EVALUATING THE USABILITY OF PASSTHOUGHT AUTHENTICATION

by

Joshua K Carr

A thesis submitted to the Faculty of Graduate and Post Doctoral Affairs
in partial fulfillment of the requirements for the degree of

Master of Applied Science in Human-Computer Interaction

at

Carleton University
Ottawa, Canada
September 2020

Table of Contents

List of Tables . . . . . **v**

List of Figures . . . . . **vii**

Abstract . . . . . **ix**

Acknowledgements . . . . . **x**

Chapter 1 Introduction **1**

1.1 Usability of Passwords 1

1.2 Password Alternatives 3

1.3 Passthoughts: Brain-based Authentication 6

1.4 Contributions 8

Chapter 2 Literature Review **11**

2.1 Introduction: What is a BCI? 11

2.2 Invasive BCIs 13

2.3 EEG-based BCIs 17

2.4 fNIRS-based BCIs 19

2.5 Other BCI Modalities 21

2.6 BCI Applications 24

2.7 BCIs for Authentication 26

2.8 Barriers to BCI Adoption 29
2.8.1 Acceptance of BCIs among persons with disabilities. 30
2.8.2 Concerns about security and privacy. 32

Chapter 3 Mental Command Graphical Password System . . . **35**

3.1 Motivation 35

3.2 System Requirements 36

3.3 Design 39

3.4 Implementation . . . 44
3.4.1 General architecture and system overview. . . . 44
3.4.2 Command training and input. . . . 49
3.4.3 Cortex API. . . . 52
3.4.4 Grid interface. . . . 53
3.4.5 Using the application. . . . 56

3.5 System Evaluation . . . 58
3.5.1 Feasibility Study Design . . . 59
3.5.2 Pilot and Obstacles . . . 63
3.5.3 Outcome . . . 68
3.5.4 Future Directions . . . 69

Chapter 4 Brain-Computer Interface Expert Interview Study 72

4.1 Background . . . 72

4.2 Methods . . . 74
4.2.1 Participants and Recruitment . . . 74
4.2.2 Interview Guide . . . 75
4.2.3 Procedure . . . 78
4.2.4 Analysis . . . 79

4.3 Results . . . 80
4.3.1 Safety . . . 82
4.3.2 Usability . . . 89
4.3.3 Development . . . 93

4.4 Interpretation . . . 97
4.4.1 Limitations . . . 99
4.4.2 Conclusion . . . 100

Chapter 5 Mechanical Turk BCI Questionnaire Study . . . 101

5.1 Introduction and Background . . . 101

5.2 Methods . . . 102
5.2.1 Instruments . . . 102
5.2.2 Participants and Recruitment . . . 109
5.2.3 Data Analysis . . . 110

5.3 Results . . . 112
5.3.1 Descriptive Statistics . . . 112
5.3.2 Hypothesis Tests . . . 120

5.4 Interpretation . . . 127

5.4.1 Summary . . . 127
5.4.2 Limitations . . . 130
5.4.3 Conclusion . . . 131

Chapter 6 Conclusions . . . 134

6.1 Summary . . . 134
6.1.1 Timeline of Studies . . . 135

6.2 Contributions . . . 136

6.3 Limitations . . . 138

6.4 Future Work . . . 140

6.5 Final Thoughts . . . 141

Appendices . . . 168

Appendix A Research Ethics Approval . . . 169

A.1 Authentication System Usability Study . . . 169

A.2 Interview Study . . . 178

A.3 MTurk Questionnaire Study . . . 185

Appendix B R Code . . . 193

B.1 Data Validation and Pre-Processing Script . . . 193

B.2 Data Analysis and Hypothesis Testing Script . . . 195

List of Tables

4.1 The finalized interview guide with 24 question items grouped into five topics. 76

4.2 Frequency table showing the number of interviewees who reported having experience using each of several commercially-available BCI devices. 80

4.3 The unsorted list of codes generated from three iterations of the code generation procedure described in Section 4.2.4. . . 81

4.4 The structure of the *Safety* meta-theme, including its three sub-themes and their respective codes. 83

4.5 The structure of the *Usability* meta-theme, including its two sub-themes and their respective codes. 89

4.6 The structure of the *Development* meta-theme, including its three sub-themes and their respective codes. 94

5.1 The final items used for the modified Comfort Rating Scale used in this study. Reversed items are used for response validation. 104

5.2 Survey items for the BCI Acceptance Scale (BAS) grouped by subscales. 106

5.3 Possible answers to BAS item 17_b ("What sort of information might they be able to learn (select all that apply)?"). 107

5.4 Frequency table of levels of education for the sample. 113

5.5 Descriptive statistics for the subscales of the TIPI. 114

5.6 Descriptive statistics of the subscales of the SeBIS. 117

5.7 Descriptive statistics of the six dimensions measured by the CRS. 117

5.8 Descriptive statistics for the four subscales of the BIS. 117

5.9 Frequency table of the responses to the BIS:Security item "A hacker could use data intercepted from a BCI device to infer private information about the user." 120

5.10 Frequency table of the responses to the followup question "What sort of information might they be able to learn (select all that apply)?" 120

5.11 Results and p-values of Spearman correlation tests and Wilcoxon rank sum test for the SeBIS hypotheses. 121

5.12 Results and p-values of Spearman correlation tests and Wilcoxon rank sum test for the TIPI hypotheses. 123

5.13 Summary of the results of the hypothesis tests indicating whether they were supported by the collected data. 127

List of Figures

1.1 Bonneau et al.[1]'s comparison of text passwords and various alternatives 4

2.1 Images of invasive BCI sensors (sEEG, ECoG, and PMA). . 14

2.2 A comparison of a typical MEG system with a more usable version. 22

2.3 An example of an fMRI scan of a human brain. 23

2.4 An example of a grid speller interface. 25

2.5 Reconstruction of a participant's visual field using fMRI data from Shen et al.[162] 34

3.1 Design sketches from the planning phase of application development. 39

3.2 Design sketches from the planning phase of application development. 40

3.3 The default Android touchscreen pattern lock screen (left) and a different implementation of the same system (right). Reproduced from Colley et al.[169]. 42

3.4 A comparison of the Epoc and Insight BCI devices from Emotiv.[57] 44

3.5 The contact quality page of the Cortex application for the Emotiv Epoc.[57] 45

3.6 The training profile interface of the EmotivBCI[57] application. 46

3.7 A schematic diagram of the authentication application showing relations between the major server-side and client-side components. 48

3.8 Command training interface of the EmotivBCI[57] application. 50

3.9 The main manu and password creation interface of the authenticator prototype. 54

3.10 A walkthrough of the usage of the application, including the initial setup and training of a mental command profile in EmotivBCI.[171] 57

3.11 The mental rotation task interface.[181] 62

5.1 The images of the Emotiv Insight[57] that were shown to participants before the CRS and BAS scales. 103

5.2 Distribution of ages and completion times for the survey sample. 113

5.3 Histogram of levels of education for the sample. 114

5.4 Histograms of the Big 5 personality dimensions for the sample. 115

5.5 Histograms of the four subscales of the SeBIS. 116

5.6 Histograms of the six comfort dimensions assessed by the CRS. 118

5.7 Histograms of the four subscales assessed using the BAS. . . 119

5.8 Pairwise scatterplots for the SeBIS hypotheses. 122

5.9 Pairwise scatterplots for the first four TIPI hypotheses. . . . 124

5.10 Pairwise scatterplots for the last four TIPI hypotheses. . . . 125

Abstract

Traditional passwords have numerous problems, but so far no alternative system has been able to replace them. Authentication using brain-computer interfaces (BCIs), or *passthoughts*, has been proposed as an alternative because of the unique biometric properties of neurophysiological data, but significant questions remain regarding usability and practicality. In this thesis I explore issues related to the usability of BCIs and passthoughts. I designed and built a prototype passthought authenticator, which revealed significant usability issues surrounding the use of mental commands. By interviewing expert BCI users and researchers, I identified barriers relating to perceived safety, usability, and applicability of BCIs. A survey of MTurk workers with no prior BCI experience revealed that personality characteristics as well as security behaviours were related to respondents' acceptance and perceived usability of BCIs. These studies revealed significant barriers and areas for improvement of passthoughts and BCIs in general.

Acknowledgements

This thesis would not have been possible without the support and mentorship of Dr. Robert Biddle. Thank you for everything.

Thank you to my Mom and Jake for always believing in me.

And thank you Alëna for your constant inspiration and support. I couldn't have done this without you.

Chapter 1

Introduction

Passwords are a ubiquitous feature of modern life, but are known to have significant shortcomings which impact their usability as an authentication mechanism. Brain-computer interfaces (BCIs) have been suggested for their potential to enable novel forms of authentication which may address these problems. However, the proposed approaches are not without limitations and have received comparatively little scrutiny relative to other password-alternatives. In this thesis I consider these limitations and propose a new approach for BCI authentication based on mental commands and graphical passwords.

1.1 Usability of Passwords

Virtually all online accounts and personal devices are secured behind some form of password, passphrase, or PIN. Even in situations when other methods are available, such as fingerprint scanners emerging on many current-generation smartphones, a password or PIN is generally still required as a backup authentication system in the event that the primary method fails. The situation with passwords is perhaps best summarized by Bonneau et al. [1] in the opening of their 2012 paper on alternative authentication systems:

> "The continued domination of passwords over all other methods of end-user authentication is a major embarrassment to security researchers. As web technology moves ahead by leaps and bounds in other areas, passwords stubbornly survive and reproduce with every new web site.

> Extensive discussions of alternative authentication schemes have produced no definitive answers." — Bonneau et al. [1]

When used correctly, passwords are not a terrible authentication system *per se*, but a significant usability burden impairs their robustness as an authentication scheme. The only major inherent weakness of passwords is their vulnerability to capture, which can be accomplished through in-person observation or using a camera (called *shoulder-surfing*), or a software key-logger installed on the system. However, passwords have poor security in the real world due to poor usability which encourages users to develop compensatory behaviours to circumvent the system requirements. The most significant user behaviour issues with password authentication are the use of predictable sequences, reuse of passwords across multiple accounts, and the tendency of users to write their passwords down in a form that they can be stolen.

In order for passwords to be secure against dictionary-based guessing attacks, they must contain sufficient entropy to ensure a large password space. This can be accomplished in a number of ways, such as increasing the length of the password and combining upper and lower-case letters with numbers, punctuation, and other symbols. Strong passwords should also avoid common patterns and dictionary words because these are susceptible to automated guessing attacks.[2] Password expiration is a common tool intended to improve password security by forcing the user to change their password at regular intervals, but empirical investigations have found that the security advantage of these policies is marginal at best and associated with a significant usability cost.[3] Given these requirements for password security and the fact that individuals are now maintaining an increasing number of online accounts,[4,5] the burden of memorizing a different long, unpronounceable, and frequently-changing password for each account is very apparent.

