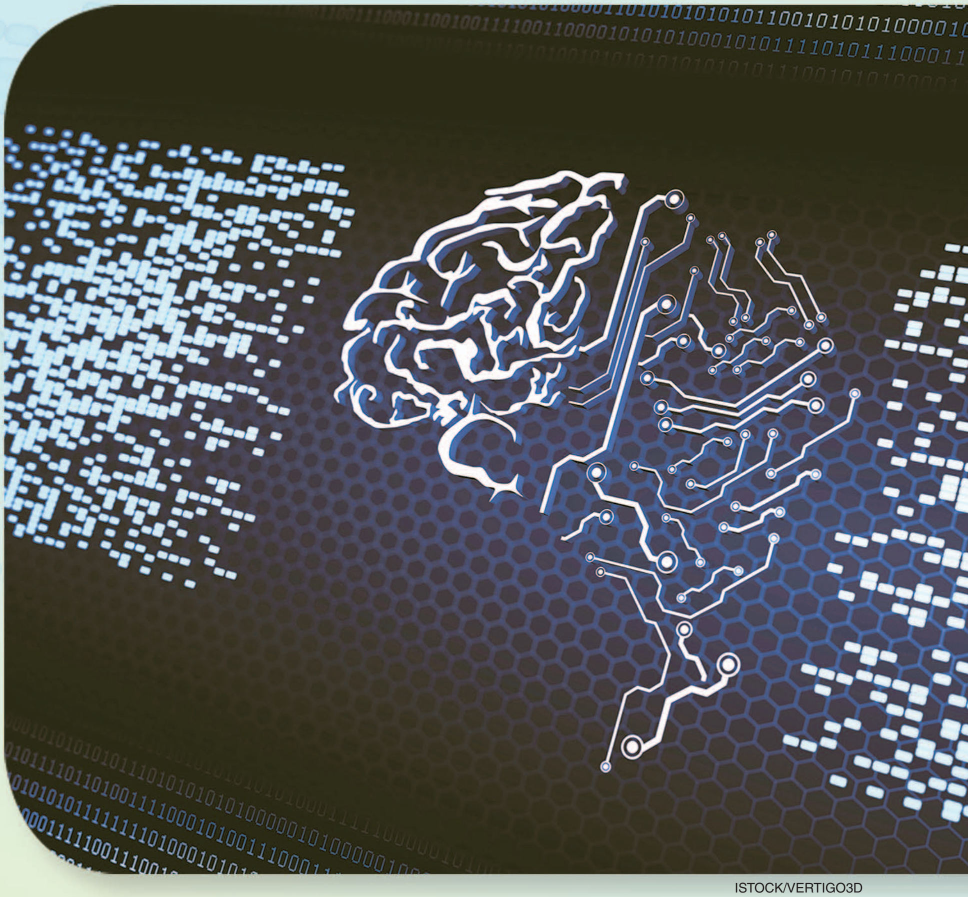
App Stores for the Brain

Privacy and Security in Brain-Computer Interfaces

Tamara Bonaci,
Ryan Calo, and
Howard Jay Chizeck



ISTOCK/VERTIGO3D

A large number of Brain-Computer Interfaces (BCIs) are currently under development, or being proposed, for both medical and non-medical applications. These applications include advertising, market surveys, focus groups and gaming. For example, in 2008, the Nielsen Company acquired Neurofocus, for the development of neural engineering technologies aimed at better understanding customer needs and preferences [1]. In May 2013, Samsung, in collaboration with the University of Texas, demonstrated how BCIs could be used to control mobile devices [2]. In the same month, the first neurogaming conference gathered more than 50 involved companies [3]. In September 2013, Neuroware presented Neurocam, a wearable EEG system equipped with a camera. The system is set to automatically start recording moments of interest based on inferred information from users' neural signals [4].

Several neural engineering companies, including Emotiv [5] and NeuroSky [6] currently offer low-cost, consumer- grade BCIs and software development kits. These companies have recently introduced the concept of BCI "app stores" [7], with the purpose of facilitating expansion of BCI applications. Future BCIs will likely be simpler

Digital Object Identifier 10.1109/MTS.2015.2425551
Date of publication: 19 June 2015

to use and will require less time and user effort, while enabling faster and more accurate translation of users' intended messages.

These developments raise questions about privacy and security. At the 2012 USENIX Security Symposium, researchers introduced the first BCI enabled malicious application, referred to as "brain spyware." The application was used to extract private information, such as credit card PINs, dates of birth, and locations of residence, from users' recorded EEG signals [7].

As BCI technology spreads further (towards becoming ubiquitous), it is easy to imagine more sophisticated "spying" applications being developed for nefarious purposes. Leveraging recent neuroscience results (e.g., [8]-[11]), it may be possible to extract private information about users' memories, prejudices, religious and political beliefs, as well as about their possible neurophysiological disorders. The extracted information could be used to manipulate or coerce users, or otherwise harm them. The impact of "brain malware" could be severe, in terms of privacy and other important values. A question arises: is it in the public interest to allow anyone to have unrestricted access to the private information extractable from neural signals? And if not, how should we grant such access, and how can this be managed, regulated, or otherwise controlled?

While U.S. federal law protects medical information [12] and generally guards against unfair or deceptive practices [13], few rules or standards currently limit access to BCI-generated data. Importantly, platforms are immunized for apps that third parties submit, such that BCI-manufacturers are not necessarily incentivized, from a legal vantage, to police against abusive apps.

