Brain-Computer Interface Applications: Security and Privacy Challenges

QianQian Li
University of Padua, Italy
qianqian@math.unipd.it

Ding Ding
University of Padua, Italy
ding@math.unipd.it

Mauro Conti
University of Padua, Italy
conti@math.unipd.it

***Abstract*—Brain-Computer Interfaces (BCI) are becoming increasingly popular in medical and non-medical areas. Unfortunately, manufacturers of BCI devices focus on application development, without paying much attention to security and privacy related issues. Indeed, an increasing number of attacks to BCI applications underline the existence of such issues. For example, malicious developers of third-party applications could extract private information of users.**

In this paper, we focus on security and privacy of BCI applications. In particular, we classify BCI applications into four usage scenarios: 1) neuromedical applications, 2) user authentication, 3) gaming and entertainment, and 4) smartphone-based applications. For each usage scenario, we discuss security and privacy issues and possible countermeasures.

***Index Terms*—brain-computer interfaces; BCI applications; neuromedical; gaming; security; privacy; smartphone**

I. Introduction

Brain-computer interfaces (BCI) are interfaces that collect data related to users' brain activities through sensors and transfer this data to computers. In BCI systems, the brain does not use peripheral nerves in order to give orders to our body. Instead, the orders are captured directly by BCI devices and encoded into electro-physiological signals. These signals become commands that can control external devices and computer applications. For example, in order to control a cursor, signals are transmitted directly from the brain to the application that moves the cursor, rather than taking the "route" through peripheral nerves from the brain to the hand to move a mouse. This technology makes it easier for a human to communicate with computers or external devices, such as prosthetic devices (especially for the patients with severe neuromuscular disorders). With the development of intelligentization, BCI technology has been pervasive in several fields of our life, such as, neuromedical field, authentication, gaming, entertainment, and marketing. Unfortunately, BCI manufacturers are developing devices and applications without taking much the security and privacy issues into account. Using such devices, individuals' private information could be stolen by malicious third party applications.

Figure 1 shows the working of brain-computer interfaces. First, the brain neural signals are captured by BCI devices (step 1): this process is named signal acquisition. After signal acquisition, BCI systems transform these analog signals into digital signals (step 2). Then, using signal processing, the features are extracted and classified (step 3 and step 4). Then, the signal output is sent to BCI applications (step 5).

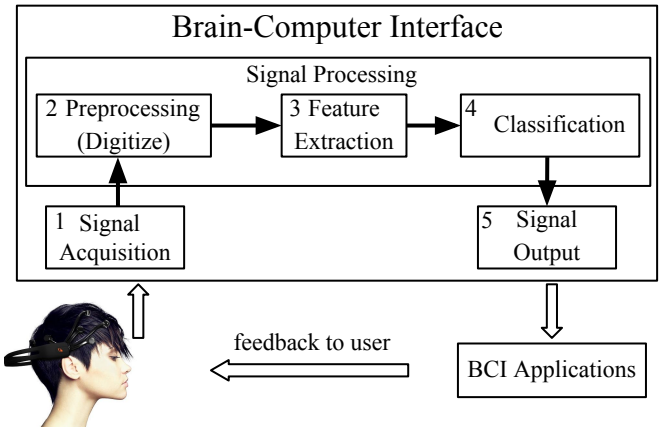


Fig. 1: Working of Brain-Computer Interfaces.

BCI systems could be classified into three main groups: 1) invasive system [1], 2) partial invasive system, and 3) non-invasive system. An invasive system requires physical implants of electrodes into the grey matter of the brain by neurosurgery, which makes it possible to measure local field potentials. A partial invasive system (e.g., electrocorticography - ECoG) is applied to inside of the skull but outside of the grey matter. A non-invasive system (e.g, electroencephalography - EEG, and functional Magnetic Resonance Imaging - fMRI) is the most frequently used neuron signal capturing method. This system is applied to outside of the skull, just applied on the scalp. It records the brain activities inside of the skull, and on the surface of the brain membranes. Both EEG and fMRI give different perspectives and enable us to "look" inside of the brain [2].