1.2 Password Alternatives

A number of alternatives have been proposed and tested with the hope of providing a replacement for text passwords as the *de facto* standard for authentication. Bonneau et al. [1]'s 2012 review comparing different authentication schemes remains the most comprehensive treatment of this topic, and demonstrates both the reason for the continued dominance of passwords and the key areas on which other methods perform poorly. Bonneau et al. [1] propose a scheme to evaluate and contrast authentication systems based on three overarching criteria: *security* (whether the system is resilient to attacks of different types), *usability* (the *ease-of-use* of the system on the part of the end-user), and *deployability* (the scalability and *ease-of-implementation* of the system on the part of the system owner/administrator).

Bonneau et al. [1] conducted a comparative analysis using their evaluation framework for text passwords (or *legacy passwords*) and various alternative systems including graphical passwords, hardware tokens, biometrics, and others. A summary of the breakdown of authentication systems across three dimensions (usability, deployability, and security) is reproduced here in Figure 1.1. Notably, text passwords have relatively poor usability and security characteristics, but excel in deployability wherein they meet all criteria. Overall, some systems excel in usability (e.g., federated authentication, biometrics), and others in security (e.g., hardware tokens), however none meet the majority of both usability and security criteria, and none demonstrate deployability comparable to text passwords. Thus, it seems that no one scheme stands out as an obvious candidate to replace text passwords.

Biometric authentication has been widely examined for its potential to replace text passwords, and is one of the methods that has seen the greatest adoption by the public. A 2018 review by Rui and Yan [6] covers a number of biometric authentication systems including those based on fingerprints, iris, voice, cardiac

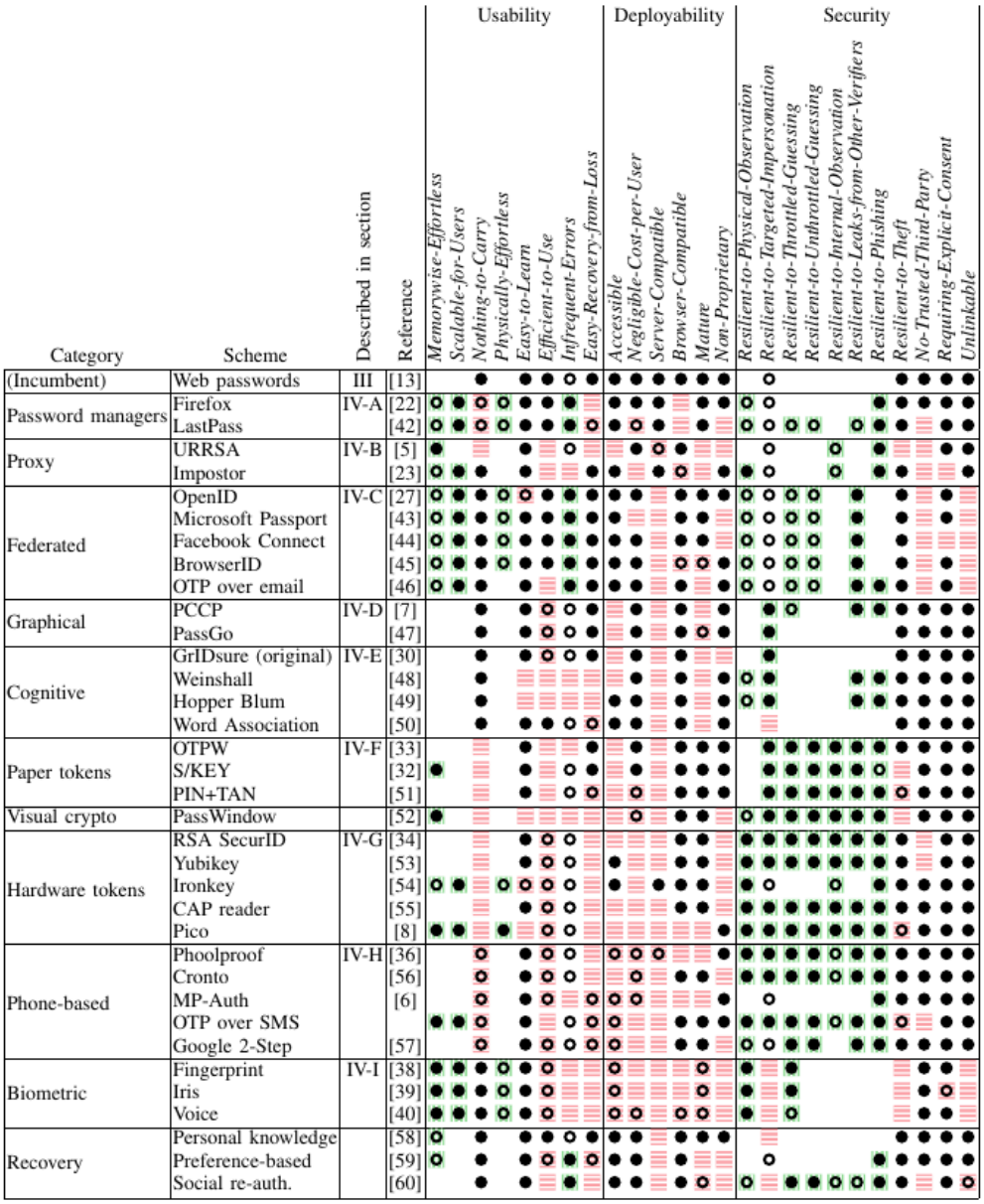

Figure 1.1: A comparison of text passwords and various proposed alternative authentication systems according to the criteria of usability, deployability, and security. Reproduced from Bonneau et al. [1].

rhythm, and keystroke dynamics. Broadly, the review identifies that all of the methods studied were seriously flawed. For example, iris-based authentication demonstrates high security but poor usability, whereas fingerprint authentication is very to easy to use but has poor security due to the ease with which fingerprints can be copied from essentially any surface that a victim has touched.

According to Rui and Yan [6], one of the most significant threats to biometric authentication is a *replay* attack or *spoofing* attack, wherein an attacker compromises biometric authentication by acquiring an image or *copy* of the biometric feature of interest and *replaying* it to the authentication system in order to falsely authenticate as the victim. For example, a scan of a victim's iris could be used to fool an iris-based authentication system.[7] A related difficulty with biometrics is related to *changeability* (or *cancelability*), because biometric features like fingerprints or irises are difficult—if not impossible—to change in the event of compromise.[8] For these reasons text passwords remain as a backup authentication method even in contexts where biometrics are deployed.

Multi-factor authentication (*MFA*) is another approach for improving the security of password authentication that has been studied extensively and has been widely implemented in the last several years. The basic principle of MFA is to augment a primary *authentication factor* (usually text passwords) with a second factor such that there is no longer a single point of failure.[9] In essence, the user is asked to log-in using a combination of different methods; the consensus of multiple authentication factors strengthens the conclusion that the user's identity is genuine. Authentication factors are generally classified into one of three categories: a *knowledge* factor (something you **know** such as a secret text password), a *possession* factor (something you **have**, a physical token like a mobile phone or USB key), or an *inherent* factor (something you **are**, such as a unique fingerprint, cardiac rhythm, or facial geometry). A strong MFA system will use multiple factors

from at least two of these categories. For example, after entering a username and password as normal, a user may be asked to enter a code sent via push notification to their mobile phone; thus the user must demonstrate *knowledge* of the correct account credentials, as well as *possession* of the mobile phone associated with the account in order to successfully authenticate and gain access to the account.

While MFA undoubtedly improves security, a number of studies and reviews have come to the general consensus that usability of MFA is poor, and the process overburdens users.[10–13] For example, Krol et al. [11] studied the use of MFA in online banking, finding that users view MFA as cumbersome, prone to mistakes, and getting in the way of their primary task. Das et al. [13] conducted an analysis of user comments for MFA applications on major mobile app stores (Google, Apple, and Amazon) in order to determine general sentiments around MFA as well as specific issues preventing acceptance and adoption. Some themes were identified, including issues with setup, integration and compatibility with other applications and systems, backups, and being *forced* to use MFA by one's workplace or educational institution. The findings of Das et al. [13] support the notion that public perception of MFA is not particularly positive, and users are not willing to accept or adopt it without some form of enforcement.

1.3 Passthoughts: Brain-based Authentication

An interesting possibility for authentication was proposed by Thorpe, van Oorschot, and Somayaji[14] in 2005, termed *passthoughts*. Passthoughts involve using a brain-computer interface (BCI) to record the activity of the user's brain while they engage in a specific mental task (the *passthought*); the recorded brain activity is compared against a known genuine example in order to validate the identity of the user. The mental task or passthought itself is a knowledge-based authentication factor, but there is a biometric component as well because of the

unique way in which a given thought is expressed between individuals at the level of neuronal activity. Constructed in this way, passthoughts enable two-factor authentication which nonetheless requires only a single step on the part of the user, essentially sidestepping the significant usability burden normally associated with MFA. In recent years this paradigm has been extended to include three authentication factors by treating the BCI device itself as a physical authentication token.[15]

In addition to the potential for single-step MFA, passthoughts provide several other benefits:[14] unlike other biometrics, they are *cancelable* or *changeable*, meaning that they can be revoked or changed in the event of a data breach; depending on the implementation, passthoughts can be immune to observation or *shoulder-surfing* attacks that are problematic for text passwords and many other knowledge-based authentication systems; and passthoughts are accessible for individuals with severe impairments that prevent them from being able to use other authentication methods such as locked-in syndrome or advanced amyotrophic lateral sclerosis (ALS). This last point is especially relevant because individuals with severe impairments of communication or motor ability are one of the most important user groups for BCIs in general.

Despite these factors, there remain unanswered questions regarding the public acceptance and adoption of passthoughts. It is generally understood that usability is a critical component of security systems, and that poor usability is itself a security vulnerability.[16] This is often framed as a trade-off, where increasing the level of security tends to decrease the system's usability.[17] The usability of passthoughts has only been seriously investigated in a few studies,[18–20] and without a definitive answer to the questions of whether passthoughts could be usable for daily life, under what circumstances, and for whom. The usability of BCIs in general has

been more thoroughly addressed, leading to the identification of several significant usability barriers, which is concerning for the case of passthoughts.

The aim of the present work is to explore these and other issues related to the practicality and usability of passthought authentication. The remainder of this thesis is organized as follows: Chapter 2 will introduce the reader to brain-computer interfaces through a review of related work, leading into a discussion about BCI-based authentication and its merits. Chapter 3 presents a novel approach to BCI authentication that combines BCI mental commands with graphical passwords. I describe a prototype system following this approach that I built for usability testing, as well as outlining an evaluation study to test the prototype which was unsuccessful due to complications with using mental commands. Chapters 4 and 5 describe my attempts to reveal and understand factors related to acceptance and adoption of BCIs and BCI-based authentication through qualitative semi-structured interviews with BCI experts (Ch. 4) and a quantitative survey of BCI-naïve MTurk[21] workers (Ch. 5). Chapter 6 summarizes previous chapters and provides some closing remarks before concluding the thesis.