We believe emerging BCI privacy concerns call for a coordinated response by engineers and neuroscientists, lawyers and ethicists, government and industry. Ideally, *devices, algorithms, standards and regulations* can be designed to mitigate BCI privacy problems and ethical challenges. The first step towards doing so should be an open discussion between ethicists, legal experts, neuroscientists, and engineers.

Overview of BCI Technologies

A Brain-Computer Interface (BCI) is a communication system between the brain and the external environment. In this system, messages between an individual and an external world do not pass through the brain's normal pathways of peripheral nerves and muscles. Instead, messages are typically encoded in electrophysiological signals, such as electroencephalograms (EEG), signals directly measuring electrical potentials produced by neural synaptic activities [14]–[16].

The initial motivation for the development of BCIs came from the growing recognition of the needs of people with disabilities, and of potential benefits BCIs might offer. The first BCI was developed in the 1970s [15]. Since then, many research programs have focused on the development of BCIs, for assistance, augmentation and repair of cognitive and sensorimotor capabilities of people with severe neuromuscular disorders, such as spinal cord injuries or amyotrophic lateral sclerosis.

In recent years, however, BCIs have seen a surge in popularity in fiction, gaming, entertainment, and marketing. There are currently several consumer-grade BCI-based systems (e.g., Emotive System [5], NeuroSky [6], and g-tec Medical Engineering [17]) offering relatively low-cost EEG-based BCIs and software development kits to support and facilitate expansion of BCI-enabled applications. The supported applications can broadly be classified into: a) *accessibility tools*, such as mind-controlled mouse and keyboard, b) *hands-free arcade games*, such as Brain Bats, mind-controlled Pong game [18], and c) *"serious games,"* i.e., games with purpose other than pure entertainment, such as attention and memory training [19].

BCIs are also emerging as a tool for personalized entertainment. It has been known for some time that the ability to make inferences about a user's cognitive processes and emotional responses, such as satisfaction, boredom, or confusion, enables the development of more adaptive and responsive entertainment products. There already exist several gaming consoles that use pressure, motion, or gaze sensors to make inferences about a user's behavioral states [7]. Very recently researchers from Taiwan have proposed a method of predicting success of an online game by analyzing a user's electromyographic (EMG) signals (i.e., electrical signals produced by a user's skeletal muscles) over the first 45 minutes of the game [9].

In addition to the gaming and entertainment industries, in recent years market research companies have also shown an increased interest in BCI-enabled technologies. In 2008, for example, the Nielsen company has introduced the Mynd, an EEG-based BCI device specifically developed for market research [7]. It is reasonable to expect more and more information about users' cognitive and behavioral processes, as well as their emotional states will be extracted (with and without permission) for a variety of entertainment and marketing studies, as BCI-enabled applications become more widespread.

Components of a BCI

A BCI is a system used to translate electrophysiological signals, reflecting activity of an individual's central nervous system, into a user's intended messages that act on the external world [15]. From an engineering perspective, it is a *communication system*, consisting of inputs (user's neural activity), outputs (external world commands), and components translating inputs to outputs, known as *signal acquisition* and *signal processing*. A high-level block diagram of a typical BCI is depicted in Fig. 1.

Based on the recording location, BCIs can be divided into: a) invasive, b) moderately invasive, and c) non-invasive systems. Invasive BCIs involve electrodes or electrode arrays that are directly implanted into the brain during a surgery. Inside-the-brain implanted BCIs enable the highest quality measurements of neural activity.

Moderately invasive BCIs, such as electrocorticography (ECoG) are implanted inside the skull, typically on top of the brain. They provide signals of lower noise and higher selectivity than non-invasive BCIs, which record neural signals from the scalp.

Most non-invasive BCIs are based on electroencephalography (EEG). While known to be susceptible to noise and signal distortion, EEG signals are easily measurable. In addition, EEG-based BCIs have relatively low cost and low risk, which makes them the most widely used BCI devices [14].

The signal processing component of a BCI typically consists of two parts: *feature extraction* and *decoding (translation) algorithms*. The feature extraction part processes recorded neural signals, in order to extract signal features. These are assumed to reflect specific aspects of a user's current neural signal. Decoding algorithms take those abstracted feature vectors and transform them into application-specific commands.

Depending on the application, many different decoding algorithms are being used in BCIs. As pointed out in [15], effective decoding algorithms are able to adapt to: 1) individual user's signal features, 2) spontaneous variations in recorded signal quality, and 3) adaptive capacities of the brain (neural plasticity).

Ethical and Legal Considerations of Neural Engineering

With an increasing number of neural engineering applications, specifically BCIs and neural imaging, researchers have recognized the need to address emerging ethical and legal questions [20]-[27]. In 2003, Jonsen introduced *neuroethics* as "a discipline that aligns the exploration and discovery of neurobiological knowledge with human value system." It was recognized that neuroethics will have to address questions related to a) incidental findings, b) surrogate and biomarkers of diseases, and c) commercialization of cognitive neuroscience [23].

In 2005, The Committee on Science and Law considered possible legal implications of neural engineering [25]. An emphasis was put on privacy implications of neural imaging, in particular on the use of neural imaging in non-medical research. The committee recognized *neuromarketing*, defined as the field of marketing research that studies consumers' sensorimotor, cognitive, and affective response to marketing stimuli [26] and *brain fingerprinting*, defined as a technique that purports to determine the truth by detecting information stored in the brain [27], as emerging non-medical areas using neural imaging data.

