Biometric Access & Neural Control: let me in" 24 Nov 2002.URL: http://www.technologyreports.net/securefrontiers/?articleID=684 (16 Jan 2004).

[12] Yudkowsky, Chaim. "Biometrics: The Passwords of the Future" 1999. URL: http://www.byteofsuccess.com/columns/biometric.asp (22 Jan 2004).

[13] Wolpaw, JR. Brain Computer Interfaces For Communication And Control" 2000.URL: http://nichd.nih.gov/about/symposium/wolpaw_abstract.htm (17 Jan 2004).

[14] Kuster, Lisa. "An Overview of Biometric Technologies" 22 Oct 2003. URL: http://www.giac.org/practical/GSEC/Lisa_Kuster_GSEC.pdf (16 Jan 2004).

[15] Olsson, Tricia. "Strengthening Authentication with Biometric Technology" 26 Aug 2003. URL: http://www.giac.org/practical/GSEC/Tricia_Olsson_GSEC.pdf (16 Jan 2004).