1.4 Contributions

Chapter 3 describes my design and implementation of a novel type of prototype passthought authentication system based on BCI mental commands and graphical passwords. Passthought systems based on mental commands have not previously been reported in the research literature to my knowledge. Attempts to conduct usability testing with the prototype were initially stalled due to difficulty and unreliability of training a mental command classifier, and later suspended indefinitely due to closure of the University due to COVID-19.

Despite failed attempts to conduct usability testing, a few valuable lessons were learned about the implementation of passthought authentication based on mental

commands. In general, it appears that the amount of time and effort required to achieve reliable detection and discrimination of four mental commands, if it is possible at all, would be far too onerous to justify their use for the purpose of authentication only. It is possible that a system requiring fewer commands (i.e., two or three) would be more feasible. Alternatively, the burden of mental command training might be offset if the same set of commands could be used for a more general set of tasks beyond just authentication.

I conducted semi-structured interviews with BCI experts, described in Chapter 4, intended to identify barriers related to the acceptance and potential adoption of BCIs and passthought authentication. Thematic analysis of the interview data revealed several barriers which were encapsulated by three general themes: the perceived safety of BCI devices, their usability (including difficulty as well as physical and psychosocial comfort), and a need for further development of BCI technologies and applications to make BCI usage more worthwhile. The role of uncertainty and lack of knowledge about the brain was a common feature of all three themes. A significant implication for passthoughts is that passthought systems can only be as usable as the BCI systems they use. In spite of these significant limitations, interviewees generally indicated that they believed BCIs would become significantly more prevalent in the future.

Finally, Chapter 5 describes an online survey of Amazon Mechanical Turk workers aimed at identifying factors related to perceptions of and attitudes toward BCIs among a general population sample which no prior experience with BCIs. The survey assessed Big 5 personality dimensions, security-related behaviours, perceived comfort of a BCI device, and beliefs and views about BCIs in general.

Despite generally reporting very little prior knowledge about BCIs, survey respondents were significantly concerned about the security of BCI devices, strongly endorsed the need for increased consumer protection regulation concerning BCI

devices, and thought it at least somewhat likely that BCI devices would become common or mainstream in the future. Correlational analysis of the subscale scores for the four instruments revealed some intuitive relationships. For example, those who scored highly on the *Emotional Stability* Big 5 dimension were more likely to report a positive evaluation of the appearance of a BCI device and less likely to report that wearing the device would cause anxiety; the same pattern was observed for those high in *Openness to Experience.*

Chapter 2

Literature Review

This chapter is intended as a general introduction to the topic of brain-computer interfaces (BCIs) and BCI-based authentication (also called *passthoughts*). The chapter is organized as follows: Section 2.1 discusses the general principles and components that are common to all BCI schemes. Sections 2.2—2.5 cover different types of invasive and non-invasive BCIs. Section 2.6 covers various applications and implementations of BCI systems, and Section 2.7 will explore the case of BCI authentication in greater detail. Finally, Section 2.8 discusses obstacles and barriers preventing more widespread adoption of BCIs and BCI authentication by the public.

2.1 Introduction: What is a BCI?

Any technology that can image or record electrophysiological activity of the brain has potential to be used as a BCI, though there are significant limitations to each method which affect the device's capability, usability, or applicable use-cases. BCIs may also include devices which directly affect the brain, such as deep-brain stimulators used to attenuate motor symptoms in Parkinson's disease, cochlear implants, as well as transcranial electrical/magnetic/direct-current stimulators (tES/tMS/tDCS).

Brain-computer interfaces can broadly be divided into three categories based on their level of invasiveness, i.e., invasive, partially-invasive, and non-invasive. The distinction between invasive and partially-invasive BCIs relates to whether

the device is implanted into neural tissue. Invasive BCIs are implanted *into* the brain, whereas partially-invasive BCIs are implanted below the skull but outside of the brain. There is a general trend that more invasive BCIs generate better data for BCI use due to increased signal quality and the ability to access signals from deeper structures of the brain.

Invasive and partially-invasive BCIs have demonstrated impressive capabilities, such as precisely controlling a robotic prosthetic arm,[22,23] or piloting a flying drone through targets in three-dimensional space.[24] Current non-invasive BCI implementations do not approach this level of control. This suggests that there is substantial room for improvement with non-invasive BCIs; as new methods of non-invasive neuroimaging are developed and existing methods are refined and improved, it is possible that BCI capabilities that are currently exclusive to invasive and partially-invasive methods may become achievable with non-invasive ones.

In 2006, Pfurtscheller, Graimann, and Neuper [25] proposed a framework for BCI systems comprises five steps that form a closed loop:

1. Signal acquisition: the physiological activity of the brain must be recorded, for example using electroencephalography (EEG), electrocorticography (ECoG; also called intracranial EEG), or functional near-infrared spectroscopy (fNIRS).

2. Preprocessing: The signal must be processed into a form which is useful for further analysis. For EEG, this means filtering out 50/60 hz ambient electrical noise as well as applying various other band-pass filters to isolate the frequency spectra of interest.

3. Feature Extraction: The system must identify features of the signal that correspond to the user's intent and distinguish these from non-task-related

activity. In the case of EEG, it is common to apply a Fourier transform to extract band power in the frequency spectra of interest (e.g., alpha, beta, delta).

4. Classification: The extracted features are fed into a classification algorithm which attempts to estimate the user's intent. Various machine learning approaches have been used for this step with varying success. There is a great deal of room for improvement in this step as the fields of artificial intelligence and machine learning continue to advance.

5. Application: The user's intended action is executed in the hardware or software application.

Pfurtscheller, Graimann, and Neuper[25]'s framework was meant to apply to EEG-based BCIs, however, the same structure has been adopted for BCIs based on other technologies such as functional near-infrared spectroscopy (fNIRS).[26]

2.2 Invasive BCIs

Invasive BCIs are those that require surgical implantation. Three methods of invasive neuroimaging are typically used for BCIs, reviewed in detail by Ajiboye and Kirsch[27]: stereoencephalography (sEEG), electrocorticography (ECoG), and penetrating microelectrode arrays (PMAs). sEEG uses long, thin electrodes that have multiple sensor contacts along their length, which are implanted through holes drilled in the skull in various locations according to their intended application. sEEG is advantageous in that it can be used to record signals from virtually any location within the brain, including deeper subcortical structures that are difficult to access with other methods. ECoG uses flat sheet-like grids or strips of microelectrode sensors which are implanted below the skull but outside of the brain.

While it is not particularly suitable for accessing deeper structures, ECoG is able to cover a broader region of the cortical surface. PMAs are made of up a series of small wires or shafts attached to a flat surface which penetrate 1–1.5 mm into the surface of the brain. PMAs record signals from only a small region of the cortical surface but allow for the collection of very detailed information, including single action potentials of individuals neurons.

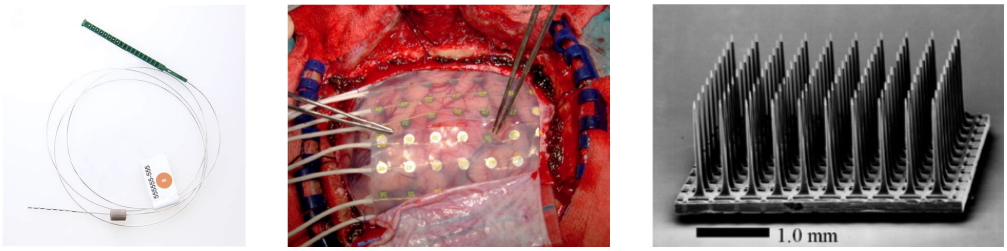

Figure 2.1: *Left:* An intracranial electrode used for stereoencephalography (sEEG). Reproduced from Renishaw Plc.[28] *Middle:* A subdural electrode array on the surface of the brain being used to conduct electrocorticography (ECoG), from Amaral et al.[29]. *Right:* A penetrating microelectrode array (PMA) developed by Blackrock Microsystems.[30]

Many authors have drawn a distinction between invasive BCIs which are surgically implanted into the brain and so-called *partially-invasive* BCIs which require surgical implantation but do not penetrate the tissue of the brain. However, it is worth noting that invasive can also be viewed in terms of the severity of the surgical procedure, rather than whether the implanted sensors penetrate the brain. For example, ECoG is typically considered a partially invasive technique[27] because the sensors are placed below the skull but outside of the brain, while sEEG is considered invasive because electrodes are inserted into brain tissue. However, as noted in Ajiboye and Kirsch[27], the surgical procedure for ECoG involves removing large sections of the skull and can therefore be seen as more invasive than the implantation process for sEEG, in which electrodes are inserted through small holes drilled

through the skull. For the remainder of this review I will not make a distinction between invasive and partially-invasive neuroimaging methods and will consider any technique requiring surgery to be invasive.

Invasive BCIs carry significant risk. In addition to the risks normally associated with any surgery, there is the possibility of unintended damage to the brain during implantation as well as glial scarring which can occur in the long term.[27] Further, implanted sensors can degrade over time,[27] and can only be repaired or replaced by undergoing additional invasive surgery. For these reasons, research into invasive BCIs in humans is relatively sparse and limited to conditions in which a patient is undergoing an invasive neuroimaging procedure due to medical necessity and volunteers to participate in a BCI study. This presents an additional difficulty for research because the number, type, and locations of sensors for these patients is heterogenous and based on the specific aims of the procedure with respect to their condition.

However, invasive methods offer distinct advantages over non-invasive ones for BCI use. They can achieve very high resolution in both spatial and temporal domains; for example, using PMAs it is possible to record single action potentials of individual neurons[27] which have been shown to encode movement related information and are therefore a valuable control signal for motor-based BCIs. Invasive methods can achieve a better signal-to-noise ratio than non-invasive[27] ones and can record a wider spectrum of electrical activity due to the lack of obstruction by the skull.

The capabilities of invasive BCIs can be life-changing for individuals with severe impairments. One of the first major successes of invasive BCIs was the cochlear implant first patented in 1986,[31] which can restore hearing by delivering electrical stimulation directly to the cochlea. Spinal cord injury (SCI), amyotrophic lateral sclerosis (ALS), and traumatic brain injury (TBI) are conditions

which often lead to significant loss of mobility or communication, and restoring function for individuals with these conditions is one of the most significant and well-studied use-cases for invasive BCIs.