Note that, invasive and partial invasive systems are prone to scar tissue, and they are difficult to operate. Furthermore, both of them are quite expensive. Although EEG signals can be effected by noise and signal distortion, they are easily measured and have good temporal resolution. Therefore, the most widely used method for recording brain activity in BCI systems is EEG. EEG-based devices directly measure electrical potentials produced by brain's neural synaptic activities. Five waves from human brain activities that could be captured by EEG devices are as follows: 1) gamma waves are in the frequency range of 31Hz and up, and are associated with arousal and excitement activity of our brain; 2) beta waves are in the frequency range of 12-30Hz, and are related with action and concentration; 3) alpha waves are in the frequency range of 8-12Hz, which reflect

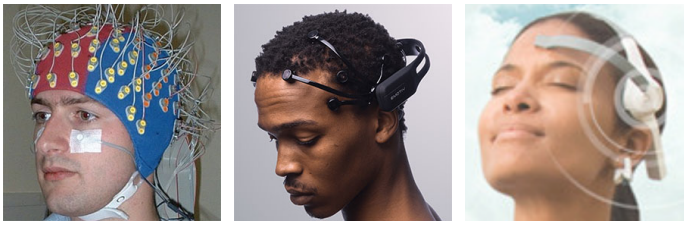
978-1-4673-7876-5/15/$31.00 ©2015 IEEE

relaxation and disengagement; 4) theta waves ranging from 4 to 7Hz, are linked to inefficiency and daydreaming; 5) delta waves ranging from 0.5 to 4Hz, are the slowest waves and occur when a user is in hypnoidization.

Currently several companies produce BCI devices, for different purposes, ranging from clinical-grade BCI devices to consumer-grade BCI devices. Table I lists the main features of three common devices, while Figure 2 shows the appearances of these devices.

TABLE I: Comparision of BCI devices.

Device	Price	Electrodes	Resolution	Interface
BioSemi Active [3]	$12000	256	24 bits	Wired
Emotiv EPOC [4]	$399-499	14	14 bits	Wireless
NeuroSky [5]	$50-150	1	8 bits	Wireless



(a) Biosemi Active (b) Emotiv EPOC (c) NeuroSky

Fig. 2: BCI devices.

Contribution: In this paper, we discuss the main security and privacy challenges of brain-computer interfaces with respect to BCI applications. Because of the importance of private information in our brain (i.e., all of our knowledge, ranging from passwords to our habits), it is vital to prevent them from being leaked to attackers. We list the security and privacy challenges of BCI applications and then discuss their possible countermeasures.

Organization: The rest of this paper is organized as follows. In Section II, we revise the main BCI applications (i.e., neuromedical applications, authentication, gaming and entertainment, and smartphone-based applications), and for each application scenario we discuss the key security and privacy challenges together with possible countermeasures. We conclude this paper in Section III.

II. BCI Security and Privacy Challenges

In this section, we classify BCI applications into four different application scenarios according to their usage purpose (i.e., neuromedical applications, authentication, gaming and entertainment, and smartphone-based applications). For each application scenario, we provide a description, as well as possible attacks (either already doable, or envisaged to be possible in the near future). Finally, for each application scenario we also discuss possible countermeasures.

A. Neuromedical Applications

Since BCI technology makes it easier for a human to communicate with external devices or computers, it is widely used in the neuromedical area to help patients to control their body through BCI devices instead of nerves. BCI technology can help patients, especially with serve neurological disorders, e.g., Parkinson disease. Several neural implantable devices [6] will be available in the near future. Because of being closely related with health, security and privacy concerns become especially necessary to be taken into consideration. An example of neuromedical applications that might be exposed to attacks is prosthetic limb application [7], for which, in what follows, we list possible attacks and countermeasures.

Attacks: As a representative case of neuromedical applications, prosthetic limb application allows physicians to connect wirelessly to adjust settings of neural implant devices. If complete brain neural signals are transmitted, an attack can intercept the transmission, save brain neural signals, and decompose the raw signals to obtain private information. We underline that these attacks are possible even when information is transmitted in an encrypted format [8]. Furthermore, attacker could try to control prosthetic limbs of patients and give dangerous movement to patients. Under this condition, an attacker does not need to be physically in the proximity of the victim. Instead, the attacker only needs to have attack hardware placed near the patient. Another possible scenario is the case in which patients are attackers who might modify settings on their own prosthetic limbs. They might just want to override mechanical safety settings to gain extra strength or interfere with limb feedback to eliminate the ability of feeling pain.

Countermeasures: There are some appropriate safeguards in the design of the neuromedical applications which can be deployed in the coming years. For these neuromedical applications used to give treatment for patients, it is clear that the main countermeasures should focus on preventing life-threatening attacks. Also, we should protect private feelings and emotions of patients from being leaked to attackers. In addition, these applications should prevent attackers from remotely eavesdropping on the wireless signals and collecting private information about patients' activities. The communication between neural implantable devices and patients must be kept confidential. Furthermore, if they are in sensitive condition such as depression, trying to prevent wireless attackers from detecting the presence of these implant devices is effective to protect safety. In the future, more effective countermeasures should be proposed to guarantee that neuromedical applications are not only safe and effective, but also these applications are robust enough to prevent attacks.