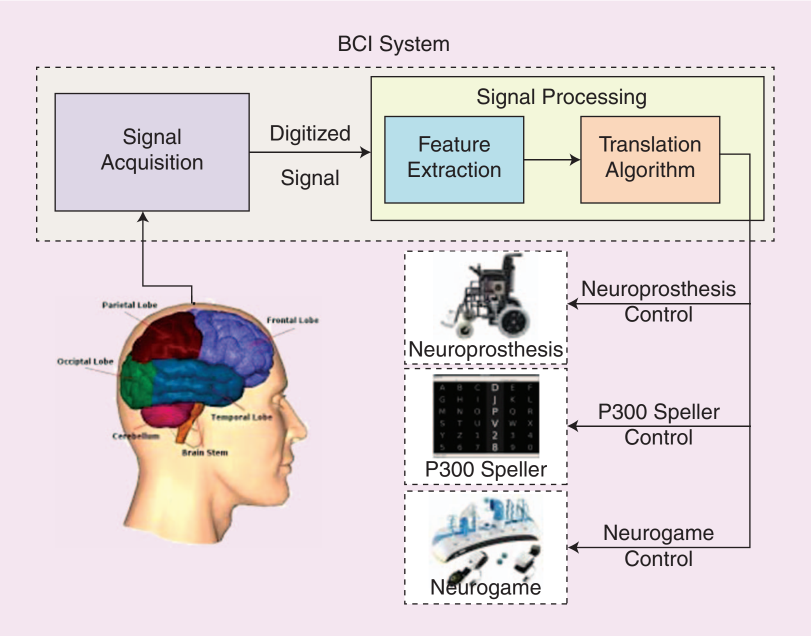


FIGURE 1. High-level block diagram of a typical brain-computer interface.

The committee observed there are important similarities between genetic and brain data, in that: 1) "both genetic and brain data hold out the promise of prediction (not only disease, but also behavior)," and 2) "both types of information expose unique and personal, and to a large extent, uncontrollable aspects of a person that previously were unobservable" [25]. Based on these observations, the committee proposed exploring and leveraging for neuroethics those medical, ethical, and legal rules already set forth in genetic research.

In [21], Farahany observed that modern neuroscience and neural engineering pose an novel set of legal challenges to the existing U.S. Self-Incrimination doctrine of the Fifth Amendment, which states that "no person shall be compelled to prove a charge from his own mouth, but a person may be compelled to provide real or physical evidence" [21]. The author presented several examples, showing how modern neuroscience is expected to facilitate evidence collection during criminal investigation. The presented examples strongly indicate the traditional boundary between testimonial and physical evidence becomes blurry when applied to evidence collected by neural engineering techniques.

Finally, at the 2011 Ethicomp conference, Whalstrom *et al*. introduced the question of BCI privacy. The authors reviewed the European Union's privacy directives and analyzed how the directive's legal context and requirements apply to emerging BCI privacy issues [27].

Privacy and Security Issues in Neural Engineering

Neural Signals for Identification and Authentication

Based on the observation that neural signals of each individual are unique and can therefore be used for biometrics [28], many researchers have recognized potential benefits of using neural data for user identification and authentication [28]–[31], respectively defined as the identity selection out of a set of identities (identification) and verification that the claimed identity is valid (authentication). EEG signals have shown to be particularly useful for these applications.

In [31], a method using an α-rhythm was proposed for identification, and correct classification scores in the range of 72% to 84% were reported. Further, an EEG-based identification method that uses data collected only from the two frontal electrodes was proposed in [32]. In [33], the authors present an overview of biometric identification methods based on EEG, electrocardiogram (ECG), and on skin conductance signals, also known as electrodermal response (EDR).

In [28], the practicability of different mental tasks for authentication was investigated, and it was shown that some tasks are more appropriate for authentication than others. Finally, [34] proposed neural data can be used to prevent coercion attacks (also known as rubber hose cryptanalysis), where users are forced to reveal cryptographic secrets known to them. The proposed approach is based on the idea of *implicit learning*. Instead of asking users to consciously memorize a secret and use it for identification and authentication, in this approach the users are identified and authenticated based on specific patterns that they have learned and can use without ever being aware they know them.

Neurosecurity

In 2009, Denning *et al*. [35] recognized that "the use of standard engineering practices, medical trials, and neuroethical evaluations during the design process can create systems that are safe and that follow ethical guidelines; unfortunately, none of these disciplines currently ensure that neural devices are robust against adversarial entities trying to exploit these devices to alter, block, or eavesdrop on neural signals." Potential security threats that can be mounted against implanted neural devices were identified, and the term "neurosecurity" was introduced as "the protection of the confidentiality, integrity, and availability of neural devices from malicious parties with the goal of preserving the safety of a person's neural mechanisms, neural computation, and free will" [35].

Brain Spyware - BCI-Enabled Malicious Application

At the 2012 USENIX Security Symposium, Martinovic *et al*. [7] presented the first malicious software designed to detect a user's private information using a BCI. They referred to is as the "brain spyware." The authors used a commercially available BCI to present users with visual stimuli and record their EEG neural signals. They focused on the P300 response, and analyzed the recorded signals in order to detect users': a) 4-digit PINs, b) bank information, c) months of birth, d) locations of residence, and e) if they recognized the presented set of faces.

