Brain Hemorrhage: When Brainwaves Leak Sensitive Medical Conditions and Personal Information

Ajaya Neupane*
Department of Computer Science
University of California Riverside
Riverside, USA
ajaya@ucr.edu

Kiavash Satvat*
Department of Computer Science
University of Illinois at Chicago
Chicago, USA
ksatva2@uic.edu

Mahshid Hosseini*
Department of Computer Science
University of Illinois at Chicago
Chicago, USA
mhosse4@uic.edu

Nitesh Saxena
Department of Computer Science
University of Alabama at Birmingham
Birmingham, USA
saxena@uab.edu

Abstract—**Brain Computer Interfaces (BCI) are rapidly gaining popularity in consumer market. It is therefore important to analyze the security and privacy threats these devices may introduce to their users. In this paper, we explore how malicious access to brainwave signals may surreptitiously reveal users' privacy-sensitive medical conditions and personal information, while they are browsing the web (or interacting with an app). At a conceptual level, we investigate the potential of brainwave signals, captured during a user's normal interactions with visual stimuli (e.g., images and audio-visuals) through a website or computer, in exposing whether the user is suffering from a given medical disorder (e.g., drug abuse or autism) and to which demographics group the user belongs (e.g., young vs. elderly or male vs. female). At an empirical level, as two representative case studies into such conceptual attacks, we present a concrete brainwave privacy attack, *(Brain) Hemorrhage*[1], focusing on the leakage of Alcohol Usage Disorder (AUD) and users' age group.**

***Hemorrhage* is designed using machine learning techniques to identify the users suffering from AUD and age group by analyzing the seemingly innocuous brainwave signals leaked online in response to users' viewing of simple images or watching of videos. Based on the publicly available EEG datasets on AUD and aging, our study shows that *Hemorrhage* can predict the presence or absence of alcohol usage disorder with the precision of 96% and the presence or absence of aging condition with 94% accuracy. We also analyze, visualize and interpret the differences in the brainwave signals corresponding to AUD and aging, which serves to justify why our attack succeeds. While the use of neuroimaging devices to diagnose medical disorders in clinical settings is a common practice in the medical field, our study constitutes one of the first steps towards exploring the malicious use of brainwave devices in compromising people's health information privacy in an online setting (otherwise protected under the HIPAA law) as well as their age privacy. Given any website can have unfettered, permission-less access to the signals captured by the current BCI devices, we believe that our work raises a serious online health privacy and age privacy issues as these devices get widely deployed.**

I. Introduction

Electroencephalography (EEG) based Brain Computer Interface (BCI) devices are fast prevailing in the commercial entertainment and gaming market. These devices provide a non-invasive method of recording the electrical fields directly produced by neuronal synaptic activity related to a task, referred to as *event-related potentials (ERPs)*. Vendors like Emotiv[18], Neurosky[44], Neurofocus [43]) have made their BCI devices available in the commercial market. Several applications based on these devices like, hands-free phone dialing application [8] and hands-free control system for gaming applications [35] are already available in these markets.

With the advancement of these devices, and the interesting use cases they facilitate, they are being rapidly introduced in the daily spheres of our lives. These headsets may be worn by people while they are doing different routine tasks like driving, using mobile phones and computers. In this light, it is important to analyze the potential security and privacy threats these devices may introduce, and the measures to mitigate such threats.

One serious issue raised by current BCI devices is that they allow any website (via JavaScript) or an application to have uncontrolled access to the brainwaves recorded via these devices, without the need for a prior approval, or awareness of the user. This opens up many potential attack vectors. Indeed, recent studies [34], [41] have shown that the brainwaves measured when users are viewing images or entering passwords can be leveraged to reveal their private information, e.g.,banking information, PINs and passwords.

In this paper, we take this important line of research to another dimension and study the possibility of exposing the private demographic information and sensitive medical disorders people may be suffering from (and may not want to reveal in public) based on malicious access to brainwave signals during their normal web or computer browsing sessions.

*Work done at UAB.

[1]In the context of our work, the term "Hemorrhage" is an attack against brainwave privacy. Brain Hemorrhage is a type of alcoholic cocktail, and hence the terminology is also intended to capture one of the case studies of our work on Alcohol Use Disorder.

978-1-7281-3265-5/19/$31.00 ©2019 IEEE

Prior medical diagnostic studies have shown that the neural activations in users suffering from medical conditions, such as autism [32], epilepsy [3], depressive disorders and schizophrenia [13], and drug abuse disorders [9] are different than normal healthy users. Given this founding premise, the attackers who obtain the neural signals captured through the BCI devices have the potential to retrieve such private information about users online. This will give attackers the capability to expose the users in public, perform targeted attacks, send targeted advertisements, prejudice against or potentially blackmail them — the possibilities are numerous and devastating.

As a concrete demonstration of our general threat explained above, we empirically investigate the potential of brainwaves maliciously and surreptitiously captured when users are viewing different images or listening to audio/video clips on the website/computer to infer their age group and predisposition to alcoholism, referred to as *Alcohol Use Disorder* (AUD). The previous neuroscience studies have shown that the neural activities are different between alcoholics and non-alcoholics when they are resting or performing some audio/video task [50], [51]. This may be due to the effect of alcohol use on different brain regions. So, we started our study with the hypothesis that the pattern of neural activities when the users suffering from AUD and non-alcoholic users are viewing simple images while browsing the web will be different. These differences in the neural activities can then be used to build automated machine learning models which can identify if a user is suffering from AUD or not. A similar premise applies to the leakage of age group as there may be substantial differences in the brains of young and elderly users.

The knowledge that someone is suffering from AUD or the knowledge that a user belongs to certain age-group could violate the privacy of that individual and make them susceptible to different forms of attacks, social stigma, and discrimination [52]. For example, if an employer learns about an employee's long-term alcohol abuse disorder, it may jeopardize the employment [60]. If an insurance company knows about users suffering from AUD, their premium rates might increase. Similarly, a phishing site can launch targeted attacks based on the medical conditions or the age-range in a hope that they may be more prone to such scams. Also, the online predators might benefit from the potential leakage of age-group on online platform.

Our Contributions and Novelty Claims: In this paper, we introduce a new attack vector called *(Brain) Hemorrhage* that secretly extracts users' private information, particularly the age group and Alcohol Use Disorder from event-related potentials measured by brain computer interfaces online. Our contributions are two-fold:

- We provide two concrete case studies of differentiating between: (1) people suffering from Alcohol Usage Disordes vs. healthy indiviuals, and (2) people belonging to different age groups, in particular young vs. aged. The *Hemorrhage* attack is designed using machine learning techniques to identify the such users by analyzing the brainwave signals in response to users' viewing of simple images or listening of audio/video signals. Such images/videos can be easily embedded as part of a regular benign-looking web browsing session (e.g., on social media sites), image-based CAPTCHAs, gaming or IQ level testing sites, and therefore the attack can remain oblivious to the users. We focus on AUD and aging as our two case studies in this paper given neuroscience literature that human brain may get impacticized with the usage of alcohol and with normal aging effects. Therefore, our goal is to bring these seemingly distinct, but in fact highly relevant, attributes on a common platform through our work.
- Based on two publicly available EEG datasets regarding AUD and aging, we provide a comprehensive analysis of the *Hemorrhage* system. In particular, we first analyze the differences in the neural activities corresponding to alcoholic and healthy participants, and elderly and young subjects then use these differences in neural activations to evaluate the performance of our machine learning based classification models in predicting the users predisposition to alcohol and their age-group. Based on the prior literature [49], [4], [26], [25] we interpret that these differences exist because of the potential damages of brain cells from excessive alcoholic intake in the users suffering from AUD or due to natural aging effects. Our study shows that we can identify the users having alcohol usage disorder with a precision of 96% and age-group with the precision of 94%.