A number of studies have demonstrated the ability for invasive BCI methods to allow a user to control the position of a cursor in one,[32] two,[33–36] or three-dimensional space,[24,37] suggesting the possibility of computer use for individuals with limited mobility. Possibilities for communication include high-performance *speller* applications (as in Figure2.4)[38,39] or, more elaborately, directly decoding imagined syllables and translating them into text or synthesized speech.[40,41]

In terms of physical mobility, invasive BCIs have been used to control robotic external prosthetic devices (*neuroprosthetics*),[22,23,42] or a full exoskeleton.[43] In a landmark achievement, Hochberg et al.[22] developed a BCI system based on implanted microelectrode arrays that enabled a patient with tetraplegia to drink coffee from a bottle using a robotic arm. Many individuals with motor impairments due to disease or injury nonetheless have functional musculature remaining in their impaired limbs which can be controlled to create movement by the application of electrical currents, a practice called *functional electrical stimulation* (FES).[44] An extension to the neuroprosthetic approach is to use to stimulate a patient's impaired limbs based on signals recorded from a BCI.[45,46] Although it is not applicable in all cases, BCI-based FES blurs the distinction between prosthesis and rehabilitation and offers a more naturalistic restoration of function without the social and technological complexities of a robotic prosthetic.

Overall, there are compelling capabilities of invasive BCIs which may outweigh their significant risks by restoring lost function to people with severe impairments. However, the capabilities of invasive BCIs are important for the study of non-invasive BCIs as well, as the process of reading brain signals and interpreting them to control a system is fundamentally the same in both cases. The performance

improvement of invasive BCIs over non-invasive ones is primarily due to their better spatial resolution, signal-to-noise ratio, and access to deeper structures of the brain, all of which could conceivably be achieved through further refinement of existing non-invasive methods such as EEG or MEG (discussed in Section 2.5). Therefore it is not unreasonable to expect that future non-invasive BCIs will at some point achieve performance that is currently only possible with invasive ones.

2.3 EEG-based BCIs

By far the most prevalent technology used for non-invasive BCIs is electroencephalography (EEG). First demonstrated on humans in 1924,[47] EEG has been widely as a medical diagnostic tool. The use of EEG signals to interact with a computer system was first proposed by Vidal [48] in 1973, credited as the origin of the term *brain-computer interface*. A series of experiments over the subsequent decades gradually advanced the state of the art of EEG-based BCIs and demonstrated impressive capabilities using medical-grade EEG systems.[49–53] A review by Wolpaw [54] summarized the work on BCIs and the state of the field in 2007. One of the most significant developments in EEG-based BCIs over the last decade has been the emergence of of low-cost consumer-oriented EEG-BCI devices aimed at a variety of BCI applications.[55–58] EEG has several advantages over other methods that make it a suitable input for BCI use:

1. Safety: EEG has been extensively studied by neurophysiology researchers and used as a basic diagnostic tool in medical practice for many decades and has not been associated with any negative side-effects.

2. Portability: recent advances in EEG hardware have enabled the development of highly portable systems. All of the components required for a functional

EEG setup can be comfortably fit into a simple head-worn device, and modern smartphones and laptops are sufficiently powerful to process EEG data in real time for BCI applications.

3. Low cost: As EEG technology has been refined over many decades, the cost has decreased dramatically. Several consumer-facing EEG devices have been developed which retail for less than one thousand dollars (e.g., Emotiv[57] and Muse[56] devices, some of the OpenBCI[58] kits). The accessibility of EEG setups are further increased by the rise of low-cost 3D printing which can enable researchers or BCI enthusiasts to build their own BCIs out of standard electrical components and 3D-printed parts. For example, OpenBCI[58] uses this 3D printing approach extensively, allowing customers to save a substantial portion of the cost of a BCI device by printing many of the non-electrical components themselves.

4. High temporal resolution: The electrical potential fluctuations generated by the firing of neurons occurs imperceptibly fast, and modern EEGs are capable of sampling at rates well over 1000 Hz, allowing EEG to resolve activity on the order of milliseconds.

While the advantages of EEG are significant, it is not without limitations. The electrical fluctuations measured by EEG are very small and can easily be drowned out by electrical interference, body movements, or contamination from other physiological signals such as the heartbeat or muscular activity. EEG signals must pass through the skull before they can be detected from the surface of the scalp which degrades the signal substantially; frequencies in the gamma range (30-200 Hz) are particularly susceptible to this. EEG suffers from low spatial resolution because, even with many electrodes, each electrode measures the activity of many tens of thousands of neurons, making it difficult to establish from *where* any

particular waveform originates. Compounding this is the fact that EEG signals are spatially correlated (i.e., a given electrode's signal *overlaps* with that of other nearby electrodes), requiring sophisticated signal processing techniques to isolate the unique signal of each electrode. EEG is limited to recording activity of neuron populations near the surface of the brain and is not practical for measuring activity of internal structures that might be of interest for BCIs.

2.4 fNIRS-based BCIs

Near-infrared spectroscopy (NIRS) is a relatively new method of neuroimaging that has been investigated as an input for non-invasive BCI systems.[26] NIRS is a non-invasive optical imaging method that uses light in the near-infrared spectrum passed through biological tissues to detect and quantify the presence of various molecular targets (e.g., hemoglobin) based on their spectral absorption properties.[26] Functional NIRS or fNIRS refers the use of NIRS for functional neuroimaging by measuring changes in oxygenated and deoxygenated hemoglobin in specific areas of the cortex (called the *blood oxygen level dependent* or BOLD signal), which can be used to infer relative levels of neuronal activity in those regions based on the principle that more active neurons have an increased metabolic demand for oxygen.[59]

Near-infrared light (with a wavelength between 700 and 1000 nm) does not interact with bone, and can therefore pass through the skull unimpeded, but is absorbed differentially by different types of biological tissue based on its wavelength.[60] fNIRS imaging involves emitters and detectors placed on the surface of the scalp. NIR photons of varying wavelengths are emitted into the brain, which scatter as they interact with brain tissues. Some of these scattered photons are captured by the detectors, and the intensity of the captured versus the emitted

photons can be compared to determine changes in the ratio of oxy- and deoxy-hemoglobin in the path of the emitter.[26] The position of the emitter on the scalp determines the location on the cortex that is measured, and the distance and positioning of the detectors relative to the emitter determine the depth from which the measurements are taken.[26] The wavelengths of the emitted photons are selected based on the absorption coefficients of the molecules of interest (typically oxy- and deoxy-hemoglobin), and can be varied in order to investigate different processes.

fNIRS has several features that are desirable for BCI applications.[26] It involves relatively low cost relative to other neuroimaging methods (though it is generally more costly than EEG setups); it can be portable and is generally robust to movement of the user; it is non-invasive and safe; it is easy to setup and use; the signal-to-noise ratio is high; and it is not affected by ambient electrical noise like EEG and magnetoencephalography (MEG). fNIRS has very high spatial resolution, and the location and depth of the measurements can be precisely controlled.

Common brain regions of interest for fNIRS-BCIs are the primary motor cortex (PMC) and the prefrontal cortex (PFC).[26] The PMC affords BCI control using motor execution (performing a physical action) and motor imagery (imagining oneself performing a physical action), whereas the PFC lends itself to higher-order cognitive processes such as concentration, mental arithmetic, and counting. The first implementation of fNIRS-BCI documented in the research literature comes from a pair of studies by Coyle *et al.*[61,62] who used a motor imagery approach to have users control a binary switch in a prototype system called *Mindswitch*.

The main limitation of fNIRS, especially as it related to BCIs, comes from it's temporal resolution. Whereas EEG and MEG directly measure electrical or magnetic properties of action potentials which are virtually instantaneous, the BOLD signal that is measured by fNIRS is indirect and changes in activity are

only observable after a delay of several seconds.[26] This makes fNIRS poorly suited for BCI applications that require precise timing or rapid input.

The poor temporal resolution of fNIRS-based BCIs makes them poorly suited for directly controlling a primary task. In order to circumvent the this, a category of *passive BCIs* have been proposed[63] which do not require voluntary input from the user. Rather, passive BCIs monitor the state of the user and automatically make adjustments to improve the user's interaction with a computer system.

A number of fNIRS-based passive BCI approaches have been studied by Jacob *et al.* (e.g., Bosworth, Russell, and Jacob[64]). For example, Afergan et al.[65] used fNIRS over the prefrontal cortex to assess users' engagement while they completed an unmanned aerial vehicle (UAV) path planning task in which they had to manage a variable number of UAVs. Difficulty of the task was modified in accordance with the prefrontal cortex activity by adding UAVs to the simulation to increase difficulty when engagement was low (indicating boredom) or removing UAVs when engagement was very high (indicating that the user may be overwhelmed). In this case, BCI-based dynamic difficulty adjustment resulted in a 35% reduction in errors relative to static difficulty, successfully demonstrating the principle of dynamic difficulty adjustment based on neurophysiological indices of engagement.

2.5 Other BCI Modalities

Magnetoencephalography (MEG) is akin to EEG in that it non-invasively records the net electrical activity of large populations of neurons below a sensor placed on the scalp.[66,67] Whereas EEG directly measures fluctuations in electrical currents occurring in the brain, MEG detects the magnetic fields that are generated by those currents.[66,67] One of the significant advantages of MEG over EEG is that the magnetic fields measured by MEG are not attenuated by bone and can therefore pass unimpeded through the skull. This fact enables MEG to capture

frequency spectra such as high-gamma activity which are ordinarily not capturable with EEG due to attenuation by the skull. Unfortunately, several factors prevent MEG's applicability for BCI use: MEG apparati are room-scale devices, which require significant magnetic shielding to prevent interference from ambient electrical noise,[66–68] and are therefore non-portable, prohibitively expensive to purchase and maintain, and require significant expertise to operate.

Nonetheless, several researchers have examined the applicability of MEG for BCI systems with encouraging results,[69–73] suggesting that the MEG signal contains information that is useful for BCI applications. A wearable MEG system designed by Boto et al. [68] significantly advanced the state of the art of MEG-based BCIs by enabling a greater degree of mobility and portability. While the requirement of magnetic shielding and barriers related to cost and operability remain, Boto et al. [68]'s wearable system enables substantially more freedom of movement and articulation relative to a traditional MEG system as can clearly be seen in Figure 2.2. Given this trajectory, further refinements to MEG technology may tip the cost-benefit analysis to be more favourable for real-world BCI applications.

Figure 2.2: A comparison of a typical MEG system that requires the user to remain stationary (left) and a wearable MEG system that affords greater freedom of mobility and articulation (right). Adapted from Boto et al. [68].