While the authors of [7] have focused only on the P300 response, it is not hard to imagine brain spyware applications being developed to extract private information about users' memories, prejudices, and beliefs, but also about their possible neurophysiological disorders. Currently, there does not seem to exist a way to resist these attacks. Moreover, recent results [36] show that attempts at willful deception can themselves be detected from an individual's neural signals. Going a step further, the same authors [36] show that non-invasive brain stimulators, emitting imperceptible DC electrical currents, can be used to make a user's responses noticeably slower when attempting to lie.

Thus, there is a growing need to address the potential privacy and security risks arising from the use of BCIs, in both medical and non-medical applications. As a first step, we are exploring which components of the EEG signal can be used to infer private information about a user, and quantifying the amount of exposed information.

Threat Model

Consider an example model of an attacker who uses BCIs to extract private information about users. We assume this will involve non-invasive BCI devices, mostly intended for consumer use. Manufacturers of non-invasive EEG-based BCIs generally distribute software development kits and guides with their products, as well as technical support. Their intention is to promote application development, but such "open- development" platforms may compromise user privacy and security, since there is currently no review process, standards, or guidelines in place to protect users: nor is there technical protection to restrict inappropriate or malicious BCI use.

As depicted in Fig. 1, a typical BCI system consists of three main components: an *acquisition system*, an *application*, and a *signal processing system*, where the signal processing system consists of *feature extraction* and *decoding (translation) algorithm* components. The existing BCI open-development platforms typically grant every application developer full control over all of these components. For the purposes of discussion here, we will assume an attacker has an access to all of these resources. We next consider how an attacker uses these resources to develop malicious applications.

Types of Attackers

In Fig. 2, two types of attackers are shown (as described in the caption). We distinguish between these types based on the way an attacker analyzes recorded neural signals. The first type of attacker extracts users' private information by *hijacking the legitimate components of a BCI system*. Such an attacker exploits for malicious purposes those feature extraction and decoding algorithms that are intended for the legitimate BCI applications.

The second type of attacker extracts users' private information by *adding or replacing the legitimate BCI components*. Such an attacker implements additional feature extraction and decoding algorithms, and either replaces or supplements the existing BCI components with additional malicious code. As can be observed from Fig. 2, the difference between the two attacker types is only in the structure of the "brain malware" component.

Methods of Extracting Private Information

We consider scenarios where an attacker interacts with users by *presenting them with specific sets of stimuli*, and recording their responses to the presented stimuli. In the current literature, there are several well-established methods of presenting stimuli to users:

- Oddball paradigm – a technique where users are asked to react to specific stimuli, referred to as *target stimuli*, hidden as rare occurrences in a sequence of more common, *non-target stimuli* [37].
- Guilty knowledge test – a technique based on the hypothesis that a familiar stimulus evokes a different response when viewed in the context of similar, but unfamiliar items [38].
- Priming – a technique that uses an implicit memory effect where one stimulus may have an influence on a person's response to a later stimulus [39].

We assume an attacker can use any of these methods to facilitate extraction of private information. In addition, an attacker can present malicious stimuli in an *overt (conscious)* fashion, as well as in a *subliminal (unconscious)* way, with subliminal stimulation defined as the process of affecting people by visual or audio stimuli of which they are completely unaware [40]. Ways of achieve unawareness typically include reducing a *stimulus intensity* or *duration* below the required level of conscious awareness.

Examples of "Brain Malware" Information Misuse

Private information about BCIs users, extracted using "brain malware," may be of interest to multiple parties, those using it for greater good and potential improvement of the quality of human lives, but also to those using it to increase their own (financial) gains, as well as those using it simply to harm others. One can easily imagine the following examples of concerning BCIs use:

Example 1: As exemplified in Farahaney's work [21], an access to an individual's memories and emotional responses might be used by police enforcement and government agencies during criminal investigation, as well as for crime and terrorism prevention.

Example 2: BCI-recorded neural signals may be used in a variety of entertainment and relaxation applications. A person's emotional response and satisfaction/annoyment level may, for example, be used to provide better (more accurate) music and/or movie recommendations. Similarly, information about a person's activity and anxiety levels may be used to tailor a more personalized training routine or a relaxation session.

Example 3: Personal information, extracted from neural signals, could also be used for targeted advertisement, where in addition to (or instead of) information about a person's activities on the Internet, an advertiser/retailer would have a real-time access to a person's level of interest, satisfaction, or frustration with the presented material.

Example 4: On the other end of the spectrum, however, extracted information about a person's memories, prejudices, beliefs, or possible disorders could be used to manipulate a person or coerce her/him into doing something.

Example 5: Finally, extracted neural information could also be used to cause physical or emotional harm to a person. Examples of such actions have already been observed in the literature. Denning *et al.* [35], presented the case of individuals who placed flashing animations on epilepsy support webpages, eliciting seizures in some patients with photosensitive epilepsy.

Need for a Coordinated Prevention Approach

Issues arising from inappropriate use of BCI technology most likely do not pose a critical concern yet, considering their limited use outside of research communities. However, existing and emerging privacy and security threats may be viewed as an attack on human rights to privacy and dignity [41]. Thus, they deserve immediate attention and careful consideration.

