Investigating an Intrusion Prevention System for Brain-Computer Interfaces

Saul D. Costa, Dale R. Stevens, and Jeremy A. Hansen

Norwich University, Northfield, VT 05663, USA
{saulcosta18,voltechs}@gmail.com, jeremyhansen@acm.org

Abstract. Neurosecurity focuses on the security of the increasingly intimate coupling of human brains and computers, addressing issues surrounding modern computer security and how they relate to brain-computer interfaces (BCIs). Although several elements of this field are not yet relevant in today's society, the goal is to examine what can be done to avoid the post-patch-just-in-time security solution seen in today's computer architectures and networks. Modern computer security has been the unfortunate result of afterthought; patched on out of necessity, often just-in-time at best.

1 Introduction

Neuroscience, the field of study relating to the brain's structure and nervous system functionality, has received increased attention in recent years as educational institutions and government organizations are realizing the potential in precisely interacting with the brain through technology. Researchers and developers of technology are beginning to explore ways to interface with a brain using devices such as prosthetic limbs [10]. In the past, researchers have recorded the electrical charges discharged across the scalp by a brain by employing brain-computer interfaces (BCIs) such as electroencephalogram (EEG) headsets [12]. BCI-enabled technological devices expose critical security vulnerabilities not only for the device, but the physical brain as well. Neurosecurity is a new field of study of vulnerabilities in the brain and BCI-enabled devices [4]. The objective of this research paper is to apply intrusion prevention methods used in computer networks to devices and neurological systems enabled with a BCI in a device agnostic manner.

Until recently, the idea of a brain susceptible to attack via a technological interface has not been considered. This oversight is due to previously limited BCI-enabled devices such as cochlear implants and those that aided the restoration of sight, which lacked the ability to affect the state of a brain [14]. The aforementioned devices have been described as invasive, and because of the complexity of implanting such a device, their danger to the user and inability to stimulate specific areas of the brain; they have not seen widespread deployment.

L. Marinos and I. Askoxylakis (Eds.): HAS/HCII 2013, LNCS 8030, pp. 23–28, 2013.

A new technology called optogenetics has enabled the activation of individual neurons within a brain in a manner that is safe to the subject [8]. Considering there are on average over eighty billion neurons in the human brain, optogenetics is far ahead of similar technologies [13]. Optogenetics works by infecting specific neurons with light-sensitive algae infused with genes such as channelrhodopsins and activating them with ultraviolet blue light [3]. Using other genes and wavelengths of light, researchers have also been able to inhibit activity within specific neurons, which prove extremely effective in the research and treatment of epilepsy [9]. Although still complex to implement and not yet in use with human subjects, optogenetics has allowed for a variety of new applications of neuroscience: more effective restoration of vision, treatment of post-traumatic stress disorder, movement control, and triggering the recall of thoughts [2,11].

In the world of computer networking, a device referred to as an Intrusion Prevention System (IPS) is used to keep unwanted traffic out of private computer networks. This device is positioned at the edge of the network and filters all traffic to internal devices. If the traffic appears to be dangerous to the machines residing on the network, the IPS rejects the traffic. This is done by examining the traffic and comparing it to a set of static rules regarding the types of traffic allowed or disallowed [15]. The IPS examines the traffic's origin, its destination, and what type of service it is requesting. Intrusion Prevention Systems are far from perfect; computer networks are compromised daily around the world, costing companies and governments billions of dollars each year [1]. When a computer network is compromised, sensitive or valuable data is often lost. Contrast this with the effects of a compromised BCI-enabled device, given its ability to affect a person's brain. The outcome of a successful attack could be much worse and potentially result in the loss of human life [4].

There are other methods employed to keep computer networks safe in addition to an IPS. Antivirus programs typically reside on a user's personal computer and watch for abnormal or malicious looking program activity. Because the programs an antivirus system examines are rarely identical, it must take a more dynamic approach than the methods used by an IPS in how it defends the computer. To achieve this, it maintains a list of what dangerous program activity looks like, referred to as signatures. If it sees one of these signatures appear within a program's code, it will prevent the program from executing. Antivirus software also watches for programs that were created by individuals known to produce malicious software. This approach has facets that could be implemented in a neurosecurity system.

A neurosecurity system would require certain functionality that would ensure its effectiveness with dynamic input. First, it must be resilient to attacks at the network layer. If the system relies on a TCP/IP network, the proper steps must be taken to ensure that traffic routed to the device travels through secure channels. Common network security methods such as encryption would do well in

this situation, as would certificate authentication. Furthermore, the neurosecurity application itself must be developed in a manner that protects the program code from exploitation. The hardware used by any BCI-enabled device must also be resilient to attack. These concepts are not new, but it is crucial to make sure that the manner in which a neurosecurity system is implemented is effective in preventing intrusion.