Magnetic resonance imaging (MRI) is a non-invasive medical imaging technique which uses a powerful magnet and radio-frequency emitter to manipulate the orientation of hydrogen ions (i.e., protons) in a living organism.[74] MRI has unparallelled spatial resolution and the ability to examine any location or depth of a sample. Briefly, a strong electromagnetic field is applied which forces all protons within field to become aligned with it. Radio pulses are emitted which disturb the protons and cause them to spin out of alignment. Once a radio pulse has ended, the protons return to alignment, releasing energy which is detected by the apparatus. The amount of time taken and energy released by the protons returning to alignment with the magnetic field reflects the density as well as other chemical properties of the sample. The magnetic resonance (MR) signal can be detected from any depth within the sample (provided it fits inside the scanner) and can therefore resolve even the deepest structures in the brain. The magnetic field is moved across the subject to scan the entire area of interest, which can be as small as a few millimeters or include the entire body. The resulting *image* is a model of the sample composed of three-dimensional voxels that can be used to detect the presence of tumours, tissue damage, vascular abnormalities, and many other conditions.

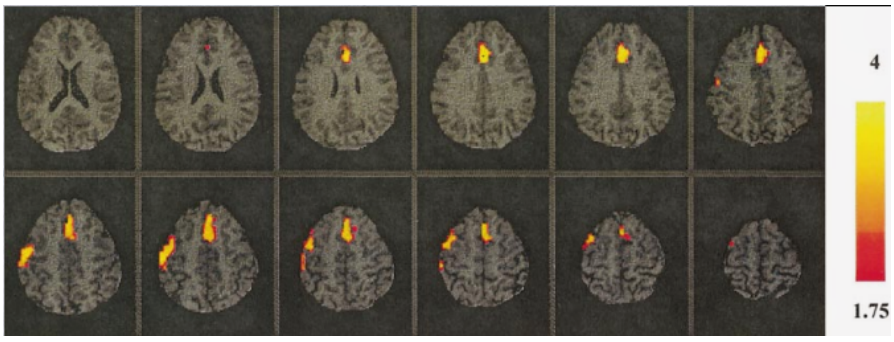

Figure 2.3: A series of fMRI images showing increased activity in various brain regions at a single point in time, as measured by the BOLD signal. Each image is a horizontal slice of the human brain, starting from the most inferior (i.e., lowest) slice in the top left corner and moving to the most superior slice (at the top of the brain) in the bottom right corner. Reproduced from Langleben et al. [75].

Functional MRI (*fMRI*) is the application of MRI to functional neuroimaging by utilizing the BOLD signal (as in fNIRS, described in Section 2.4).[74] However, whereas fNIRS is limited to recording activity near the surface of the brain, fMRI can access any structure of arbitrary depth. Disadvantages of fMRI are analogous to those of MEG: MRI scanners are very expensive, non-portable, difficult to operate, and prohibit movement of the subject during the scan. In addition, fMRI shares the drawback of fNIRS that the hemodynamic response that generates the BOLD signal takes on the order of several seconds to be observed, making BOLD measurements indirect and temporally imprecise. Several BCI systems have been developed which use the BOLD readings from various brain areas as a control mechanism to interact with a computer system for such purposes as neurofeedback,[76–81] control/mental commands,[82–86] and communication.[87–91]

A further possibility for non-invasive BCIs comes from the combination of two or more recording modalities. For example, the combination of EEG and fNIRS enables both the electrophysiological and neurovascular activities of the user to be used as control signals. Similarly, strictly brain-based recordings can be combined with other biometric signals such as eye-blinks (using an *electrooculogram EOG*) or muscular activity (with an *electromyogram* or *EMG*). The various types of hybrid BCIs that have been implemented are too numerous to be described in full here, but a 2017 review by Hong and Khan [92] provides an overview.

2.6 BCI Applications

A number of non-medical applications have been investigated for BCIs which include neurofeedback and meditation training, communication,[93] entertainment and gaming,[94–96] integrated control of connected internet-of-things (IoT) devices,[97] dynamic skill learning,[94,98] and workload management.[65,99,100]

A	B	C	D	E	F
G	H	I	J	K	L
M	N	O	P	Q	R
S	T	U	V	W	X
Y	Z	1	2	3	4
5	6	7	8	9	0

Figure 2.4: A typical grid speller interface, which allows a communication-impaired person to compose text messages using any type of unary signal. Rows are highlighted one at a time, top to bottom, and the user issues a signal when the highlighted row contains their target character. Each character in the row is then highlighted individually, from left to right, and the user responds again once their target when the speller reaches their target letter.

The P300 speller BCI paradigm has been used for a number of years to enable communication for individuals with severe motor or communication impairments.[101] Briefly, the P300 speller takes advantage of the P300 event-related potential (ERP), which can be reliably detected immediately following the presentation of a target stimulus. The basic idea is to present a sequence of letters to the user while monitoring for a P300 response. The P300 is used as an indication that the letter that has just been presented is the one that the user wants to add to the message. Rather than presenting a stream of letters, most P300 spellers show a grid of letters (as in Figure 2.4) and have users first select the row that their target letter appears in before cycling through the letters in that row. The P300 speller system can be extended to enable novel forms of telecommunication between individuals. Kerous and Liarokapis[93] developed an application, BrainChat, which combines a P300 speller with an *augmented reality* (AR) interface that enabled two individuals to communicate remotely.

Vasiljevic and Miranda[96] published a comprehensive review of 82 BCI games based on consumer EEG devices covering a wide range of devices, control

paradigms, and genres. They found that the majority of BCI games were intended for serious applications such as training, research, and healthcare, whereas relatively few were intended for entertainment purposes. Based on their findings, the authors make recommendations for the development of BCI games as well as open areas for research (most notably a general lack of research around the *user experience* of BCI games in favour of performance-centric measures).

Jacob and colleagues have pursued the applications of passive (or *implicit*) BCIs based on fNIRS.[65,94,98–100] Their general approach is to passively monitor indices of engagement and attention using fNIRS over the frontal cortical areas and based on that make adjustments to a different system that the user is engaging with. Jacob's group has successfully demonstrated this passive control paradigm with respect to skill learning,[94,98] and multi-tasking.[99,100] These findings raise interesting possibilities for BCIs to facilitate human-machine cooperation.

2.7 BCIs for Authentication

The biometric specificity of EEG has been seriously investigated since at least the 1970s,[102] though it was not until much later that this was applied for the purpose of biometric authentication. Poulos, Rangoussi, and Alexandris [103] and Paranjape et al. [104] published studies in 1999 and 2001 respectively demonstrating classification systems which could identify individuals from a small sample based on features of their EEG with accuracies between 80 and 100%. Since then a number of studies[15,105–109] have implemented biometric authentication systems based on resting-state EEG with reasonable success, demonstrating that the uniqueness of individual users' EEGs is sufficient for biometric authentication, at least within a restricted population.

Stimulus-response EEG authentication can be viewed as an extension of resting-state EEG biometric authentication in which a (typically visual but sometimes auditory[110]) stimulus is presented to the user in order to provoke a particular pattern of activity in the EEG which is compared for authentication.[110–117] A common stimulus-response paradigm involves the P300 ERP described in Section 2.6. For example, Lin et al.[118] developed a system which used P300 responses evoked from viewing a series of target and non-target images.

The idea of BCI authentication or *passthoughts* was first outlined in detail (although not successfully implemented) by Thorpe, van Oorschot, and Somayaji,[14] though some earlier work was done on the broader concept of using EEG signals as a biometric.[103,104] Passthoughts are an extension of EEG-based biometric authentication in that they include a secret mental task which is used to evoke the EEG signal used for comparison. This in theory provides strong security in the form of two-factor authentication because the passthought comprises both a secret and a biometric component[14,119] which can be presented to the system simultaneously. Passthoughts are also advantageous over other types of biometric authentication in that they are *changeable* (or *cancelable*); that is, the secret component of the passthought can be revoked or altered in the event that the passthought is compromised, with a theoretically extremely large possibility space.[119] Passthoughts also possess the capacity to be *unobservable*, rendering them immune to shoulder-surfing attacks.[14]

A number of concrete implementations of passthoughts were published since Thorpe, van Oorschot, and Somayaji's[14]'s original proposal.[120–134] A 2017 review by Merrill, Curran, and Chuang[119] discussed the advantages, implications, and some future possibilities of passthoughts such as single-step multi-factor authentication, continuous authentication, and organic passwords that change over time. The most comprehensive high-level treatment of this topic is a 2019 review by Gui

et al. [135], which covers a number of issues related to passthought authentication including comparisons of classifiers, signal collection and processing protocols, and the permanence and stability of EEG biometrics over time and across differing mental states. For a more detailed examination of concrete passthought implementations, Jayarathne, Cohen, and Amarakeerthi [136] provide a review of several studies, contrasting their approaches and the level of accuracy achieved.

A few studies have addressed the question of the stability of EEG-based passthoughts over time,[105,118,128,137–139] but the most direct empirical exploration of this topic is found in a 2016 study by Maiorana, Rocca, and Campisi [140]. After acquiring a database of EEG recordings taken from 50 subjects at three time points over one month, the authors analyzed the similarity of features extracted from the EEG for each subject over time. Results using different classifiers, EEG frequency spectra, and electrodes placements supported the conclusion that some features of the EEG are sufficiently stable over time to be used for biometric authentication. A comparison of 19 studies addressing the permanence of EEG biometrics in Gui et al. [135] supports this conclusion.

A fundamental tension in authentication is the balance between security and usability;[16] *strong* authentication methods tend to be difficult for an average user to use properly, whereas *simple* or *easy* authentication methods tend to lack strong security. The majority of published studies detailing passthought authentication schemes are concerned primarily with technical details such as minimizing the false acceptance and false rejection rate of their classifiers. While the system performance is a critical component of usability, an understanding of the subjective *experience* of a person using BCI authentication is essential to understand the potential role of passthoughts in society.

The first empirical work on the usability of passthought authentication was published by Chuang et al. [18] in 2013, with two significant contributions. Firstly,

it is demonstrated that EEG-based passthought authentication can be achieved in a sample of 15 individuals using a single-channel dry-contact EEG headset (Neurosky Mindwave[55]), which is much less intrusive and cumbersome than the more sophisticated multi-channel gel- or saline-based EEG devices that are typically used in passthought studies. Secondly, by allowing participants to test a range of different types of passthought tasks it was demonstrated that users display clear preferences in the types of tasks that they would prefer to use as passthoughts. The types of tasks that users rated as the most repeatable were those that were not rated as being either *boring* or *difficult*. Somewhat surprisingly, passthought tasks that were chosen by the users themselves were rated as more boring, more difficult, and less repeatable than some of the researcher prescribed tasks such as counting instances of a colour or focusing on breathing.

2.8 Barriers to BCI Adoption

Prior work examining barriers to adoption of BCIs is mostly limited to specialized populations such as those with severe neuromuscular disorders.[141–145] This is to be expected as the restoration of communication or motor functions for those with disabilities is one of the most promising and meaningful applications of BCIs. These findings, however, are difficult to extend to the general population because the potential non-medical benefits of BCIs are much more limited in scope. I am not aware of any work directly assessing barriers to adoption of commercial non-invasive BCIs amongst the general population.