While the use of neuro-imaging devices to diagnose medical disorders in clinical settings is a common practice in the medical profession, our study constitutes one of the first steps towards exploring the malicious use of brainwave devices in compromising people's personal and health information privacy in a web browsing setting, the latter information in particular is otherwise protected under the HIPAA [2] law. Given any website or app can have unregulated access to the signals captured by the current BCI devices without user knowledge, we believe that our work raises a serious online personal and health privacy issue as these devices get widely deployed in the consumer domain.

Related to *Hemorrhage*, recent research studies [34], [41] have shown that EEG signals measured from BCI devices can be exploited to extract private information, e.g., PINs or passwords, known to users. Our study is radically different from these prior studies in the type of information we learn from the brainwave signals. While the previous studies focused on PINs and passwords, we study the potential of leakage of personal and medically sensitive information, like drug usage, diseases, and mental disorders getting exposed via brain signals. We believe that the stolen PINS or passwords can be used by attackers until they are changed by the victim users, but the personal information and medical conditions may be more persistent (possibly long-lasting or even permanent) and can have a potentially more severe impact on the privacy, security and safety of individuals.

II. Background & Prior Work

A. EEG & BCI Devices Overview

Electroencephalography is a non-invasive methodology of measuring brain's neural activities in terms of event related potentials (ERPs) with high temporal resolutions. These ERPs contain the number of peaks which are related to different cognitive events and therefore can be used to understand human information processing in real time [16]. The BCI devices measure such ERPs when users are performing a task. The current commercial BCI devices may not be equally capable as clinical-grade devices, however, with the involvement of industrial giants like Facebook [21] and Neuralink [42] leading their development, more sophisticated devices are imminent. These devices, with a capability similar to clinical devices (like the one employed in the dataset used), will become mainstream in the near future and the attacks we have studied in the paper will be more viable and devastating.

B. Related Work

EEG-based BCI devices have been explored by researchers as a vector of side-channel attack to retrieve users private information [34], [24], [41]. Martinovic et al.[34] presented the possibility of inferring users' private information (e.g., user's PINs, passwords, banks, ATMs) by analyzing the brain signals measured by a BCI device when users were viewing images of many banks, numbers, and ATMs. These images familiar to users evoked different neural responses. So, when a user saw an image of the bank with which he has an account or the digit which he uses often in his PIN code, he had high peak ERPs. This was further exploited to explore users' private credentials. Frank et al. [24] proposed similar, but a less intrusive subliminal attack. They exposed victims to portrait pictures for a duration insufficient for conscious cognitive perception and extracted whether the user knew the identity of the person in the picture. Neupane et al. [41] used event related potentials measured when participants were entering random PINs/passwords to deduce the entered digits or alphabets. Our *Hemorrhage* study is different compared to previous work as we study the feasibility of exposing privacy-sensitive information and disorders, unlike PINs/passwords, upon sniffing the brain signals. Also, the attacks they proposed considered access to brain signals via malicious website only, while we study the feasibility of malicious websites' access to these brain signals via JavaScript, which makes the attack easier and more powerful (as no malicious application needs to be installed on the users' devices).

EEG has also been employed by researchers to classify mental states of a user [6], [5], drowsiness [29] and mental tasks users are performing [58], [20]. Brain signals recorded by EEG-based BCI devices have been used to replace mouse or joysticks in mindgames [22]. The ERP measured in an independent color-naming stroop task is found to be correlated to users' beliefs in God/religion [28]. Waismann et al. [61] and Flor et al. [23] have correlated ERPs with sexual orientation, and sexual interests of the users. Somewhat related to our work, the BCI devices are also used to understand user behavior in security tasks (e.g., [38], [39], [40]).

Apart from EEG, fMRI, and fNIRS based neuroimaging devices have also been used to understand users' neural activations in several tasks. Doehrmann et al. [15] showed angry vs. neutral faces or emotional vs. neutral faces to participants with social anxiety disorder to predict their response after cognitive behavioral therapy. They found that brain imaging can provide biomarkers that substantially improve predictions for the success of cognitive behavioral intervention. Chai et al.[11] used resting state brain images were used to understand the possibility of depression on children of the parents with depression. Shanon et al. [55] used resting state brain images to identify impulsivity in juvenile offenders. These studies depict the potential of brain waves in leaking the users' sensitive private disorders, which serves as a premise for our work.

Similar to our work, there are neuroscience studies showing differences in event related potentials, and the continuous EEG between alcoholics and non-alcoholics [50], [51], [19]. However, the tasks used in these studies (oddball paradigm Audio/Visual task [19] and resting state [50]) are difficult to exercise in real world web browsing attack settings as they could make users suspicious of the attacks, or users may not wear these devices in resting state. Also, unlike our work, these neuroscience studies do not show how attackers can exploit brain signals to reveal users' sensitive medical conditions during web-browsing sessions. The novel aspect of our study is the way stimuli can be presented to capture a real-world attack, which is not captured in these prior neuroscience studies.

Similarly with respect to the literature on aging, [64], [14] showed that brain signals patterns gradually alter with age, meaning that the neural activities in elderly people differ from that of young people. [14] used deep learning methods to predict individual's brain age. However, no prior study has investigated the adversarial context of aging information that may leak from brainwaves.

III. Attack Scenarios

Brain Activity Correlates with Visual Stimuli: Pictures and mental tasks have been used by several neuroscience researchers to understand user behavior in different tasks. The ERPs generated in the brain when users view different images are associated with users' familiarity or unfamiliarity with those images. So, the malicious attacker with access to these ERPs has the potential to infer stimuli known or unknown to the users. The researchers [34], [41] have previously used this nature of ERPs to extract private information.

Further, the researchers have shown that the neural activations during simple visual tasks in users with autism [32], depressive disorders and schizophrenia [13], and drug usage problems [9] are different from those compared to normal healthy users. So the attackers who obtain the neural signals have potential to retrieve such information about the user.