B. User Authentication

Authentication is a process that ensures and confirms a user's identity. It plays an important role in security systems. Using EEG brain signals as authentication measure has been proposed in many literatures and proved to be effective. Authors in [9] aim at authenticating users, based on brainwave signals. In particular, they use single-channel EEG signals to do authentication. In this authentication system, BCI devices record brainwave signals when a subject performs a custom task (e.g., singing, breathing or finger movement). Then, brain signals are wirelessly transmitted to a computer application which collect and process this data. Their authentication system analyses the similarity between such brain data and training data to authenticate subjects. The authors show that their

proposed authentication mechanism has the same accuracy as multi-channel EEG authentication, about 99% accuracy. Similar to [9], authors in [10] take EEG brainwave features as neural passwords to do authentication. The entire process is performed automatically, without human supervision. The authors use an algorithm that automatically extracts neural events corresponding to an individual's blinking, jaw-clenching, and eye-rolling activities. The results show that accuracy of this authentication method ranges from 67% to 95% with single-trial inputs.

Attacks: Using EEG brainwaves to authenticate might result in risks for the privacy of users. For example, authors in [11] propose an authentication system that verifies an individual EEG signal when a subject performs a custom task (e.g., singing, breathing or finger movement). They also design an attack model by impersonating the thoughts of subjects. The authors make deliberate attacks from thought impersonators to test the robustness of the authentication system. Similar to [12], an adversary can attack the authentication system via synthetic EEG signals, using EEG generative model based on the historical EEG data from a subject can also attack the authentication system [13].

Countermeasures: To mitigate the authentication attacks mentioned about, a possible way is to reduce authentication error rate. For example, we can enlarge the number of participants, use recruited attackers, and integrate the data processing methodology with a real-time authentication framework to achieve reduced authentication error rate. Moreover, another possible method to enhance the robustness of authentication is by leveraging multidimensional method [14]. For example, using multiple authentication signals (e.g., the signals of singing, breathing, or being shocked). Besides, we can combine the existing authentication methods on smartphone device to perform multidimensional authentication.

C. Gaming and Entertainment

With the development of BCI technology, there are several BCI games available in entertainment industry [15] [16] [17]. The principle of most BCI games works in a way similar to P300-speller. In this kind of games, an amplitude peak in the EEG signal is detected at more or less 300ms after a stimulus. In the game P300-speller, stimuli are alphanumeric characters shown on the screen. The characters are arranged in a matrix where rows and columns flash on a screen in a rapid succession. According to the being spelled word, users choose one character using eyes from the screen. Through analyzing peaks occurring in the brainwaves, authors get the spelled word. Another game named Snake [18] is also based on the same principle of P300-speller. In this game, a snake can move in three directions: forward, left and right. The goal is to locate and eat apples on a map. Eating apples makes the snake grow in length, and becomes as large as possible. For the sake of having speed in the game, moving forward is automatic, and both turning left or right is controlled by the user via EEG signals.

Attacks: Brain-computer interfaces are becoming increasingly popular in the gaming and entertainment industries. Martinovic et al. [19] highlight the existence of side-channel attacks by malicious third-party games on BCI devices. Similar to smartphone games, third-party BCI games depend on common APIs to access BCI devices. Thus, such APIs supply unrestricted access to raw EEG signals for BCI games. Furthermore, such games have complete control over the stimuli that can be presented to users. As a consequence, attackers can display the contents and read their corresponding EEG signals. The content might be videos, pictures, or numbers, which users see when they playing games. Therefore, attackers can specifically design some videos and images shown to users in order to maximize the amount of leaked information. In particular, the impact of exploiting or mishandling BCI devices is difficult to estimate. Authors in [19] demonstrate BCI games could be exploited to extract individuals' private information, such as 4-digit PINs, bank information, date of birth and location of residence, using users' recorded EEG signals.

Countermeasures: Authors in [20] identify security and privacy issues arising from possible misuse or inappropriate use of "Brain Malware" information. In particular, they propose an interdisciplinary approach to enhance the security of BCI systems by the aid of several experts from different areas, such as neuroscientists, neural engineers, ethicists, as well as legal, security and privacy experts.