We suggest that methods to prevent and mitigate BCI-enabled privacy and security threats must be developed now, in the early design phase. Doing so will allow us to keep up with Privacy-by-Design [42] values, as well as with general values of privacy-enhancing technologies.

We view the development of prevention and mitigation tools as an interdisciplinary effort, involving neuroscientists, neural engineers, ethicists, as well as legal, security, and privacy experts. Isolated, individual expertise in each of these areas is unlikely to result in an effective approach to security; a more comprehensive understanding is required, and multiple disciplines can help deliver that understanding.

The first step of an interdisciplinary approach should be an open discussion, aimed at answering the following questions: a) Who should be allowed access to an individuals' neural signals? b) Which components of these neural signals should those entities have an access to? c) How noisy, distorted or distilled should these components be made before making them available? d) Which purposes are the entities allowed to use the neural signals for? and e) What are the risks associated with the misuse of the provided components, i.e., what amount of private information can be extracted from the provided components?

We propose a *"triangle" approach* towards enhancing privacy and security of BCI technology. This model is meant to emphasize three aspects of security that should be interrelated: prescriptive, theoretical, and developer aspects.

On one vertex of the triangle, the prescriptive vertex, we place legal experts and ethicists, defining a set of laws and policies to govern legitimate use of neural signals. As an example of possible legal intervention, the law could examine whether BCI platforms should indeed be immunized for the apps they sell, or is some other balance between manufacturers and application developers more appropriate for BCI technologies.

On the second vertex, the theoretical vertex, we place a group of neuroscientists and engineers, in charge of developing and establishing a set of industry and research standards, methods, processes, and practices for secure and privacy-preserving BCI systems. One such practice may, for example, require there to exist a centralized authority in charge of reviewing and validating every BCI application before allowing its use in general population.

Finally, at the third vertex, the developer vertex, we place BCI systems manufacturers and application developers. These parties are developing, implementing, and using engineering practice, methods, and tools, in order to prevent and mitigate specific classes of security and privacy attacks.

BCI Anonymizer

One engineering approach to enhancing neural privacy and security is the use of the BCI Anonymizer described in a patent application by two of the authors of this article [43].

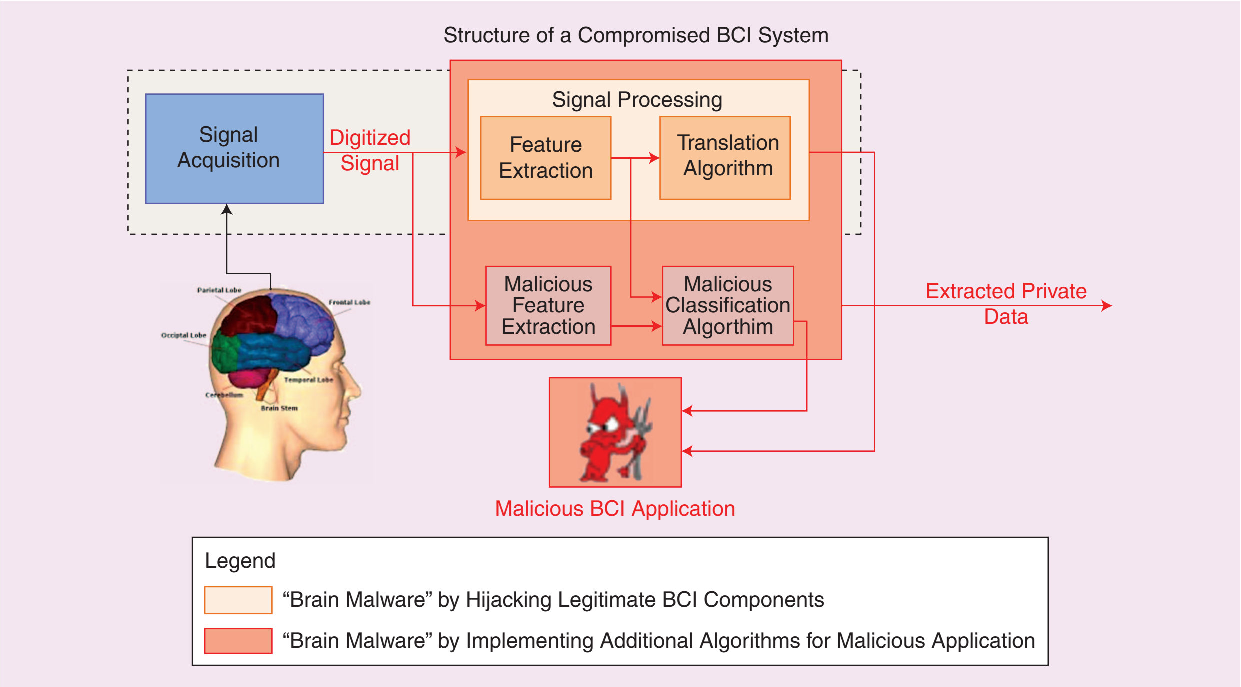

Structure of a Compromised BCI System
Signal Acquisition
Digitized Signal
Signal Processing
Feature Extraction
Translation Algorithm
Malicious Feature Extraction
Malicious Classification Algorithm
Extracted Private Data
Malicious BCI Application
Parietal Lobe
Frontal Lobe
Occipital Lobe
Temporal Lobe
Cerebellum
Brain Stem
Legend
"Brain Malware" by Hijacking Legitimate BCI Components
"Brain Malware" by Implementing Additional Algorithms for Malicious Application

FIGURE 2. A simplified diagram of a compromised BCI system. We distinguish between two types of attackers: a) an attacker who exploits the legitimate feature extraction and decoding (translation) algorithms (denoted as orange blocks in the diagram), and b) an attacker who implements an additional malicious application, and either replaces or supplements the legitimate BCI resources (denoted as red blocks in the diagram).