Attack Model: Learning Private Information via Simple Image Display: Based on these prior studies, we focus on the vulnerability of the brain signals in revealing the age-range of users or their medical conditions, specifically the privacy sensitive alcohol usage disorder. To perpetrate our proposed *Hemorrhage* attack, the adversaries can design and develop BCI-based malicious applications or websites. The users using these websites will find them to be benign as the interface may only contain images or require inconspicuous mental tasks. To evaluate the *Hemorrhage* attack setting, we used two pre-existing datasets involving the AUD and aging (see section VDescription of Datasetssection.5). To emulate our *Hemorrhage* attack, therefore, the attacker can develop a website disseminating interesting news items or other content. The attacker can then ask its users to view some images for the first few seconds before they enter the website. Also, the images can be embedded in the form of CAPTCHAs the users need to solve prior to accessing some information on the website. The audio/video can be embedded in the websites as an advertisement. The attacker can then collect the brain signals when users are viewing these images. The brain signals recorded while performing these tasks can be used to infer

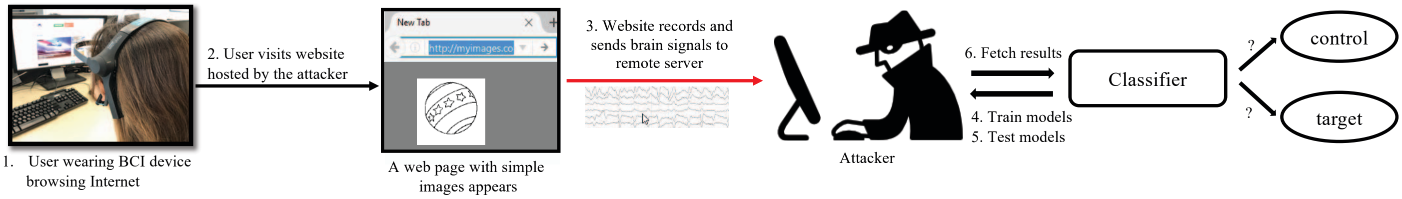


Fig. 1: High level overview of our attack: how malicious access to brain activity correlated with visual stimuli can be used to learn targeted (medical and aging) information via simple image display in a routine web browsing interaction.

users' private information, specifically the predisposition to alcohol usage disorder or the age group information. Figure 1High level overview of our attack: how malicious access to brain activity correlated with visual stimuli can be used to learn targeted (medical and aging) information via simple image display in a routine web browsing interaction.figure.caption.1 depicts how an attacker can infringe an individual's privacy sensitive information when browsing a website.

Attack Consequences: Learning medically sensitive disorders such as alcohol abuse or the age-group of the user can have frigid implications. This may enable attackers to launch targeted phishing attacks against users, and extract other private information from users' neural activity, for example, familiar faces or voices, familiar places, familiar cuisines, etc. The information can be used for user modeling to launch targeted ads, targeted attacks, or even for blackmailing users. Knowing the medical disorders of users, the attackers can launch targeted medical scams which can eventually harm people. The employers learning about these disorders and behaviors can harm the growth of the employee irrespective of his/her capability. Also this breach of privacy may negatively impact victims in their health insurance, social relationships, and potential opportunities.

Remotely Monitoring Brainwaves: While the previous brain privacy leakage studies [34], [41] only focused on the access to the brainwave signals by malicious mobile applications, we tested the feasibility of malicious websites to obtain the brain signals measured by BCI devices without user knowledge using Neurosky [45], a commercially popular BCI headsets.

NeuroSky offers a list of APIs which provides the potential to interact with their devices [62], [45], [47]. We used this EEG-based headset record brainwave signals through a webpage. This simulates a potential for a real world attack which can be launched against the users of this device during their web navigation. This process occurs in the background and in a silent manner using a JavaScript when a user is browsing the malicious webpage. For testing this scenario, we set up a remote server to open a socket and listen to the incoming traffic from the client side using node package manager (NPM) [45], [47].

The JavaScript code in the website collected the users' brain signals and sent them to a remote server, which in our case was a node server, through a socket connection. This depicts the attackers capability to remotely monitor brain signals measured by BCI devices to infer users' private information at real time.

IV. Threat Model

In our study, an attacker is a malicious adversary trying to gain access to the users' private information, and a victim is the user whose private information is targeted. We assume the attacker is technically knowledgeable and equipped to develop desktop or mobile applications capable of capturing event related potentials measured by brain computer interfaces when victims are browsing websites or entering private information. The goal of the attacker in this study is to extract private sensitive information about victims, surreptitiously monitoring their brain signals.

We consider two phases for our attack model. In the first phase, the attacker creates a training model of the user behavior, and in the second phase, the attacker uses the model to predict the behavior of the user he is attacking.

Training Phase: The attacker can develop a training model to detect the age range of users or identify users suffering from AUD using the data collected on his own. He can run a research or crowd-sourced study with healthy and alcohol usage disorder users and also with elderly and young people. The task can be similar to the one employed in the study used for collecting the dataset used in our paper [65]. The attacker can then process this dataset and extract features to build machine-learning based classification models.

In general, there are also several publicly available neural datasets [54], [7]. The attacker can choose a relevant study, their dataset and build a training model using it. The training model will be dependent on the stimuli used in these studies. However, it will not be difficult for attacker to simulate these stimuli in real-time attacks. Also, the attacker can choose the designs easier to implement in real-life attacks. The creation of these training models can be cost-effective to attackers.

These training models are easier to build unlike the training models proposed for attacks in [34], [41]. Martinovic et al. [34] and Neupane et al. [41] proposed the threat model which works better only if the training data was collected from the potential victims themselves. However, our training model can be built from a general population and be used to launch attacks on targeted individuals.

Testing Phase: The attacker can develop websites or applications hosting the tasks he used to develop the training model. The tasks can be embedded such that the users may not become suspicious. For example, as discussed in Section IIIAttack Scenariossection.3, the images can be embedded in the pop-ups where advertisements are loaded. These websites have unrestricted access to the brain signals measured by BCI devices, and hence the attacker can capture the brain signals when users are viewing these images without user knowledge.

These neural activities captured by the website can then be sent to the remote attacker, who then uses it to infer user's private information.

In another attack model, we can assume that the attacker has developed a malicious website with in-built training model. This website can be used to identify the private information in real time and use it for targeted attacks.

V. Description of Datasets

A. AUD Dataset

The dataset were recorded by an EEG device (ECI, Electrocap International) of sampling rate 256Hz at the Neurodynamics Laboratory, SUNY Downstate Medical Center [17], [59]. The device had 64 electrodes of which two electrodes were mounted for Electrooculography (EOG) and one nose electrode. All scalp electrodes were referred to Cz. The electrodes were positioned based on international 10-20 system [48] at the following locations: "FP1", "FP2", "F7", "F8", "AF1", "AF2", "FZ", "F4", "F3", "FC6", "FC5", "FC2", "FC1", "T8", "T7", "CZ", "C3", "C4", "CP5", "CP6", "CP1", "CP2", "P3", "P4", "PZ", "P8", "P7", "PO2", "PO1", "O2", "O1", "X", "AF7", "AF8", "F5", "F6", "FT7", "FT8", "FPZ", "FC4", "FC3", "C6", "C5", "F2", "F1", "TP8", "TP7", "AFZ", "CP3", "CP4", "P5", "P6", "C1", "C2", "PO7", "PO8", "FCZ", "POZ", "OZ", "P2", "P1", "CPZ", "nd" and "Y". The electrodes 'X' and 'Y' measured electrooculography (EOG) signals, and 'nd' was a reference nose electrode. The trials with excessive eye and body movement were rejected online.

In the study, the data was collected from a group of alcoholics and control subjects for the study of participants' genetic predisposition to alcoholism. There were 45 right-handed male participants with an age range of 19.4 – 38.6 years in the control group and 77 male participants with an age range of 22.3 – 49.8 years in the alcoholic group. The alcoholic participants had a history of heavy drinking for a minimum of 15 years and were diagnosed with alcohol abuse or dependence by the psychiatrist [30]. However, the subjects were abstinent from alcohol at least 28 days before the start of the experiment. The control participants had no history of personal or family alcohol or drug abuse.