There are several actions malicious entities could perform after a successful attack against a BCI-enabled device, whether it is a device affecting the state of the brain or an external device such as a prosthetic limb. If an attacker were able to access the BCI, they could potentially release harmful or deadly combinations of neurotransmitters into the brain, capture the user's thoughts, or modify the user's neurological processes [4]. An attack on a BCI-enabled device that does not interface directly with the nervous system (e.g. a prosthetic limb) may not have direct physical effects on the user, however it could disable a device the user requires to sustain an important part of their life. Considering that BCI-enabled devices may one day permeate educational, government, military, and private settings, devices in need of protection could be as prevalent as personal computers are today.

2 Signal Processing and Neural Networks

Several different methods would be necessary to develop a security system to protect a brain or BCI-enabled device. In the field of neuroscience, there are methods by which a brain wave captured using a device such as an EEG headset can be characterized and classified [16,17]. So far, these methods have been used to classify whether a particular brain wave falls on the spectrum of a specific disorder such as epilepsy [16]. This requires a brain wave to first be converted from an analog signal into a digital format for a computer program to process. There are several methods use by researchers to convert the analog signal, the most popular currently being the Discrete Wavelet Transform (DWT) algorithm which takes raw brain waves as input and produces a matrix of numbers [7,17]. Wavelet transforms are also extremely adjustable in the depth of granularity with which they process a given signal, a useful feature that a neurosecurity system could employ. Examining a brain wave too closely results in unnecessary processing and increased storage requirements, whereas not examining it in enough detail would generate outputs that are not accurate enough to be useful.

Because no two brain waves are identical, a set of hardcoded rules would limit the usefulness of filtering signals in a BCI-enabled device. An artificial neural network (ANN) is modeled after a simple brain and consists of a directed graph with weighted edges between the vertices [16]. An ANN is trained by adding weight to particular edges to represent the strength of that edge and direct the flow of data within the ANN, and are efficient at solving nonlinear problems that share varying degrees of similarity.

One of the properties ANNs share with biological brains is the ability to learn. This can be done in the form of "training", whereby an ANN is fed data in a controlled manner with the outcomes known, and is rewarded for correctly classifying or otherwise outputting the expected result. This property also allows ANNs to learn from experience, which make them strong candidates for keeping pace with evolving intrusion techniques in the paramount task of guarding the brain. As such, ANNs are an ideal technology for working with brain waves [16]. After brain waves have been converted into a digital format using a DWT, they will be used in conjunction with a predetermined classification enumerating the danger of each input to train an ANN. The ANN then learns the patterns between the input and the classification, and after enough training, will develop signatures similar to those used by antivirus programs. Once these signatures have been developed, just the digitized brain waves can be input, and the ANN will return the danger classification that best matches that input. This process will result in an ANN that can examine input to BCI-enabled devices for dangerous patterns, much like an antivirus examines program code for malicious functionality.

3 Security System Architecture and Interface

Currently, most BCI-enabled devices can only read activity in the brain for the purpose of interpreting the intentions of the user. The applications that directly stimulate specific parts of the central nervous system to produce some useful effect (e.g. cochlear) are generally ineffective because of the electrical stimuli used. This method of neurological modification will trigger or even harm surrounding parts of the brain. However, through the development of more precise technologies like optogenetics, seemingly futuristic methods become realistic [10]. The aforementioned functions merely scratch the surface; it has already been shown that the bodies of mammals–rats and monkeys–can be controlled through the use of optogenetic BCIs [6]. Future applications will likely go beyond medical applications of neuroscience, and will be used in everyday life to teach and enable humanity. Because of this widespread deployment, neuroscience and BCI-enabled technologies could be more damaging than any disease outbreak in history [5].

To enable technology developers to include a neurosecurity system with their device without unnecessary effort, the security system must include what is referred to as an Application Programming Interface (API). An API is used to tie a program to another one without requiring existing code to be rewritten. Rather, the functions that are required to allow the new program to interact with the existing program are made accessible to the developer. The availability of an API will help to ensure widespread deployment of the neurosecurity system.