The basic idea of the BCI Anonymizer is to pre-process neural signals, before they are stored and transmitted, in order to remove all information except specific intended BCI commands. Unintended information leakage is prevented by never transmitting and never storing raw neural signals and any signal components that are not explicitly needed for the purpose of BCI communication and control.

The BCI Anonymizer can be realized either in hardware or in software, as a part of the user's BCI device, but not as part of any external network or computational platform. It thus acts as a secured and trusted software or hardware subsystem that takes the raw neural signal and decomposes it to specific components. Upon request, instead of the complete recorded neural signal, the BCI Anonymizer provides a BCI application only with a needed subset of requested signal components. A block diagram of a BCI system with the proposed BCI Anonymizer component is depicted in Fig. 3. A critical task in the development of this approach is the development of fast and accurate signal processing tools for real time decomposition of neural signals.

The described approach is similar to the approaches taken in smartphone security, where an attacker, using a malicious smartphone app, can attempt to access a user's private identifying information (PII), such as a user's location or address book entries. In the smartphone industry, such attacks on a user's privacy are typically prevented by limiting access to the phone's operating system and a user's PII. In other words, an application only has access to a limited subset of PII data and operating system states and functionalities. (For examples of current prevention and mitigation strategies, please see, e.g., [44], [45]). Neural signals, acquired by BCI recording electrodes, have a similar role as a user's smartphone PII data, in that they contain information beyond the intended information.

Address BCI Privacy Threats in Early Design Phase

Privacy and security threats arising from BCI-enabled technologies may not pose a critical concern at this moment, given the fairly limited deployment of BCI systems outside of research and medical communities. We believe, however, that the right time to address these issues is now, and we propose that methods to prevent and mitigate BCI-enabled privacy and security threats should be developed in the early design phase, and embedded throughout the entire life of the technology.

We view the development of these prevention and mitigation tools as an interdisciplinary effort, involving neuroscientists, neural engineers, ethicists, as well as legal, privacy, and security experts. This article represents an initial step towards facilitating the necessary interdisciplinary discussion and starting the effort to make BCI systems inherently privacy preserving and secure. We are currently examining the best legal and policy infrastructure BCIs, and experimenting with engineering approaches that could lead to best privacy enhancing practices.

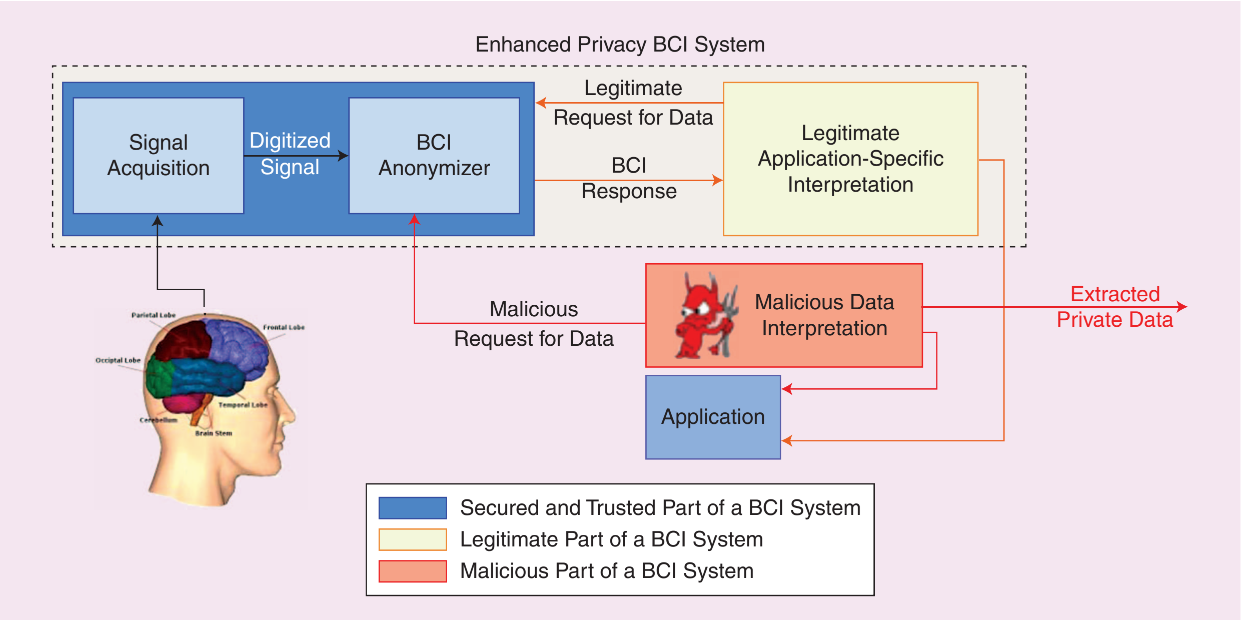

Enhanced Privacy BCI System
Signal Acquisition
Digitized Signal
BCI Anonymizer
Legitimate Request for Data
BCI Response
Legitimate Application-Specific Interpretation
Malicious Request for Data
Malicious Data Interpretation
Extracted Private Data
Application
Parietal Lobe
Frontal Lobe
Occipital Lobe
Temporal Lobe
Cerebellum
Brain Stem
Secured and Trusted Part of a BCI System
Legitimate Part of a BCI System
Malicious Part of a BCI System