The participants were shown a series of object pictures chosen from the Snodgrass and Vanderwart picture set [56]. Two picture stimuli appeared in succession with a 1.6 sec fixed interstimulus interval. The duration for the first (S1) and second (S2) picture stimulus in each trial was 300ms where the interval between each trial was fixed to 3.2 sec. All the pictures were paired either as matching or non-matching conditions. The participants pressed mouse key in one side if the S2 matched S1 and to press a mouse key in the other side if the S2 differed from S1.

B. Aging Dataset

The dataset [1] was recorded by an EEG device (SA Instruments, Home-Grown Digitizer, Electro-Cap International) of sampling rate 100Hz at the University of California, San Diego. The electrodes were positioned based on international 10-20 system [48] at the following locations: "Fp1", "Fpz", "Fp2", "AF3", "AF4", "F7", "F3", "Fz", "F4", "F8", "FC5", 'FC1", "FC6", "FC2", "T7", "C3", "Cz", "C4", "T8", "CP5", "CP1", "CP2", "CP6", "P7", "P3", "Pz", "P4", "P8", "PO3", "PO4", "O1", "Oz", "O2", "LM", "Reye", "LEye". The data [1] was collected from a group of 49 elderly and young subjects with no history of psychiatric, neurological, or medical disorders, to study the impacts of aging on the processing of sensory auditory and visual stimuli [10]. From the total 49 participants attended in the experiment, we chose 46 subjects (three participants were removed from our study due to the significant interruption during data collection), 18 subjects with an age range of 20 to 40 years in the young group and 28 subjects with an age range of 67 to 89 years in the elderly group. In the experiment, there were one Focus Auditory (FA) block and one Focus Visual (FV) block which were followed by 12 Shift (SH) blocks and another 3 FA and FV blocks each for each of the participants. There were no specific order of the FA and FV sequences and it was randomized across subjects. In the Shift condition, participants need to move their attention between the visual modality and the auditory modality based on the order that 'Look' and 'Hear' cues appear. The stimuli were displayed in blocks of 264 for a duration of 2.64 min [10].

TABLE I: Statistical analysis between average ERPs of AUD users and control users at multiple channels using Mann-Whitney U Test. The channels are grouped into different columns based on the brain regions they measure.

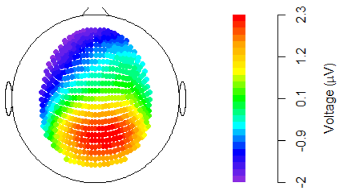
Frontal		Central		Temporal		Parietal		Occipital	
Ch	**Sig**	**Ch**	**Sig**	**Ch**	**Sig**	**Ch**	**Sig**	**Ch**	**Sig**
AF1	.000	C1	.248	T7	.034	CP1	.000	O2	.000
AF2	.000	C2	.059	T8	.001	CP2	.000	O1	.000
AF7	.000	C3	.002	P5	.000	CP3	.000	POZ	.000
AF8	.007	C4	.002	P6	.000	CP4	.000	PO7	.000
AFZ	.000	C5	.015	P7	.000	P1	.000	OZ	.000
F1	.000	C6	.017	P8	.000	P2	.000	PO2	.000
F2	.000	FC1	.000	TP7	.001	P3	.000	PO1	.000
F3	.000	FC2	.000	TP8	.000	P4	.000	PO8	.000
F4	.000	FC3	.000	FT7	.041	PZ	.000		
F5	.000	FC4	.000	FT8	.000	CPZ	.000		
F6	.000	FC5	.000	CP5	.000				
F7	.004	FC6	.001	CP6	.000				
FP1	.000	FCZ	.000						
FP2	.000	CZ	.006						
FZ	.000								
FPZ	.000								
F8	.000								

VI. Neural Signatures

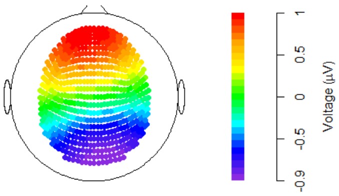
In this section, we analyze the ERPs collected in the dataset used to evaluate the performance of the *Hemorrhage* attack system in detecting young vs. elderly individuals, and alcoholic vs. healthy group of users. We designed a neural analytics software to average the ERPs measured at different electrodes related to each trial presented in the experimental task of the dataset for each participant in the aging and AUD datasets.

A. AUD Signatures

For AUD analysis, each trial was represented by a row vector with 61 values representing 61 channels each. Then, the ERPs were averaged across all trials at each channel to represent a user with a single row vector. The row vector was labeled as alcoholics or control condition depending on dataset they belonged to. We then performed the statistical analysis on the neural data. We were interested in measuring the differences in the ERPs between alcoholics and control



(a) Control Group



(b) Alcoholic Group

Fig. 2: Visualization of ERPs in different regions for (a) the control group and (b) the alcoholic group.

participants to find the unique neural markers related to alcohol usage disorder. First, we used *Kolmogorov-Smirnov Test* to determine if the data was normally distributed. The p-value of the test was statistically significant ($p<.05$) showing that the distribution of the data was non-normal. The study procedure followed a "between-subject" methodology. So, we used the *Mann Whitney U Test* for measuring the differences in the mean ERPs of alcoholics and control groups. Since we had performed 61 pairwise comparisons, we applied Bonferroni correction on the p-value and considered the comparisons with the significance level (p-value) less than .0008 to be statistically significant. After correction, we observed that there were statistically significant difference in the means of the ERPs measured by all channels except AF8, F7, C1, C2, C3, C4, C5, C6, CF, C6, CZ, FC6, FT7, T7, TP7, and T8, between alcoholic and control users. Table IStatistical analysis between average ERPs of AUD users and control users at multiple channels using Mann-Whitney U Test. The channels are grouped into different columns based on the brain regions they measure.table.caption.2 depicts channels with statistically significant differences in mean distribution of ERPs after Bonferroni correction.

For better demonstration of brain response differences between the groups of alcoholic and controlled participants, we used a dense spatial plot (see Figure2Visualization of ERPs in different regions for (a) the control group and (b) the alcoholic group.figure.caption.3) which represents brain activity across the different participants to specifically show how the brain signals could be varying from one group to another. It can be seen that there are notable differences in ERPs between alcoholic and controlled participants in frontal and occipital lobes of the brain. For example, the central region does not show notable differences in ERPs between alcoholic and control participants.

B. Aging Signatures

In the aging case, each trial was represented by a row vector with 36 values representing 36 channels each. We took the same approach as the AUD case to represent a user with a single row vector. The row vector was labeled elderly or young depending on group they belonged to. On using WSRT, running pair-wise comparison of EPRs between elderly and young, we observed statistically significant differences at PO4 ($p = .035$). In Figure 3Visualization of ERPs in different regions for (a) the elderly group and (b) the young group.figure.caption.4, we also demonstrate the brain response differences between the groups of elderly and young people and show how the brain signals could be varying from one group to another.