Lightbody, Galway, and McCullagh [146] summarized the current state of BCIs in 2014 and future obstacles for BCI technologies with an emphasis on barriers to public adoption. They identify four categories of barriers to BCI pervasiveness: scientific limitations, including basic science of neurophysiology and EEG,

BCI hardware and software; high system complexity and need for extensive support; user acceptance, including performance expectations and social stigma; and ethics, covering issues of accessibility, informed consent, privacy, and liability. The authors offer a few suggestions for critical areas for improvement: general ease-of-use of the system, good documentation and support; battery life and ergonomics of the system; more usable (i.e., dry) electrodes; and optimizations to the user experience tailored to the BCI modality.

2.8.1 Acceptance of BCIs among persons with disabilities.

Blain-Moraes et al. [143] held a focus group with individuals with ALS and their caregivers in order to identify barriers and other factors that influence BCI acceptance. Participants were recruited from a previous BCI study and so had some experience with BCIs. Several themes emerged in their analysis which were categorized into *personal factors* and *relational factors*. Personal factors include physical and cognitive fatigue, attitudes toward the technology, anxiety, distractions, and pain or discomfort. Relational factors include corporeal elements such as the electrodes which connect the person to the machine, integration of the BCI into existing hardware and software, changes in the relationship between the individual with ALS and their caregiver, the need for training and/or support personnel, and the appearance of the device.

An investigation by Geronimo et al. [144] had patients with ALS engage in a session to learn about BCIs and then asked to rate their interest in BCIs across several dimensions before and after using one. They found that participants' interest in BCIs was significantly related to the type and severity of their impairment, and that performing well using the device led participants to become more interested in BCIs whereas performing poorly was associated with decreased interest. Participants' expressed preference for 80–90% minimum accuracy, spelling rate

of 15–19 letters per minute, 10–30 minute setup time, and 2–5 required training sessions.

Huggins and colleagues conducted studies assessing attitudes toward BCIs among individuals with ALS[141] and with spinal cord injuries (SCIs).[142] The findings indicated that both patient groups were significantly interested in BCIs with similar performance expectations of at least 90% accuracy and typing speed of 15 to 20 letters per minute. Expectations were similar for the number of acceptable sessions or hours required for training as well as the relative importance of features such as *ease of use* and *ease of setup*. Those with ALS were more open to the idea of implanted electrodes than patients with SCI with more than 70% of patients in the ALS study reporting that they would be willing to undergo outpatient surgery versus 46% in the SCI study. Participants in both studies expressed a strong preference for dry electrodes over saline- or gel-based ones. These findings about performance requirements in the ALS study[141] are quite similar to those found by Geronimo et al. [144].

Diep and Wolbring [145] conducted interviews with mothers of children with disabilities who had no prior experience with BCIs. Mothers in the study were enthusiastic about the possibility of improving their child's communicative ability through BCI in order to expand their social network and to aid in interpreting their needs. The majority of mothers were against the possibility of their children having invasive BCIs. Mothers in the study also generally expressed a negative sentiment about the idea of any non-disabled person using a BCI, or that they should be used for non-therapeutic purpose (i.e., gaming). Several ethical issues were raised surrounding the use of BCIs, including accessibility (cost, qualification barriers), and concerns about whether data would be collected and who would have access.

2.8.2 Concerns about security and privacy.

The issues of security and data privacy are a significant concern to the research community[147–155] and may present a major barrier to adoption among the public. Given the proximity of (especially invasive) BCIs to the brain, as well as their role in controlling various mechanical apparati such as electric wheelchairs and robotic prosthetic limbs, there is potential for serious harm in the event that the security of these devices is compromised by a malicious attacker.

For example, Pycroft et al. [156] outline potential security threats concerning deep-brain stimulation (DBS) devices (*brainjacking*) which are most commonly used to attenuate symptoms of Parkinsonism. For example, in the extreme case it may be possible for an attacker to cause damage to a victim's brain by increasing stimulation parameters beyond safe levels. More sophisticated attacks are described that may be possible if an attacker has extensive knowledge about the symptoms and medical history of the target. The security hazards associated with DBS will vary based on the type and placement of stimulating electrodes, as well as the underlying condition being treated. Pugh et al. [155] discuss some of the more troubling implications of brainjacking with respect to individual autonomy and social responsibility.

Merrill, Chuang, and Cheshire [157] demonstrated that participants with no experience with BCIs believe that brain-sensing technology can reveal more about them than most other types of sensors, including GPS. Ienca and colleagues[149,151] have outlined data privacy challenges associated with BCIs, highlighting the general failure of legislative agencies to keep pace with technological progress. They propose measures to protect neurological data from BCIs including implementing

regulations (*e.g.* PIPEDA in Canada and HIPAA in the USA) around *neuromarketing* and expanding protections for medical data to include data generated from non-medical BCIs.

Several studies have investigated the information that can be recovered or derived from neurophysiological data.[158–161] A landmark study by Martinovic et al.[158] in 2012 demonstrated the possibility of covertly extracting private information using a maliciously constructed BCI app. By presenting various images to participants and monitoring for evoked P300 ERP responses, they were able to infer limited private information such as the area in which they live, month of birth, and preferred banking institution. This area of work was later expanded by Frank et al.[159], who demonstrated a subliminal attack by presenting stimuli too briefly to be consciously perceived while participants were engaged in an unrelated primary task. Similar to Martinovic et al.[158], Frank et al.[159] were able to determine whether subliminally presented images of faces were of someone known or unknown to the participant. Critically, when asked, participants reported not being aware of the presentation of any faces or unusual stimuli during the task.

An impressive but foreboding body of research has demonstrated the capability of statistical modelling and machine learning techniques to reconstruct images viewed by a participant undergoing an fMRI scan.[162–167] For example, a 2019 study by Shen et al.[162] demonstrated a generative adversarial network (GAN) model which produced the images in Figure 2.5. The practical relevance of these findings from a security perspective is lacking, given that fMRIs are currently not very suitable for BCI applications due to their size and cost, and the reproduced images themselves remain rather unclear, particularly if the original image is not presented for comparison. What these studies demonstrate, however, is that the retinotopic mapping of the primary visual cortex can be used to deterministically extract information about the content of a person's visual field. Continuing progress in

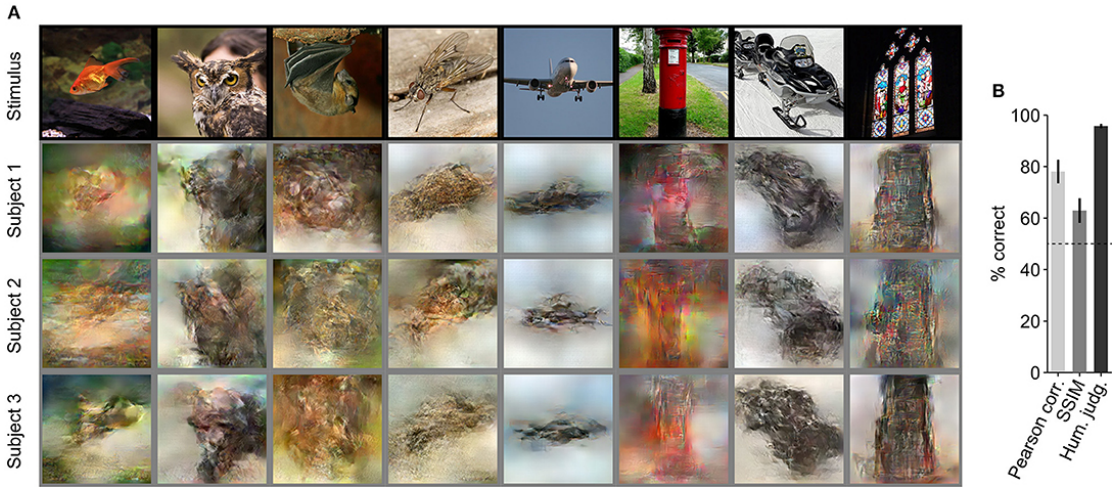

Figure 2.5: Reproduced from Shen et al. [162]. (A) Original stimuli images (top row) and images reconstructed by a deep neural network from fMRI data for three participants. (B) Average similarity between the stimulus and reconstructed images assessed using Pearson correlation, structural similarity index (SSIM), and human judgement.

machine learning methods as well as increasing sophistication of commercially available neuroimaging devices suggest that this may become a significant issue for the privacy and security of BCI devices in the future.

To summarize, the barriers to BCI adoption are numerous. All types of invasive BCIs have an inherently severe barrier in the form of surgery and the possibility of complications. Recurring themes among studies of BCI usability include the need for easier and less technical setup, as well as better system performance overall. Among those with disabilities, BCIs raise questions about social stigma due to their obvious appearance, as well as more existential concerns about the nature of the relationship between human and machine, personal autonomy, and individuality. Security and privacy issues are additional barriers which will likely need to be solved before widespread adoption of BCIs is feasible.

Chapter 3

Mental Command Graphical Password System

3.1 Motivation

In theory, BCI authentication has distinct advantages over text passwords and other biometrics. Passthoughts are *unobservable*, and are therefore immune to shoulder-surfing attacks. Unlike static biometrics, passthoughts are changeable and will naturally degrade over time unless a classifier is continuously retrained.[119] Passthoughts require a secret (i.e., a thought or mental task; a *knowledge* factor) as well as a biometric match (an *inherent* factor; the biometric specificity of EEG-based passthoughts is demonstrated in Lin et al. [118] and Merrill et al. [15]), meaning that they comprise two inherent authentication factors which can be entered in a single step,[15] overcoming a major obstacle with multi-factor authentication that typically requires a separate step for each factor. Additionally, passthoughts—as with BCIs in general—open up new possibilities for individuals with severe impairments.

In practice, however, little is known about the usability and practicality of passthoughts for real-world use. Given the security-usability trade-off that is thought to be inherent to all authentication methods,[168] it is possible that poor usability could render passthoughts ineffective as a practical authentication method for the general public despite their desirable security characteristics.

I designed a prototype passthought authentication system based on mental commands with Emotiv BCI devices in order to assess usability characteristics of

this type of BCI authentication. The mental command approach, wherein a machine learning classifier is trained to distinguish various brain states and associate them with a discrete output command, was used in order to be compatible with other BCI tasks.

The aim was to build a system to believably emulate the user experience of passthought authentication, rather than to build a fully-functional and properly secure authenticator. Modifications to the hardware and software are discussed below which could be implemented to make a truly secure version of the system, but the implementation of this is beyond the scope of this research.