FIGURE 3. A simplified diagram of a BCI with the BCI Anonymizer subsystem. A legitimate interpretation component (denoted as light orange block in the diagram) requests data and receives response from the BCI Anonymizer (denoted as light blue block in the diagram). Malicious components, added by the attacker (denoted as red block in the diagram), may request data, but will not receive a response from the BCI Anonymizer. In addition, an attacker cannot access states and functionality of BCI Anonymizer component.

Author Information

Tamara Bonaci and Howard Jay Chizeck are with the Department of Electrical Engineering, University of Washington, Seattle, WA, U.S.A. Email: tbonaci@uw.edu; chizeck@uw.edu.

Ryan Calo is with the School of Law, University of Washington, Seattle, WA, U.S.A. Email: rcalo@uw.edu.

References

[1] Nielsen, "Nielsen acquires Neurofocus," press release, May 26, 2011, http://www.nielsen.com/us/en/press-room/2011/nielsen-acquires-neurofocus.html.

[2] S. Young Rojahn, "Samsung demos a tablet controlled by your brain," *M.I.T. Technology Rev.*, Apr. 19, 2013; http://www.technologyreview.com/news/513861/samsung-demos-a-tablet-controlled-by-yourbrain/.

[3] "NeuroGaming 2013 Conference and Expo: game industry meets consumer BCI's at biggest event to date," *Neurogadget,com*, Jan. 18, 2013; http://neurogadget.com/2013/01/18/neurogaming-2013-conference-andexpo-game-industry-meets-consumer-bcis-at-biggest-event-to-date/6853.

[4] "Neurocam," *Neurowear.com*; http://neurowear.com/projects_detail/neurocam.html, accessed Jan. 19, 2014.

[5] *Emotiv Systems;* http://emotiv.com/, accessed Jan. 19, 2014.

[6] *NeuroSky*, http://neurosky.com/, accessed Jan.19, 2014.

[7] 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 *Proc.21st USENIX Security Symp.*, USENIX, 2012.

[8] M. Pessiglione, L.Schmidt, B.Draganski, R.Kalisch, H. Lau, R. J. Dolan, and C.D. Frith, "How the brain translates money into force: A neuroimaging study of subliminal motivation," *Science*, vol. 316, no. 5826, pp. 904-906, May 11, 2007.

[9] Y.-T. Chiu, "Mind reading to predict the success of online games," *IEEE Spectrum*,Feb. 5, 2013; http://spectrum.ieee.org/consumer-electronics/gaming/mind-reading-to-predict-the-success-of-online-games..

[10] M. Inzlicht, I. McGregor, J.B. Hirsh, and K. Nash, "Neural markers of religious conviction," *Psychological Sci.*, vol. 20, no. 3, pp. 385–392, 2009.

[11] J.P. Rosenfeld, J.R. Biroschak, and J.J. Furedy, "P300-based detection of concealed autobiographical versus incidentally acquired information in target and non-target paradigms," *Int. J. Psychophysiology*, vol. 60, no. 3, pp. 251–259, 2006.

[12] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, *cms.gov*; http://www.cms.gov/Regulations-and-Guidance/Regulations-and-Guidance.html, HIPAA-Administrative-Simplification/HIPAAGenInfo/Downloads/HIPAALaw.pdf, accessed Apr. 12, 2015.

[13] U.S. Federal Trade Commission, *Federal Trade Commission Act*, https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act, accessed Apr. 12, 2015.

[14] J.R. Wolpaw, N. Birbaumer, W.J. Heetderks, D.J. McFarland, P.H. Peckham, G. Schalk, E. Donchin, L.A. Quatrano, C.J. Robinson, and T.M. Vaughan, "Brain-computer interface technology: A review of the First International Meeting," *IEEE Trans. Rehabilitation Engineering*, vol. 8, no. 2, pp. 164–173, 2000.

[15] J.R. Wolpaw, N. Birbaumer, D.J. McFarland, G. Pfurtscheller, and T.M. Vaughan, "Brain-computer interfaces for communication and control," *Clinical Neurophysiology*, vol. 113, no. 6, pp. 767–791, 2002.

[16] J.R. Wolpaw and E.W. Wolpaw. *Brain-Computer Interfaces: Principles and Practice*. OUP USA, 2012.

[17] g-tec Medical Engineering, *gtec.at*; http://www.gtec.at/, accessed Jan. 19, 2014.

[18] B. Popper, "Brain Bats: Learning to play Pong with your mind," *The Verge*, Jul. 11, 2012; http://www.theverge.com/2012/7/11/3149858/brain-bats-play-pong-with-your-mind-neurosky-eeg.

[19] M.-S. Yoh, J. Kwon, and S. Kim. "NeuroWander: A BCI game in the form of interactive fairy tale," in *Proc. 12th ACM Int. Conf. Adjunct Papers on Ubiquitous Computing*. ACM, 2010, pp. 389–390.