C. Interpretation of the Differences

The differences in the neural activities between the users suffering from AUD vs. healthy individuals may be due to the effect of excessive alcohol intake in different neural regions. Previous research studies [49], [4], [26], [25] have reported damages of brain cells due to excessive alcohol usage. Berman and Marinkovic [49] reported the negative impact to the frontal-related systems including temporal, parietal and occipital areas, due to alcoholism-related aspects. Gilpin and Koob [25] suggested that chronic exposure to alcohol reduces the volumes of brain structures, including cerebellum, prefrontal cortex, and orbitofrontal areas. Similarly, Bellis et al. [4] in their fMRI study also found decreased activation in the prefrontal cortex and cerebellum.

In case of elderly users, the brain activities are different compared to young as the neurons die with age [53]. The differences in neuronal activities between elderly and young is observed with the decline in the cognitive functions, e.g., attention and memory and vision [36].

In light of these findings, in our study, the ERPs generated when users were viewing the images or listening to audio/video may have been distinguishable due to the differences in the healthiness of the brain areas between alcoholics and control users and between young and elderly.

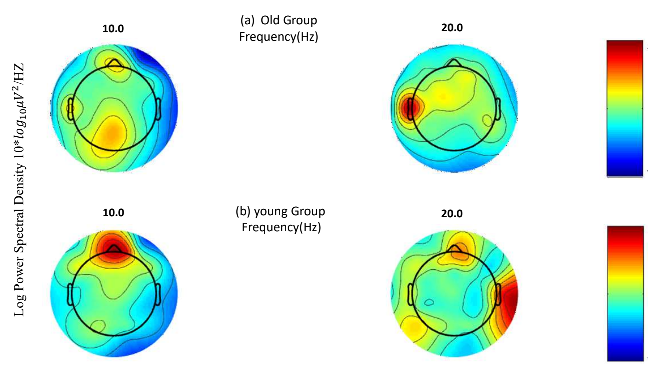


Fig. 3: Visualization of ERPs in different regions for (a) the elderly group and (b) the young group.

VII. Machine Learning Design & Results

We had observed the statistically significant differences in average ERPs measured at multiple channels between the users suffering from AUD and healthy users (Section VINeural Signaturessection.6). We have also witnessed a significant difference in average ERPs measured during the experiment between elderly and young people. In this section, we compute feature vectors representing the users suffering from AUD (alcoholic class) and healthy users (control class), and similarly extract feature vectors which differentiate elderly from young people. We further develop machine learning based classification models to automatically identify the the users suffering from AUD subjects from healthy subjects, and the elderly from young. To this end, we design classifiers, with the features generated from ERPs measured at each channel.

A. Classifiers and Performance Measures

The neural data was processed as discussed in Section VINeural Signaturessection.6. We then extracted features from the neural data to build different classifiers each based on different machine learning algorithms, e.g., *Trees* – Decision Tree (J48), Logistic Model Tree (LMT), Random Forest (RF) and Random Tree (RT) ; *Functions* – Neural Simple Logistic, Multilayer Perceptron (MP), Logistic Regression LR, Support Vector Machines (SMO), *Meta* – AdaBoostM1, meta.Bagging, *Lazy* – k-nearest neighbor algorithm (IBK), and *Rules* – JRip. We present classifiers with the best performance for both AUD and aging.

To measure the performance of these classification models in identifying the users suffering from AUD vs. healthy users and elderly from young users, we calculated the false positive (FP), false negative (FN), precision ($Prec$), recall (Rec), and F-measure (FM) metrics. *True positive* (TP) is defined as the total number of correctly identified instances belonging to the alcoholic class (the young class in the aging case) while the *true negative*(TN) is the number of times samples belonging to the control class (the elderly class) is rejected. Similarly, *false positive* (FP) represents the number of misclassified control instances (elderly instances) incorrectly recognized as alcoholic class (as young class) and *false negative* (FN) shows the number of times the alcoholic class (young class) is rejected. Based on the retrieved true positive, false positive, and false negative instance, we compute precision, recall, and F-measure as shown in equations eqs. (1) and (2).

$$precision = \frac{TP}{TP + FP}; recall = \frac{TP}{TP + FN} \tag{1}$$

$$F - measure = 2 * \frac{precision * recall}{precision + recall} \tag{2}$$

TABLE II: AUD Classification: Precision (Prec), Recall (Rec), False Positive Rate (FPR), False Negative Rate (FNR) and F-Measure (FM) obtained on testing a set of instances on training model

Classifier	**Prec**	**Rec**	**FPR**	**FNR**	**FM**
RandomTree	1.00	0.45	0.00	0.55	0.63
Logistic Regression	0.77	0.91	0.30	0.09	0.83
Multilayer Perceptron	1.00	0.82	0.00	0.18	0.90
SMO	1.00	0.91	0.00	0.09	0.95
LMT	1.00	1.00	0.00	0.00	1.00
Random Forest	1.00	1.00	0.00	0.00	1.00
Simple Logistic	1.00	1.00	0.00	0.00	1.00
Average	0.96	0.87	0.04	0.13	0.90

Precision is the accuracy of the system in rejecting instances belonging to the control classes. *Recall* is the accuracy of the system in accepting instances belonging to the alcoholic classes. Low recall leads to high rejection of positive instances, hence unusable, and low precision leads to high acceptance of negative instances, hence insecure. So we compute *F-measure* as the harmonic mean of the precision and recall of the test. It depicts the balance between precision and recall. High F-measure represents a good classification system.

B. AUD Classification

We computed the mean, slope, skew, kurtosis, and standard deviation of the ERPs measured from alcoholic and controlled users from fifty-nine channels. We excluded two channels (C1 and C2) from feature extraction as we did not see statistically significant differences in mean ERPs in our statistical analysis (Section VINeural Signaturessection.6). This resulted in a feature vector of length 295 (59 channels * 5 features per channel) for each participant. The feature vectors were labeled as alcoholic and control conditions based on the group they belonged to. Our dataset had an unequal number of the users suffering from AUD (77) and control users (44). So we only used randomly selected 44 the users suffering from AUD to make the training and testing instances equal among these two groups.

We used a "train-test" model for our classification task. In this model, the classifiers were first trained with the 34 randomly selected instances from AUD and control users each. Next, we used the remaining 10 instances from alcohol and control users as the testing set ("unseen data"). We computed the performance metrics of some classifiers in correctly predicting the groups those instances were belonging to. The results from the classifiers with the best performance are presented in table IIAUD Classification: Precision (Prec), Recall (Rec), False Positive Rate (FPR), False Negative Rate (FNR) and F-Measure (FM) obtained on testing a set of instances on training modeltable.caption.5. The classifiers, namely, LMT, RandomForest, and SimpleLogistic, achieved maximum F-measure of 100% in predicting these instances. We see that the average false positive is 4% and false negative is 13% and the average F-measure is 90%, which are significantly better than random classification model (50%). We observed the differences in average F-measure of classifiers statistically significantly greater than the average F-measure of the random classifier in the Mann-Whitney U Test ($p<.005$).

The results obtained from these classification models were significantly better than the random accuracy and demonstrate that EEG-based neural data can be used in the development of an automated mechanism to detect the users suffering from AUD. This shows the feasibility of new attack mechanisms based on the recorded neural cues via *Hemorrhage*.

