A Position for Proactive Cybersecurity Policies for Military BCIs

Ashley Boykin
Capitol Technology University
Cybersecurity Department
Baltimore, USA
e-mail: abboykin@captechu.edu

Jayfus T. Doswell
Juxtopia® Advanced Mixed Reality (JAMR) Lab
The Juxtopia Group, Inc.
Baltimore, USA
e-mail: jayfus@juxtopia.com

***Abstract* - More countries are considering equipping their soldiers with Brain-Computer Interfaces (BCI). Hence, these governments will require investment in access control policies that specifically target BCI to prevent the technology from becoming vulnerable to internal and external threats. Authors present a position on the importance of International cybersecurity policies to protect data from BCI and humans.**

Keywords – cybersecurity; policy; government; BCI; brain.

I. INTRODUCTION

Access control policies and management refers to the methods in which users are granted or denied access to users or systems. Its foundation is upholding authentication, confidentiality, integrity, reliability, maintainability, availability and non-repudiation to correctly grant and manage access to a needed resource or system [1].

A. BCI Cybersecurity Overview

The international community has expressed interest in using Brain-Computer Interfaces (BCI)s (BCI) in a variety of industry sectors, ranging from medical and commercial space to military industries. Each of these industries has investigated how technological advancements in BCI can improve human performance in completing tasks more efficiently and at lower costs. For example, BCIs allow improved human capabilities to be enhanced by augmenting human skillset and physical capabilities. However, these technical advancements potentially pose a larger attack surface for cybersecurity professionals to consider. The results of a BCI cyberattack can have devastating and adverse consequences to 1.) BCI wearer's health; and 2.) Provide an attacker with access to critical information ranging from an individual's neurological state; active memory and thoughts; to neurological illnesses/diseases [2].

Hence, understanding the creative capabilities of humans to both create and disrupt BCI infrastructures, it is prudent to take proactive processes for creating policies to, not only bolster a BCIs security mechanisms, but also to enhance BCI access control capabilities to prevent critical data from becoming susceptible to well-meaning colleagues without the appropriate authorization to access the information.

B. Non-Invasive BCI

Across the aforementioned industries, BCIs may be engineered with non-invasive and transcutaneous methods ranging from near-infrared spectroscopy (fNIRS) and electro-encephalogram (EEG) to transcranial magnetic stimulator (TMS) devices. The objective of BCIs is to assist human navigation of computer or other electro-mechanical systems or to extract neurological information from the human. Although fNIRS has positive advantages, such as being low-risk and provides high-spatial resolution, its main drawback is that it is not portable whereas EEG is portable. The disadvantage of EEG is that signals are able to be distorted by surrounding interference [3]. EEG and fNIRS are currently the best options for BCI implementation and research for military implementation.

II. BCI AND CYBERSECURITY

A. HSPD-12 Access Control Guidelines

The Homeland Security Presidential Directive 12 (HSPD-12) was established to streamline the process of access control regarding federal employees and contractors for the United States (U.S.) government. This directive forms the foundation for streamlining access control policies for greater interoperability throughout governmental agencies.

Typically, science innovates faster than policies allow. Therefore, it is a necessity that there are guidelines in place delineating strong access control policies for BCI users that are explored prior and alongside military-wide adoption of BCI for highly-skilled soldiers. Protection against bad actors as well as internal threats must be implemented alongside science, so that researchers will understand what and how to protect a person's BCI and the critical data located within their system.

B. Implementing Access Controls

The best course of action for using fNIRS is a unified physical and logical security system. This is because this method analyzes a current system's capabilities and needs as well as its future needs and goals. Therefore, this access control method will evolve with the BCI’s needs. The evolutionary access control will place the foundation for protecting the user and any components required for the BCI to operate successfully within its set of parameters.

C. Military Medicine Access Control

Scientists have also discovered that brainwaves are unique to individuals [4]. Thus, it means that brainwaves can be considered a biometric feature to implement within access control mechanisms for wearers in the future. There have been instances where BCIs have proven beneficial to those suffering from neurological conditions. However, BCI cybersecurity researchers must determine, for other reasons, how to protect the identity of BCI wearers who may suffer from cognitive abilities and comorbidities as well as those who have neurological gifts and unique skill proficiency that make the individual a target.

III. Conclusion and future work

In conclusion, strong cybersecurity access control policies must be implemented in governments, around the world, based on how soldiers and peacekeeping units are currently using BCIs and predictive how these specially skilled and protected individuals will use BCIs for battle, training and peacekeeping missions.

The adverse results from a prolonged cybersecurity attack can have devastating results on the wearer’s neurological system as well as provide an attacker with access to critical information.

The military’s exploration of incorporating BCI comes with a responsibility to ensure the proper access control policies are enabled and enforced alongside the research and development (R&D) phases and prior to implementation. In this way, vulnerabilities can be identified and policies can be created to bolder a user’s BCI efficiency as well as its internal and external security.

Acknowledgement

This research was supported by the Juxtopia® Advanced Mixed Reality (JAMR) program of The Juxtopia Group, Inc.

References

[1] CIO Council, Executive Office of the President of the United States. *Federal Identity, Credential, and Access Management (FICAM). Roadmap and Implementation Guidance.* [Online]. Available from https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FICAM_Roadmap_and_Implem_Guid.pdf. Retrieved March, 2019.

[2] J. Minguez and P. Usieto. “Avoiding brain hacking - Challenges of cybersecurity and privacy in Brain-Computer Interfaces.” Available from https://www.bitbrain.com/blog/cybersecurity-brain-computer-interface. Retrieved March, 2019.

[3] Grey Matters. Brain-Computer Interfaces (BCI)s. [Online]. Available from http://greymattersjournal.com/brain-computer-interfaces/. Retrieved March, 2019.

[4] B. Armstrong, et. al. “Brainprint: Assessing the uniqueness, collectability, and permanence of a novel method for ERP biometrics,” Neurocomputing, vol. 166, pp 59-67, Oct. 2015, doi: 10.1016/j.neucom.2015.04.025.