[20] J. Contreras-Vidal, "Ethical considerations behind brain-computer interface research," Aug. 2012; http://www.oandp.com/articles/2012-08_12.asp.

[21] N. Farahany, "Incriminating thoughts," *Stanford Law Rev.*, vol. 64, pp. 11–17, 2011.

[22] J. Illes, M.P. Kirschen, J.D.E. Gabrieli et al., "From neuroimaging to neuroethics," *Nature Neuroscience*, vol. 6, no. 3, pp. 205–205, 2003.

[23] J. Illes and E. Racine, "Imaging or imagining? A neuroethics challenge informed by genetics," *Amer. J. Bioethics*, vol. 5, no. 2, pp. 5–18, 2005.

[24] A. R. Jonsen, *The Birth of Bioethics*. U.S.A.: Oxford Univ. Press, 2003.

[25] The Committee on Science and Law, "Are your thoughts your own?: Neuroprivacy and the legal implications of brain imaging," *nycbar.org*, 2005; http://www.nycbar.org/pdf/report/Neuroprivacy-revisions.pdf.

[26] N. Lee, A.J. Broderick, and L. Chamberlain, "What is 'neuromarketing'? A discussion and agenda for future research," *Int. J. Psychophysiol.*, vol. 63, pp. 199–204, 2007.

[27] K. Wahlstrom, N.B. Fairweather, and H. Ashman, "Brain-computer interfaces: A technical approach to supporting privacy," in *Proc. 12th Int. Ethicomp Conf.: The Social Impact of Social Computing*, 2011.

[28] S. Marcel and J.R. Millán, "Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation, *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 743–752, 2007.

[29] R. Palaniappan and K.V.R. Ravi, "A new method to identify individuals using signals from the brain," in *Proc. 4th Joint Conf. on Information, Communications and Signal Processing*, vol. 3, 2003, pp. 1442–1445.

[30] R.B. Paranjape, J. Mahovsky, L. Benedicenti, and Z. Koles, "The electroencephalogram as a biometric," in *Proc. Canadian Conf. on Electrical and Computer Engineering*, vol. 2, 2001, pp. 1363–1366.

[31] M. Poulos, M. Rangoussi, V. Chrissikopoulos, and A. Evangelou, "Person identification based on parametric processing EEG," in *Proc. 66th IEEE Int. Conf. on Electronics, Circuits and Systems*, vol. 1, pp. 283–286, 1999.

[32] A. Riera, A. Soria-Frisch, M. Caparrini, C. Grau, and G. Ruffini, "Unobtrusive biometric system based on electroencephalogram analysis," *EURASIP J. Advances in Signal Processing*, 2008, 2007.

[33] K. Revett and S.T. de Magalhães, "Cognitive biometrics: challenges for the future," in *Global Security, Safety, and Sustainability*. Springer, 2010, pp. 79–86.

[34] H. Bojinov, D. Sanchez, P. Reber, D. Boneh, and P. Lincoln, "Neuroscience meets cryptography: Designing crypto primitives secure against rubber hose attacks," in *Proc. 21st USENIX Security Symp.*, USENIX, 2012.

[35] T. Denning, Y. Matsuoka, and T. Kohno, "Neurosecurity: Security and privacy for neural devices," *Neurosurgical Focus*, vol. 27, no. 1, pp. 1–4, 2009.

[36] B. Luber, C. Fisher, P.S. Appelbaum, M. Ploesser, and S.H. Lisanby, "Non-invasive brain stimulation in the detection of deception: Scientific challenges and ethical consequences," *Behavioral Sciences and the Law*, vol. 27, no. 2, pp. 191–208, 2009.

[37] S.A. Huettel and G. McCarthy, "What is odd in the oddball task? Prefrontal cortex is activated by dynamic changes in response strategy," *Neuropsychologia*, vol. 42, no. 3, pp. 379–386, 2004.

[38] P.R. Wolpe, K.R. Foster, and D.D. Langleben, "Emerging neurotechnologies for lie-detection: Promises and perils," *Amer. J. Bioethics*, vol. 10, no. 10, pp. 40–48, 2010.

[39] M. van Vliet, C. Mühl, B. Reuderink, and M. Poel, "Guessing what's on your mind: Using the N400 in brain computer interfaces," *Brain Informatics*, pp. 180–191, 2010.

[40] R. B. Baldwin, "Kinetic art: On the use of subliminal stimulation of visual perception," *Leonardo*, vol. 7, no. 1, pp. 1-5, Wint., 1974.

[41] United Nations, *The Universal Declaration of Human Rights;* http://www.un.org/en/documents/udhr/, accessed Jan. 26, 2014.

[42] P. Schaar, "Privacy by design," *Identity in the Information Society*, vol. 3, no. 2, pp. 267–274, 2010.

[43]. H. J. Chizeck, and T. Bonaci, "Brain-computer interface anonymizer," Application Number: US 14/174,818, Feb. 2014.

[44] B.-G. Chun and P. Maniatis, "Augmented smartphone applications through clone cloud execution," in *Proc. 12th Conf.on Hot Topics in Operating Systems*, USENIX Association, 2009.

[45] C. Marforio, A. Francillon, and S. Capkun, "Application collusion attack on the permission-based security model and its implications for modern smartphone systems," Dept. of Computer Science, ETH Zurich, 2011.