C. Aging Classification

We computed mean, skew, kurtosis, and standard deviation of the ERPs measured from elderly and young users from thirty-six channels. After statistical analysis and visualization of all the calculated features, in the aging case, we realized that while the combination of features (e.g., skew, kurtosis, and standard deviation) does not show statistically significant differences between elderly and young subjects, the mean ERPs of elderly subjects significantly differs from that of young subjects. Therefore, we chose the mean ERPs feature as the final predictor of the type variable (e, y), since it perfectly distinguishes elderly from young group. We extracted and employed a feature vector of length 36 (36 channels of mean ERPs) for each participant. The feature vectors were labeled as e (elderly) and y (young) based on the group they belonged to. Among the 46 subjects participating in the experiment, 18 belong to the young class and the remaining 28 belong to the elderly class.

Like for AUD classification, we employed the train-test model aging classification. Here, the classifiers were first trained with the 36 randomly selected instances from elderly and young groups. Next, we used the 10 remaining instances including both the elderly and young users as the testing set ("unseen data"). We computed the performance metrics of some classifiers in correctly predicting the groups those instances were belonging to. The results from the classifiers with the best performance are presented in table IIIAging Classification Per-Channel: Precision (Prec), Recall (Rec), True Positive Rate (TPR), False Positive Rate (FPR) and F-Measure (FM) obtained on a set of instances on training modeltable.caption.6.

TABLE III: Aging Classification Per-Channel: Precision (Prec), Recall (Rec), True Positive Rate (TPR), False Positive Rate (FPR) and F-Measure (FM) obtained on a set of instances on training model

Classifier	Prec	Rec	TPR	FPR	FM
Simple Logistic	0.92	0.90	0.90	0.06	0.90
LMT	0.92	0.90	0.90	0.06	0.90
Random Forest	0.87	0.80	0.80	0.13	0.80
IBK	1.00	1.00	1.00	0.00	1.00
AdaBoostM1	1.00	1.00	1.00	0.00	1.00
JRIP	1.00	1.00	1.00	0.00	1.00
meta.Bagging	1.00	1.00	1.00	0.00	1.00
J48	0.85	0.80	0.80	0.30	0.78
Average	0.945	0.925	0.925	0.193	0.925

In the aging case, the classifiers JRIP, IBK, AdaBoostM1 and Bagging, achieved maximum F-measure of 100% in predicting the elderly and young instances. The average false positive is 19% and the average precision and F-measure are 94% and 92% respectively which indicate that the classifiers perform noticeably better than random classification model.

VIII. Discussion and Future Work

Practicality of the Attack: In this paper, we studied how attackers with access to the brain signals can retrieve privacy-sensitive personal demographic information and medical conditions while users are browsing the web or interacting with an app. We used publicly available EEG datasets to show the feasibility of such attacks. We note that it is extremely challenging to conduct a real-world validation of our attack, especially in the context of AUD medical condition, since we need to work with participants that have a pre-existing medical condition (alcoholism), which raises significant IRB issues and recruitment hurdles. To address this real logistical challenge, our study was carefully designed to work with classical, public datasets collected by medical scientists.

The currently available commercial-grade BCI devices may not be equally capable as a clinical-grade EEG device. Although validating our attack on low-grade BCI devices may make our work more practical, even high-grade devices (like the one employed in our study dataset) *are being currently used in real-world* under daily web browsing scenarios, which serve to meaningfully demonstrate that our attack is applicable to current real-world settings. A representative example of the application of high-end devices (e.g., the B-Alert EEG Headset) in real-life settings is *NeuroStorm*, a dynamic game introduced by Cubic Global Defense, presented at the Google I/O Developers Conference [46]. B-Alert is a high-grade wireless EEG device which can be used continuously for long hours (e.g., during web browsing and even sleep monitoring) without any inconvenience which was associated with traditional EEG devices [57].

Also the advancement of BCI devices is on the rise. The technology giants like Facebook [21] and Neuralink [42] are researching to make it possible to "type" directly using your thoughts. In this light, we believe that the threat we explored *exists currently* and can be even more devastating in the foreseeable future. Apart from EEG-based BCI devices, researchers are also working on fNIRS-based BCI devices [37], and hybrid EEG-fNIRS-based BCI devices [33]. fNIRS measures the brain activity through hemodynamic responses and has higher spatial resolution than EEG. So the future commercial BCI devices have the possibility of becoming more competent than the current BCI devices or even the clinical-grade devices such as the one used in our study data set.

While it is almost clear that the future BCI devices will be more advanced, the currently available BCI devices are also equally capable of reading users' thoughts. Martinovic et al. [34] and Neupane et al. [41] have shown the feasibility of side-channel attacks with these commercial-grade BCI to reveal users private information.

Subliminal Stimuli & Resting State Attacks: In this study, we discussed the possibility of revealing users' privacy sensitive information when they are performing the visual task like browsing images wearing the BCI device. Presenting the images of attackers' choice to victims is not a difficult task as we argued, although it would be useful to make this process as seamless and transparent to the user as possible so there is little potential to raise suspicion. In this direction, it is possible that these images can be shown to users at the levels below their cognitive perception. A previous study [24] has shown the possibility to extract information using the visual stimuli hidden within the screen content that the user expects to see, for a duration of time that does not exceed 13.3 milliseconds, similar to subliminal advertisement [31]. The use of such subliminal stimuli will make our specific attack more hidden and oblivious to the user, and could be tested in future research.

Apart from visual stimuli, the brain signals acquired when users are not performing any task, e.g., resting state, can also be used to reveal users' privacy sensitive information. Chai et al. [11] used resting state brain images to understand the possibility of depression on children of the parents with depression. Shanon et al. [55] used resting state brain images to identify impulsivity in juvenile offenders. These studies could be translated to give rise to resting state health privacy attacks.

Observing the current popularity of BCI devices, their usage in users' daily spheres of lives is imminent. Yuan et al. [63] predicted that neurodevices will gradually replace the keyboard, the touch screen, the mouse and the voice command device. So the users in future may be wearing them unknowingly throughout the day like the current Bluetooth headsets and headphones. In such scenarios, the malicious attacker can have continuous access to the users' brain signals when they are performing several tasks or even resting. The attacker can also store these signals and analyze them offline to extract privacy sensitive medical conditions. This information may also be used for tracking a user as the neural activities may possibly have unique signatures based on the users' location. Further work must be undertaken to assess these attack possibilities.

Possible Technical Defenses: One of the possible strategies to mitigate the brainwave privacy threat is to automatically insert noise in the neural signals to suppress the features representing the privacy sensitive disorders. However, such suppression might affect the functionality of the benign applications. Brain-computer interface anonymizer [12] which can filter one or more features related to the privacy sensitive information has been proposed to prevent such attacks. However, to accurately identify such features suppression is another challenge and should be the subject of future research.

The another problem with the current BCI device is their permission models. The third-party applications or websites are offered unfettered access to the neural signals captured by the BCI devices without the users consent. This can be managed by introducing proper permission models, such that the applications cannot record brain signals without the users knowledge. The users should be informed when an app or a website is accessing the brainwave data like the permission models for microphone and camera. Concretely, a browser plugin can be designed that monitors access to brainwave signals and alerts the user accordingly. Future work could focus on these defensive mechanisms.