3.2 System Requirements

The overall design of the passthought authentication system was guided by the following considerations:

Plausibility as a *real* authentication system. The primary goal of the authenticator is to study aspects of the usability of passthought authentication. Therefore, priority is placed on elements of the system which the user will see or interact with. Security features that do not affect the user experience (e.g., password hashing, data encryption) are not necessary as the application is not intended to ever be deployed in a real security context.

However, in order for this work to be useful it should at least be plausibly adaptable into a secure system that could be used in a *live* context. Therefore some consideration must be given to security features and how they might be implemented if one were to develop a real authenticator based on the usability prototype.

Authentication using mental commands. Interaction with the system will be based on mental commands, in which the user issues discrete commands to the system by generating a distinct pattern of EEG activity, for example by engaging in a motor imagery task.

The mental command interaction paradigm was chosen for a few reasons. Mental commands are a common application of BCIs and are generalizable as a control scheme for any number of applications beyond authentication. Using a common BCI input method for authentication and other BCI tasks has the advantage of potentially improving authentication performance through increased system fluency. This also enables more elaborate usability tests in which users use a common control scheme for a number of tasks in addition to authentication. Directional commands are compatible with existing authentication paradigms, such as the *pattern unlock* that is common with Android devices.[169] A further advantage is that mental commands have been shown to be feasible with consumer-grade BCI devices[170] and tools exist to facilitate training mental commands and integrating them into external applications (e.g., Emotiv Cortex API[171]).

Random assignment of password sequences. Users will be assigned a password sequence by the system rather than creating their own. This constraint was added to aid usability testing by removing the potential confounding factor of users choosing password sequences with special meaning or reusing a sequence that they use for their phone, for example, which would complicate assessments of the memorability of the system.

Single-step multi-factor authentication. Merrill et al. [15] successfully demonstrated a passthought application which required three distinct authentication factors (a secret, a biometric, and a physical token) that could be authenticated in a

single step. This capability of passthoughts can potentially overcome a significant limitation to the usability of multi-factor authentication systems which typically require a separate action from the user for each factor.[172–175]

In order to achieve single-step multi-factor authentication with passthoughts, a mental task is required that can serve as a secret. In the case of mental commands, this can be a sequence of commands which form a sort of password. The biometric factor is inherent in the biometric specificity of EEG patterns; two individuals performing the same mental task would nonetheless have quite different EEGs.[15,118] Knowledge of a user's secret command sequence would be insufficient to impersonate them because the impersonator would not be capable of reliably generating the correct EEG states to produce the sequence. Note that an additional constraint must be added to the system in order for this biometric specificity to work with mental commands. The classifier that translates EEG states into commands must be directly linked to the user's identity, otherwise an impersonator with knowledge of a victim's command sequence could simply train their own classifier and use it to output the commands. This has the further implication of making the classifier a sort of authentication token. If the classifier is embedded into the firmware of the BCI headset, the headset can be considered a physical possession factor.

Minimal hardware burden. Many BCI devices have time-consuming and/or very technical setup procedures which impair usability. For example, research-grade EEG caps usually require the application of a conductive gel to each electrode which can take upward of one hour if there are many electrodes and also dirties the hair and scalp of the user. Several consumer-grade devices similarly require application of a saline solution prior to use. In addition, BCI devices can be large, uncomfortable, and/or tethered to many wires and cables. For this usability

prototype it was important to minimize these issues when selecting the hardware platform.

3.3 Design

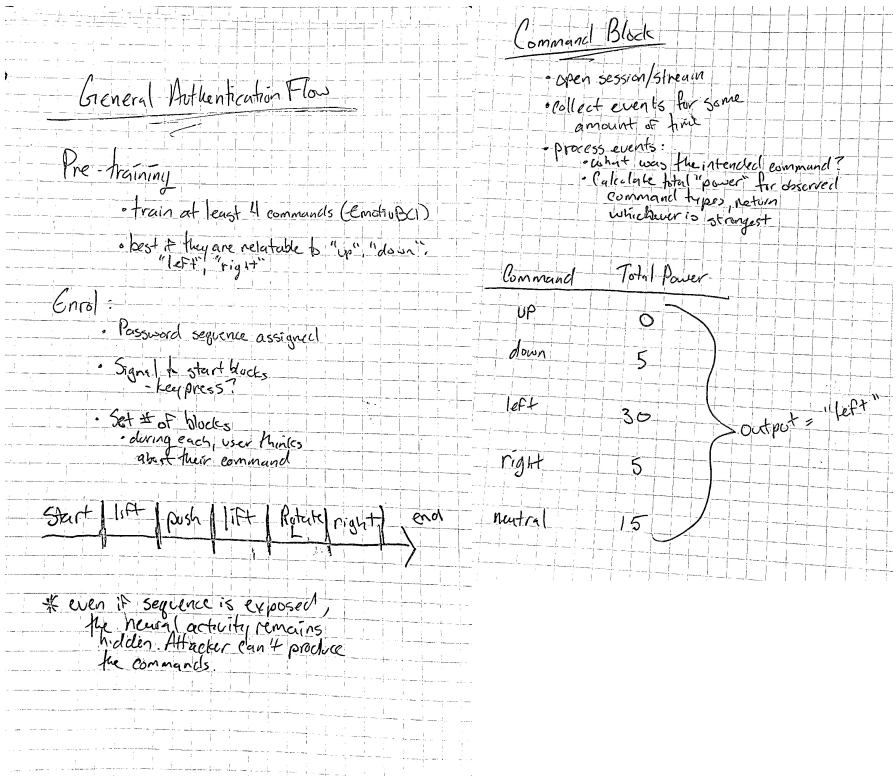

Figure 3.1: Design sketches from the planning phase of application development. *Left:* The general action sequence for enrolling a password into the system. At least four directional commands must be trained corresponsing to the directions *up, down, left,* and *right*, which are used to *draw* the password sequence. A series of *Command Blocks* comprises a password sequence of arbitrary length. *Right:* The basic concept for Command Blocks that comprise the password (discussed in Section 3.4.2). Command data is aggregated over a period of time and then processed to determine the *strongest* command during the interval, which becomes the discrete output for the block.

The choice of the BCI hardware and platform to use is a significant decision which informs the rest of the design process. A number of consumer-grade BCI devices were considered: Emotiv Epoc or Insight,[57] the Muse headband,[56] Neurosky Mindwave,[55] and an OpenBCI starter kit.[58] The Muse and Neurosky devices

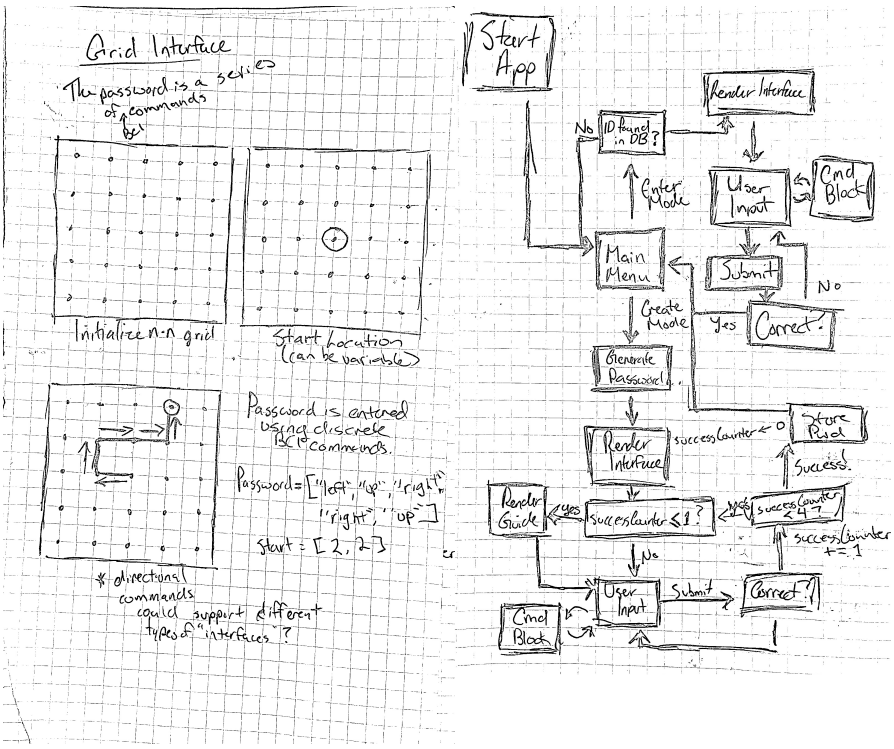

Figure 3.2: Design sketches from the planning phase of application development. *Left:* A diagram of the proposed interface. The user *draws* their password on the grid in a series of discrete movement steps using mental commands. *Right:* A flow diagram showing the essential functionality of the authenticator, beginning from the box labelled *"Start App"* in the upper left. This diagram was used to develop the structure of the software prototype.

were ruled out because their sensor configurations were not considered suitable for mental commands (too few sensors and non-ideal placement over the frontal areas only).

The OpenBCI Ultracortex[58] too was ruled out because it involves a greater usability burden due to increased weight and wet sensors, and it was thought that perceptions of usability may be impacted by the *do-it-yourself* appearance of the device, which is large, bulky, and covered in exposed wires and circuit boards. While comparable to other commercial systems in price, the OpenBCI Ultracortex is geared primarily toward researchers and developers and therefore aesthetic design is less of a priority, whereas for this project I was more interested in a more general population for whom the aesthetic component of the device would carry more weight.

The Emotiv devices provide a good balance of sensor coverage (with 5 and 14 sensors for the Insight and Emotiv devices, respectively), usability, cost, comprehensive API, and prebuilt tools to facilitate training and using mental commands in the EmotivBCI application.[171] Therefore the Emotiv devices were selected as the platform of choice for this project.

The next consideration for the design of the application was determining how to form a password from mental command events. In other words, what *form* would the password take, and how would it be stored for comparison? Part of the design process for this step is illustrated in Figure 3.1. The Emotiv[57] mental command stream[171] (discussed below in Section 3.4.1) sends several events each second, so a method was needed to further discretize the inputs. Each mental command event is associated with a *power* value, so it is possible to determine the most *strongly* detected command over a given period of time by summing the power of each command detected during that time. For simplicity I will refer to this as a *Command Block* (see Figure 3.1, right side). In theory command blocks

should improve system accuracy as the output for each block is determined by the consensus of many classifier predictions instead of one. A command-block-based password can be represented by simple data structures such as an array or string that can be cryptographically hashed or encrypted.