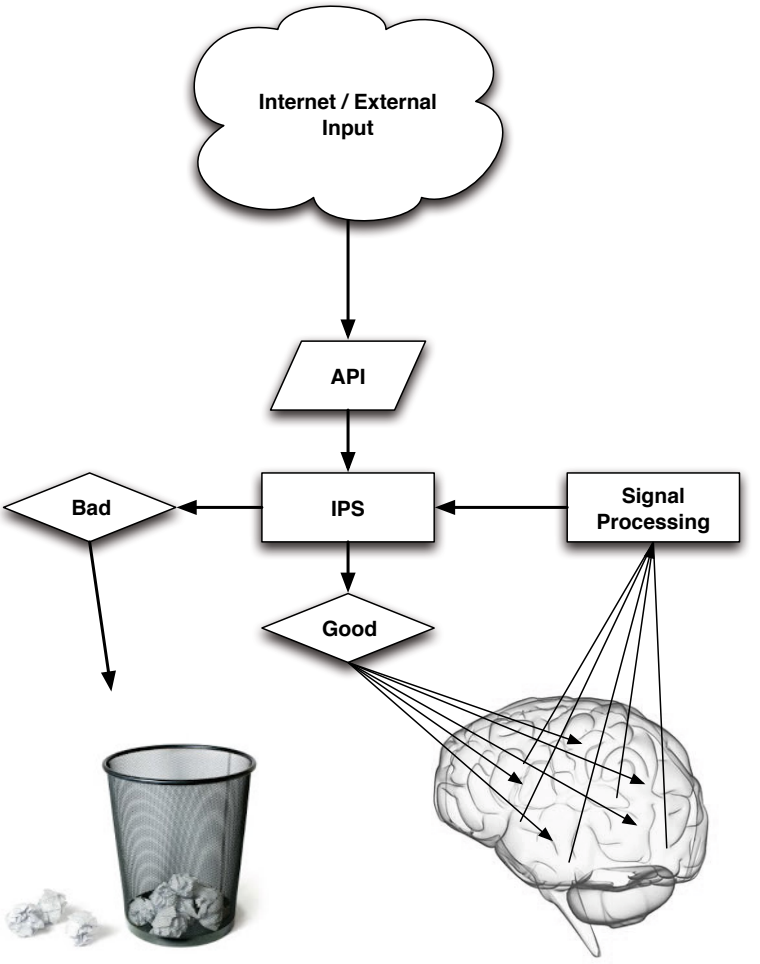

Fig. 1. High level overview of process employed by neurosecurity system providing security analysis on input to a brain-computer interface

4 Conclusion and Future Directions

Employing an artificial neural network security system alongside BCI-enabled technologies will be essential to protecting the user's brain and BCI-enabled devices from malicious activity that affect the state of the brain. As we continue to merge technology and our biology, the need for a secure communication channel becomes a serious concern. Prosthetic limbs, medication dispensers, memory boosters, secondary processing units and even implanted communication devices may soon be used to enhance the user's life, we cannot afford to leave the security of BCI technology as an afterthought. Doing so could result in widespread

negative impacts on humanity. By developing a neurosecurity system before it is required, these vulnerabilities can be mitigated in a manner that protects both the BCI-enabled devices and the users.

References

1. Norton study calculates cost of global cybercrime (September 2011)
2. Allen, B.D.: Targeted read-out, analysis, and control to elucidate dynamic-emotional processing. Massachusetts Institute of Technology (2010)
3. Arenkiel, B.R., Peca, J., Davison, I.G., et al.: In vivo light-induced activation of neural circuitry in transgenic mice expressing channelrhodopsin-2. Neuron 54(2), 205–218 (2007)
4. Denning, T., Matsuoka, Y., Kohno, T.: Neurosecurity: security and privacy for neural devices. Neurosurg Focus 27 (July 2009)
5. Essers, L.: Computer viruses could cross frontier into biological realm. PC World (March 2012)
6. Gerits, A., Farivar, R., Rosen, B.R., et al.: Optogenetically induced behavioral and functional network changes in primates. Current Biology (July 2012)
7. Hazarika, N., Chen, J.Z., Tsoi, A.C., Sergejew, A.: Classification of eeg signals using the wavelet transform. Signal Processing 59(1), 61–72 (1997)
8. Knöpfel, T., Lin, M.Z., Levskaya, A., Tian, L., Lin, J.Y., Boyden, E.S.: Toward the second generation of optogenetic tools. The Journal of Neuroscience 30(45), 14998–15004 (2010)
9. Kokaia, M., Andersson, M., Ledri, M.: An optogenetic approach in epilepsy. Neuropharmacology (January 2012)
10. Lebedev, M.A., Tate, A.J., Hanson, T.L.: Future developments in brain-machine interface research. Clinics 66(1) (2011)
11. Liu, X., Ramirez, S., Pang, P.T., et al.: Optogenetic stimulation of a hippocampal engram activates fear memory recall. Nature 484(7394) (April 2012)
12. Niedermeyer, E., da Silva, F: Electroencephalography: Basic Principles, Clinical Applications, and Related Fields. Lippincot Williams & Wilkins (2004)
13. Peron, S., Svoboda, K.: From cudgel to scalpel: toward precise neural control with optogenetics. Nature Methods 8(1), 30–34 (2010)
14. Postelnicu, C., Talaba, D., Toma, M.: Brain computer interfaces for medical applications. Bulletin of the Transilvania University of Braşov 3(52) (2010)
15. Scarfone, K., Mell, P.: Guide to intrusion detection and prevention systems. Recommendations of the National Institute of Standards and Technology (Febuary 2007)
16. Subasi, A., Ercelebi, E.: Classication of eeg signals using neural network and logistic regression. Computer Methods and Programs in Biomedicine, 87–99 (2005)
17. Zhanga, Z., Kawabatab, H., Liuc, Z.Q.: Electroencephalogram analysis using fast wavelet transform. Computers in Biology and Medicine, 429–440 (2001)