Introduction of Privacy Laws: Another way to mitigate the problems relating to brainwave privacy leakage is by preventing unauthorized access, collection, sharing and manipulating of information from the brain via introducing privacy laws [27]. With the possibility of attackers reading human thoughts and human medical conditions, the human rights such as privacy, freedom of thought, etc. are impacted. In this line, Ienca and Adorno in their study [27] proposed four new rights, namely, the right to cognitive liberty, the right to mental privacy, the right to mental integrity, and the right to psychological continuity to prevent malicious entities from retrieving unauthorized information from the brain signals. Such privacy laws may help reduce the impact of attacks.

IX. Concluding Remarks

The popularity of BCI devices is on the rise. In light of this trend, neural devices will be embedded in daily spheres of users' lives. Thus, it is important to study the possible security and privacy vulnerabilities of such devices. In this paper, we examined the possibility of one such side-channel attack, *Hemorrhage*, for the purpose of inferring users' sensitive demographic information (specifically age group), and their privacy sensitive medical conditions (specifically AUD), which otherwise is a protected health information. We observed statistically significant differences in neural activities between alcoholic and control participants when they were viewing simple images, and between young and elderly participants when they were watching audio-video samples, as part of our attack model. On the basis of these differences, we built a machine learning based detection engine, which identified participants age group with the precision of 94% and their AUD condition with an average precision of 96% when features from all channels were considered. We also discussed the feasibility of other conceptual attacks related to *Hemorrhage* and the possible defensive measures. Our work represents a crucial preemptive step to raise community's awareness of brainwave healthy privacy and demographic privacy risks as the future BCI devices with better signal ratio will probably improve the accuracy of these attacks.

References

[1] Auditory-Visual Shift Study. Available at: http://headit.ucsd.edu/studies/8d6dbb78-a236-11e2-b5e7-0050563f2612/description, 2017.

[2] Act, A. Health insurance portability and accountability act of 1996. *Public law 104* (1996), 191.

[3] Ahammad, N., Fathima, T., and Joseph, P. Detection of epileptic seizure event and onset using eeg. *BioMed research international 2014*.

[4] Bellis, M. D., Narasimhan, A., Thatcher, D. L., Keshavan, M. S., Soloff, P., and Clark, D. B. Prefrontal cortex, thalamus, and cerebellar volumes in adolescents and young adults with adolescent-onset alcohol use disorders and comorbid mental disorders. *Alcoholism: Clinical and Experimental Research 29*, 9 (2005), 1590–1600.

[5] Berka, C., Levendowski, D. J., Cvetinovic, M. M., Petrovic, M. M., Davis, G., Lumicao, M. N., Zivkovic, V. T., Popovic, M. V., and Olmstead, R. Real-time analysis of eeg indexes of alertness, cognition, and memory acquired with a wireless eeg headset. *International Journal of Human-Computer Interaction 17*, 2 (2004).

[6] Berka, C., Levendowski, D. J., Lumicao, M. N., Yau, A., Davis, G., Zivkovic, V. T., Olmstead, R. E., Tremoulet, P. D., and Craven, P. L. Eeg correlates of task engagement and mental workload in vigilance, learning, and memory tasks. *Aviation, space, and environmental medicine 78*, Supplement 1 (2007), B231–B244.

[7] Bnci horizon. http://bnci-horizon-2020.eu/database/data-sets, 2017.

[8] Campbell, A., Choudhury, T., Hu, S., Lu, H., Mukerjee, M. K., Rabbi, M., and Raizada, R. D. Neurophone: brain-mobile phone interface using a wireless eeg headset. In *Proceedings of the second ACM SIGCOMM workshop on Networking, systems, and applications on mobile handhelds* (2010), ACM, pp. 3–8.

[9] Ceballos, N. A., Bauer, L. O., and Houston, R. J. Recent eeg and erp findings in substance abusers. *Clinical EEG and neuroscience 40*, 2 (2009), 122–128.

[10] Čeponienė, R., Westerfield, M., Torki, M., and Townsend, J. Modality-specificity of sensory aging in vision and audition: evidence from event-related potentials. *Brain research 1215* (2008), 53–68.

[11] Chai, X. J., Hirshfeld-Becker, D., Biederman, J., Uchida, M., Doehrmann, O., Leonard, J. A., Salvatore, J., Kenworthy, T., Brown, A., Kagan, E., et al. Altered intrinsic functional brain architecture in children at familial risk of major depression. *Biological psychiatry 80*, 11 (2016), 849–858.

[12] Chizeck, H., and Bonaci, T. Brain-computer interface anonymizer, 2014. US Patent App. 14/174,818.

[13] Chuang, J.-Y., Murray, G. K., Metastasio, A., Segarra, N., Tait, R., Spencer, J., Ziauddeen, H., Dudas, R. B., Fletcher, P. C., and Suckling, J. Brain structural signatures of negative symptoms in depression and schizophrenia. *Frontiers in psychiatry 5* (2014), 116.

[14] Cole, J. H., and Franke, K. Predicting age using neuroimaging: Innovative brain ageing biomarkers. *Trends in neurosciences* (2017).

[15] Doehrmann, O., Ghosh, S. S., Polli, F. E., Reynolds, G. O., Horn, F., Keshavan, A., Triantafyllou, C., Saygin, Z. M., Whitfield-Gabrieli, S., Hofmann, S. G., et al. Predicting

treatment response in social anxiety disorder from functional magnetic resonance imaging. *JAMA psychiatry 70*, 1 (2013), 87–97.

[16] DONCHIN, E. Event-related brain potentials: A tool in the study of human information processing. In *Evoked brain potentials and behavior*. Springer, 1979, pp. 13–88.

[17] Eeg public dataset. https://bit.ly/2Fq68xb, 2017.

[18] Emotiv eeg headset. https://www.emotiv.com, 2017.

[19] ENOCH, M.-A., WHITE, K. V., HARRIS, C. R., ROHRBAUGH, J. W., AND GOLDMAN, D. Alcohol use disorders and anxiety disorders: Relation to the p300 event-related potential. *Alcoholism: Clinical and Experimental Research 25*, 9 (2001), 1293–1300.

[20] ESFAHANI, E. T., AND SUNDARARAJAN, V. Classification of primitive shapes using brain–computer interfaces. *Computer-Aided Design 44*, 10 (2012), 1011–1019.

[21] Facebook has 60 people working on how to read your mind. https://bit.ly/2pUgfQy, 2017.

[22] FINKE, A., LENHARDT, A., AND RITTER, H. The mindgame: a p300-based brain–computer interface game. *Neural Networks 22*, 9 (2009).

[23] FLOR-HENRY, P., LANG, R., KOLES, Z., AND FRENZEL, R. Quantitative eeg studies of pedophilia. *International Journal of Psychophysiology 10*, 3 (1991), 253–258.

[24] FRANK, M., HWU, T., JAIN, S., KNIGHT, R., MARTINOVIC, I., MITTAL, P., PERITO, D., AND SONG, D. Subliminal probing for private information via eeg-based bci devices. *arXiv:1312.6052* (2013).

[25] GILPIN, N. W., AND KOOB, G. F. Neurobiology of alcohol dependence: focus on motivational mechanisms. *Alcohol research & health: the journal of the National Institute on Alcohol Abuse and Alcoholism 31*, 3 (2008), 185.