Authors in [21] propose a tool named "BCI Anonymizer" to prevent the side-channel extraction of users' private information. The basic idea of the "BCI Anonymizer" is to remove private information from raw EEG signals before this information is stored and transmitted. "BCI Anonymizer" could be implemented either in hardware or in software, as a part of BCI devices, but not as part of any external network or computational platform. Moreover, the "BCI Anonymizer" can generate an anonymized neural signals to replace the removed signals that represent private information. However, authors in [21] do not provide a clear method to distinguish the difference between users' private information and commands to applications.

D. Smartphone-based Applications

The application scenario we want to consider in this section is actually mainly driven by a specific emerging and pervasive technology, i.e., smartphones. Along with the advances in smartphone capabilities, there is an increasing interest in using smartphone by individuals in their daily life. BCI are used in conjunction with this technology (smartphone). Recently, some BCI applications based on smartphone have been proposed in many literatures.

Authors in [22] implement a brain-controlled address book dialing app, which works in a way similar to P300-speller. Instead of showing characters in P300-speller, the dialing app shows a sequence of photos of contacts from the address book. Therefore, the user can easily select a person whom she or he wishes to dial. Authors in [23] measure a subject's attention and meditation level through EEG signals when a subject is playing a game. Authors compare the difference among all the subjects' EEG signals, according to subjects' age and gender. Their results show that, in the POKOPANG game, the average attention level of men is lower than that of women, while the meditation level is reversed. As a result, authors infer that women are more interested in POKOPANG game.

Air Brain system [24] is a portable EEG telemetry system. Different from other portable EEG monitoring systems, in order to have more storage space, this way, the stored data can be accessed from everywhere. To achieve this, the system uses 3G network of smartphone to transfer data. Air Brain system enables subjects to measure EEG signals immediately after subjects start walking. Furthermore, the system is able to detect eye closing by measuring changes of aplha wave.

Attacks: The smartphone-based BCI applications are prone to attacks that originate in the mobile device itself. Therefore, most of the possible attacks on smartphone issues could also be considered as security and privacy issues of smartphone-based BCI applications. These applications can access private data which is acquired from BCI devices and stored in smartphones or SD card. This data can be illegally transferred by a malware to a remote server (e.g., privilege escalation attacks [25]). Developers of malwares can analyse the private signals and attack the users of BCI devices. Attacks to smartphone applications also apply to smartphone-based BCI applications.

Countermeasure: Given that we are considering BCI applications in conjunction with a specific technology (smartphone), here countermeasures are mostly the ones typical for generic smartphone security. Useful security approaches could be the ones that track the flow of information. For example, TaintDroid [26] proposes a model that can track not only the way applications access sensitive data, but also the way applications use such data. FlowDroid [27] proposes an innovative and accurate static taint analysis for applications in Android platform, allowing proper analysis to handle callbacks invoked by the Android framework. In addition to the aforementioned approaches, fine-grained context-based access control [28] is another effective way to limit the leakage of private data. These mitigations are possible only by modifying Android's permission model, e.g., Android's internal middleware layer.

III. Conclusion

In this paper, we survey some common brain-computer interfaces (BCI) applications, and their possible security and privacy issues. Moreover, we consider four different application scenarios: 1) neuromedical applications, 2) user authentication, 3) gaming and entertainment, and 4) smartphone-based applications. For each scenario we provide the description of current state-of-the-art technologies, potential attacks that might threat each scenario, and envisaged countermeasures.

ACKNOWLEDGMENTS

Mauro Conti is supported by a European Marie Curie Fellowship (N. PCIG11-GA-2012-321980). This work is also partially supported by the Italian MIUR PRIN Project TENACE (N. 20103P34XC), and the University of Padua PRAT 2014 Project on Mobile Malware.