[26] HARPER, C., AND MATSUMOTO, I. Ethanol and brain damage. *Current opinion in pharmacology 5*, 1 (2005), 73–78.

[27] IENCA, M., AND ANDORNO, R. Towards new human rights in the age of neuroscience and neurotechnology. *Life Sciences, Society and Policy 13*, 1 (2017), 5.

[28] INZLICHT, M., MCGREGOR, I., HIRSH, J. B., AND NASH, K. Neural markers of religious conviction. *Psychological Science 20*, 3 (2009).

[29] JOHNSON, R. R., POPOVIC, D. P., OLMSTEAD, R. E., STIKIC, M., LEVENDOWSKI, D. J., AND BERKA, C. Drowsiness/alertness algorithm development and validation using synchronized eeg and cognitive performance to individualize a generalized model. *Biological psychology 87*, 2 (2011), 241–250.

[30] KARAMZADEH, N., ARDESHIRPOUR, Y., KELLMAN, M., CHOWDHRY, F., ANDERSON, A., CHORLIAN, D., WEGMAN, E., AND GANDJBAKHCHE, A. Relative brain signature: a population-based feature extraction procedure to identify functional biomarkers in the brain of alcoholics. *Brain and behavior 5*, 7 (2015).

[31] KARREMANS, J. C., STROEBE, W., AND CLAUS, J. Beyond vicary's fantasies: The impact of subliminal priming and brand choice. *Journal of Experimental Social Psychology 42*, 6 (2006), 792–798.

[32] KEMNER, C., VERBATEN, M., CUPERUS, J., CAMFFERMAN, G., AND VAN ENGELAND, H. Visual and somatosensory event-related brain potentials in autistic children and three different control groups. *Electroencephalography and Clinical Neurophysiology/Evoked Potentials Section 92*, 3 (1994), 225–237.

[33] KHAN, M. J., AND HONG, K.-S. hybrid eeg–fnirs-based eight-command decoding for bci: application to quadcopter control. *Frontiers in neurorobotics 11* (2017).

[34] MARTINOVIC, I., DAVIES, D., FRANK, M., PERITO, D., ROS, T., AND SONG, D. On the feasibility of side-channel attacks with brain-computer interfaces. In *Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)* (2012), pp. 143–158.

[35] Minddrone. http://emotiv.com/product/minddrone/, 2017.

[36] MORRISON, J. H., AND HOF, P. R. Life and death of neurons in the aging brain. *Science 278*, 5337 (1997), 412–419.

[37] NASEER, N., AND HONG, K.-S. fnirs-based brain-computer interfaces: a review. *Frontiers in human neuroscience 9* (2015), 3.

[38] NEUPANE, A., SAXENA, N., KURUVILLA, K., GEORGESCU, M., AND KANA, R. Neural signatures of user-centered security: An fMRI study of phishing, and malware warnings. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)* (2014), pp. 1–16.

[39] NEUPANE, A.,, RAHMAN M., SAXENA N., HIRSHFIELD L. A Multi-modal Neuro-Physiological Study of Phishing and Malware Warnings. In *ACM Conference on Computer and Communications Security (CCS), Denver, CO* (2015), ACM.

[40] NEUPANE A., SAXENA N., HIRSHFIELD L. An fnirs study of website legitimacy and familiarity detection. In *Proceedings of the 26th International World-Wide Web Conference, in Security and Privacy Track* (2017), WWW.

[41] NEUPANE, AJAYA, LUTFOR, MD. RAHMAN, AND SAXENA, NITESH. Peep: Passively eavesdropping private input via brainwave signals. In *Proceedings of the Financial Cryptography (FC)* (2017), pp. 1–19.

[42] Neuralink is developing ultra high bandwidth brain-machine interfaces to connect humans and computers. https://www.neuralink.com, 2017.

[43] Neurofocus. https://bit.ly/2dZbIe5, 2017.

[44] Neurosky eeg headset. https://www.neurosky.com, 2017.

[45] Neuroskye. https://bit.ly/31QLP5k, 2017.

[46] Re-engineering brains. https://bit.ly/2IXOGAY, 2012.

[47] Node-neurosky. https://www.npmjs.com/package/node-neurosky, 2017.

[48] NOMENCLATURE, S. E. P. American electroencephalographic society guidelines for. *Journal of clinical Neurophysiology 8*, 2 (1991).

[49] OSCAR–BERMAN, M., AND MARINKOVIC, K. Alcoholism and the brain: An overview, 2014.

[50] PORJESZ, B., AND BEGLEITER, H. Alcoholism and human electrophysiology.

[51] RANGASWAMY, M., AND PORJESZ, B. Understanding alcohol use disorders with neuroelectrophysiology. *Handbook of clinical neurology 125* (2014), 383.

[52] The stigma of alcoholism. https://bit.ly/2Y0z9GS, 2015.

[53] RIDDLE, D. R. *Brain aging: models, methods, and mechanisms*. CRC Press, 2007.

[54] Sccn ucsd. https://bit.ly/2Fqs771, 2017.

[55] SHANNON, B. J., RAICHLE, M. E., SNYDER, A. Z., FAIR, D. A., MILLS, K. L., ZHANG, D., BACHE, K., CALHOUN, V. D., NIGG, J. T., NAGEL, B. J., ET AL. Premotor functional connectivity predicts impulsivity in juvenile offenders. *Proceedings of the National Academy of Sciences 108*, 27 (2011), 11241–11245.

[56] SNODGRASS, J. G., AND VANDERWART, M. A standardized set of 260 pictures: Norms for name agreement, image agreement, familiarity, and visual complexity. *Journal of Experimental Psychology: Human Learning and Memory 6* (1980), 174–215.

[57] B-alert x-series eeg systems. https://bit.ly/1FeBt0N, 2012.

[58] TAN, D., AND NIJHOLT, A. Brain-computer interfaces and human-computer interaction. In *Brain-Computer Interfaces*. Springer, 2010.

[59] TCHESLAVSKI, G. V., AND GONEN, F. F. Alcoholism-related alterations in spectrum, coherence, and phase synchrony of topical electroencephalogram. *Computers in biology and medicine 42*, 4 (2012).

[60] Can you sue your employer if you're fired for being an alcoholic? https://bit.ly/2Fo6ioI, 2015.

[61] WAISMANN, R., FENWICK, P. B., WILSON, G. D., HEWETT, T. D., AND LUMSDEN, J. Eeg responses to visual erotic stimuli in men with normal and paraphilic interests. *Archives of sexual behavior 32*, 2 (2003), 135–144.

[62] Which api is right for me? https://bit.ly/2XmwGJS, 2017.

[63] YUAN, B. J., HSIEH, C.-H., AND CHANG, C.-C. National technology foresight research: a literature review from 1984 to 2005. *International Journal of Foresight and Innovation Policy 6*, 1-3 (2010), 5–35.

[64] ZHANG, X., YAO, L., KANHERE, S. S., LIU, Y., GU, T., AND CHEN, K. Mindid: Person identification from brain waves through attention-based recurrent neural network. *arXiv:1711.06149* (2017).

[65] ZHANG, X. L., BEGLEITER, H., PORJESZ, B., WANG, W., AND LITKE, A. Event related potentials during object recognition tasks. *Brain Research Bulletin 38* (1995), 531–538.