References

[1] J. R. Wolpaw, N. Birbaumer, W. J. Heetderks *et al.*, "Brain-computer interface technology: a review of the first international meeting," *IEEE transactions on rehabilitation engineering*, vol. 8, no. 2, pp. 164–173, 2000.
[2] J. Kropotov, *Quantitative EEG, event-related potentials and neurotherapy*. Academic Press, 2010.
[3] (2015, July) Biosemi. [Online]. Available: http://www.biosemi.com
[4] (2015, July) Emotiv epoc. [Online]. Available: https://emotiv.com
[5] (2015, July) Neurosky. [Online]. Available: http://neurosky.com
[6] T. Denning, Y. Matsuoka, and T. Kohno, "Neurosecurity: security and privacy for neural devices," *Neurosurgical Focus*, vol. 27, no. 1, p. E7, 2009.
[7] A. B. Schwartz, X. T. Cui, D. Weber, and D. W. Moran, "Brain-controlled interfaces: Movement restoration with neural prosthetics," *Neuron*, vol. 52, no. 1, pp. 205 – 220, 2006.
[8] M. Conti, L. V. Mancini, R. Spolaor, and N. V. Verde, "Can't you hear me knocking: Identification of user actions on android apps via traffic analysis," in *DASP*, 2015, pp. 297–304.
[9] J. Chuang, H. Nguyen, C. Wang, and B. Johnson, "I think, therefore i am: Usability and security of authentication using brainwaves," in *Financial Cryptography and Data Security*, 2013, pp. 1–16.
[10] A. Rajagopal, A. C. Nguyen, and D. M. Briggs, "Neuropass: A secure neural password based on EEG," in *Biomedical Engineering*, 2013.
[11] B. Johnson, T. Maillart, and J. Chuang, "My thoughts are not your thoughts," in *Proceedings of the 2014 ACM UbiComp: Adjunct Publication*, 2014, pp. 1329–1338.
[12] P. E. McSharry, G. D. Clifford, L. Tarassenko *et al.*, "A dynamical model for generating synthetic electrocardiogram signals," *Biomedical Engineering*, vol. 50, no. 3, pp. 289–294, 2003.
[13] S. T. Archer and B. D. Pless, "Stimulation signal generator for an implantable device," Feb. 10 2004, uS Patent 6,690,974.
[14] T. Naik and S. Koul, "Multi-dimensional and multi-level authentication techniques," *International Journal of Computer Applications*, vol. 75, no. 12, pp. 17–22, 2013.
[15] C. Mühl, H. Gürkök, D. Plass-Oude Bos, M. E. Thurlings *et al.*, "Bacteria hunt: A multimodal, multiparadigm bci game," *University of Genua*, 2010.
[16] M. Congedo, M. Goyat, N. Tarrin, and G. e. a. Ionescu, "Brain invaders: a prototype of an open-source p300-based video game working with the openvibe platform," in *5th International BCI*, 2011, pp. 280–283.
[17] A. Finke, A. Lenhardt, and H. Ritter, "The mindgame: a p300-based brain–computer interface game," *Neural Networks*, vol. 22, no. 9, pp. 1329–1333, 2009.
[18] E. A. Larsen, "Classification of eeg signals in a brain-computer interface system." Norwegian University, 2011.
[19] I. Martinovic, D. Davies, M. Frank, D. Perito, T. Ros, and D. Song, "On the feasibility of side-channel attacks with brain-computer interfaces," in *USENIX Security 12*, 2012, pp. 143–158.
[20] T. Bonaci, R. Calo, and H. J. Chizeck, "App stores for the brain: Privacy & security in brain-computer interfaces," in *Science, Technology and Engineering, 2014 IEEE International Symposium*, 2014, pp. 1–7.
[21] H. Chizeck and T. Bonaci, "Brain-computer interface anonymizer," Aug. 14 2014, US Patent App. 14/174,818. [Online]. Available: http://www.google.com/patents/US20140228701
[22] A. Campbell, T. Choudhury, S. Hu, H. Lu *et al.*, "Neurophone: brain-mobile phone interface using a wireless eeg headset," in *Proceedings of the second ACM SIGCOMM workshop*, 2010, pp. 3–8.
[23] J.-Y. Kim and W.-H. Lee, "Eeg signal feature analysis of smartphone game user," *ASTL*, vol. 39, pp. 14–19, 2013.
[24] K. Honda and S. N. Kudoh, "Air brain: the easy telemetric system with smartphone for eeg signal and human behavior," in *Proceedings of the 8th BodyNets*, 2013, pp. 343–346.
[25] L. Davi, A. Dmitrienko, A.-R. Sadeghi, and M. Winandy, "Privilege escalation attacks on Android," pp. 346–360, 2011.
[26] W. Enck, P. Gilbert, S. Han, and V. e. a. Tendulkar, "Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones," *ACM TOCS*, vol. 32, no. 2, p. 5, 2014.
[27] S. Arzt, S. Rasthofer, C. Fritz, E. Bodden, and et al., "Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps," in *ACM SIGPLAN Notices*, 2014, pp. 259–269.
[28] M. Conti, B. Crispo, E. Fernandes, and Y. Zhauniarovich, "Crêpe: A system for enforcing fine-grained context-related policies on android," *Information Forensics and Security*, vol. 7, no. 5, pp. 1426–1438, 2012.