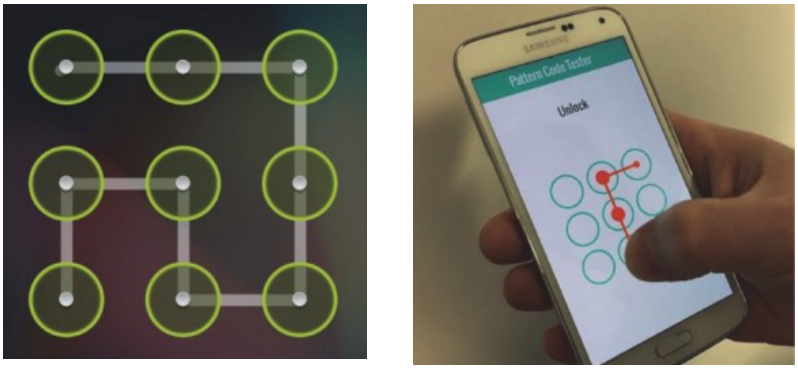

Figure 3.3: The default Android touchscreen pattern lock screen (left) and a different implementation of the same system (right). Reproduced from Colley et al. [169]'s 2016 paper on improving pattern lock authentication by incorporating additional types of gestures.

The next issue to arise was that of the interface design. The command block password structure could support a variety of graphical *front-ends* provided that they involve a task that could be accomplished with mental commands. The most apparent of these is the *pattern unlock* paradigm that is common on Android touchscreen devices (Figure 3.3). This design was pursued due to its simplicity and familiarity; the basic idea is illustrated in Figure 3.2 (left side).

The system interaction was roughly sketched out as a flow diagram (Figure 3.2, right side) to use as a guide for the development of the software prototype. A *Main Menu* page serves as a hub where a user can enter their identity and select whether to create a new password or attempt to authenticate using a previously associated password. The interfaces for the *Create Mode* and *Enter Mode* are largely identical

except that *Create Mode* provides more feedback/help and involves additional steps.

Several other factors were deemed essential for the prototype:

- In *Create Mode*, a guide showing the correct password sequence will be available.

- A *trail* will be visible indicating all of the moves that the user has made to get to their current position.

- The user will be able to easily *undo* commands in the event that they make a mistake or their intent is misinterpreted by the application.

- Similarly, the user will be able to completely reset the interface to it's starting state.

- There will be a prominent area for instructions to be displayed.

- The state of the application (*initializing, ready, command block, success/failure*) will be clearly visible at all times.

- The password length, grid size, and command block duration will be configurable.

- An experimenter running the software will be able to trigger errors (where the system executes *wrong* move regardless of the user's intent) either manually or according to a predetermined likelihood (optional/time-permitting).

3.4 Implementation

3.4.1 General architecture and system overview.

The authentication system is designed to be used with Emotiv devices.[57] Emotiv devices provide a comprehensive API for interacting with the devices as well as built-in tools for training and managing mental command profiles (called *Cortex*[171]). The ergonomics and aesthetic design of Emotiv devices are also beneficial to minimize the impact of the appearance of the device on perceptions of usability. Finally, having access to both the *Epoc* and *Insight* devices, which have 14 and 5 EEG electrodes respectively, it is possible to compare the performance of different tiers of commercial BCI devices without having to support an additional API. The two Emotiv devices are shown side-by-side in Figure 3.4.

Figure 3.4: Side-by-side comparison of the Emotiv Insight EEG headset with five electrodes (*left*) and the Emotiv Epoc EEG headset with fourteen electrodes (*right*), showing what they look like when worn on the head (*top*), as well as on their own (*bottom*). Images reproduced from Emotiv's website.[57]

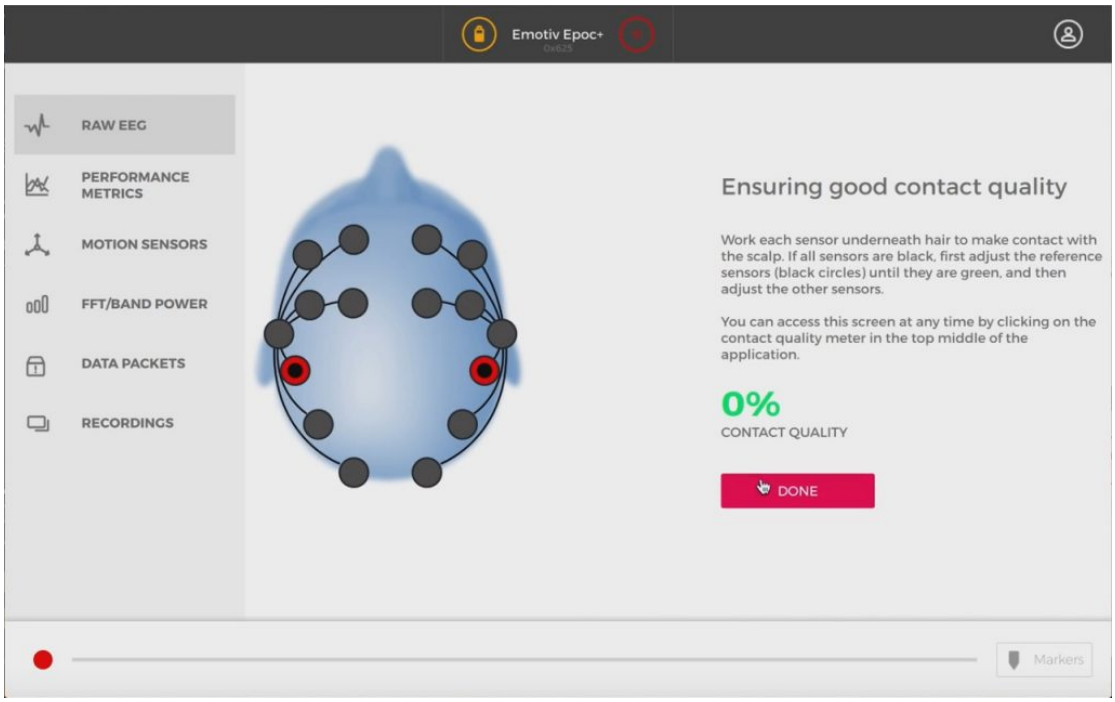

Figure 3.5: The contact quality page of the Cortex application for the Emotiv Epoc.[57] Each electrode on the headset is represented by one of the circles on the model head. The two circles indicated in red in the figure are the reference electrodes that are placed over the mastoid bone. Contact quality for each electrode is colour-coded, with dark grey indicating no contact, red and orange poor contact, and green good contact. The contact quality value in green is based on the state of all of the electrodes, where a value of 100% would mean that all electrodes have good contact (green circles). Reproduced from Emotiv Inc.[57]

The BCI headset is connected to a PC running Windows 10 by a device-specific Bluetooth dongle (all libraries, APIs, and other components of the application are compatible with MacOS, but it has only been tested on Windows). The Cortex API[171] software is launched on the PC and used to establish the connection between the PC and the device. A graphical tool is provided alongside the API which shows the contact quality for each electrode (Figure 3.5). Good contact is represented by a green circle, whereas no contact is represented by grey and bad contact by red or orange. An aggregate *Contact Quality* percentage value is also shown. It is recommended by Emotiv that at least 95% contact quality is achieved before proceeding to use the device.

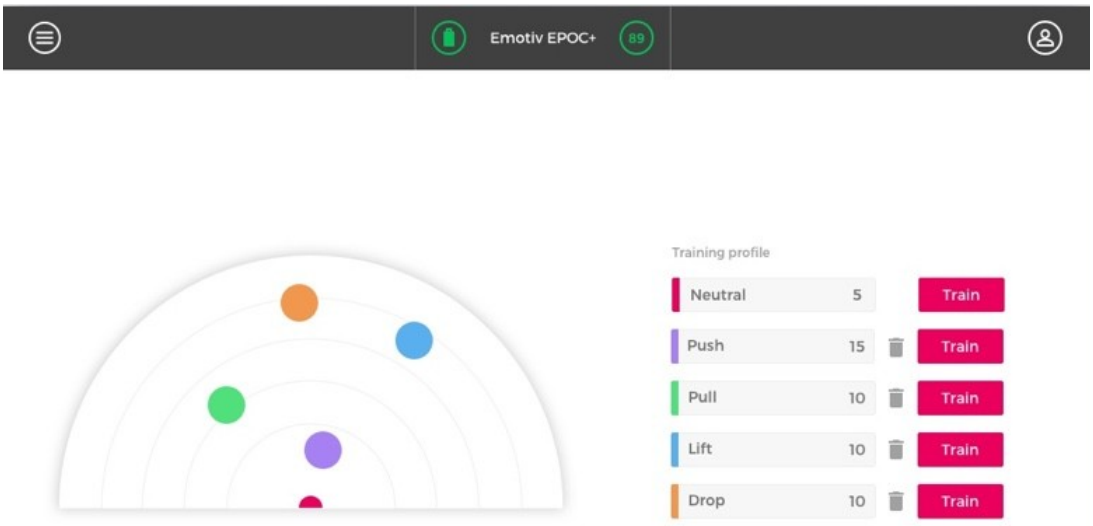

Figure 3.6: The training profile interface of the EmotivBCI application. The user can select up to four commands to train (in addition to the *Neutral* state). More than four commands can be trained (there are thirteen in total), but only four can be *active* at a given time. Clicking the *Train* button will begin a training session for that command (see Figure 3.8). The number listed next to each command indicates the number of times that the command has been trained. The diagram on the left side indicates the distinctiveness of each command; ideally the coloured circles will be far apart from one another indicating that the EEG patterns associated with the commands are sufficiently distinct. Reproduced from Emotiv Inc.[57]

The authentication system is implemented as a single-page web application written in JavaScript. A server is implemented using the `express` NodeJS library[176] which is responsible for coordinating the activity of the client-side interface, Emotiv Cortex API[57] (and thus the hardware interface), and a MongoDB[177] database. The database is used to store user passwords as well as metadata. Importantly, passwords in the database are not hashed or obscured in any way; rather, they are represented as an ordered array of text strings representing the commands that comprise the password. As discussed in Section 3.1, the goal of the software was to create a *simulation* of a secure BCI authenticator, and therefore security features that would not affect the user-experience (such as password hashing) were not considered a necessity.

The Cortex API[171] exposes a websocket which is used to send and receive API calls and responses. A JavaScript class called `Cortex` was implemented on the server as a wrapper for the Cortex API which handles constructing and sending requests to the API (in the form of JSON-RPC objects using the `socket.io` NodeJS library), receiving and processing responses from the API, as well as logging these events. The functionality of training mental commands was not implemented in the application; rather, a mental command profile is created and trained using the EmotivBCI application provided by Emotiv[57] (see Section 3.4.2). The profile is then loaded into the authentication application.

The general structure of the application is shown in Figure 3.7. Once a client connects and the main webpage is served, a script (`index.js`) runs which creates a websocket connection between the client and server before initializing the user interface. The user is asked to provide an ID, which is passed back to the server via the websocket and queried against the database. If a match is found, the user is able to select to enter their password or to create a new password (overwriting

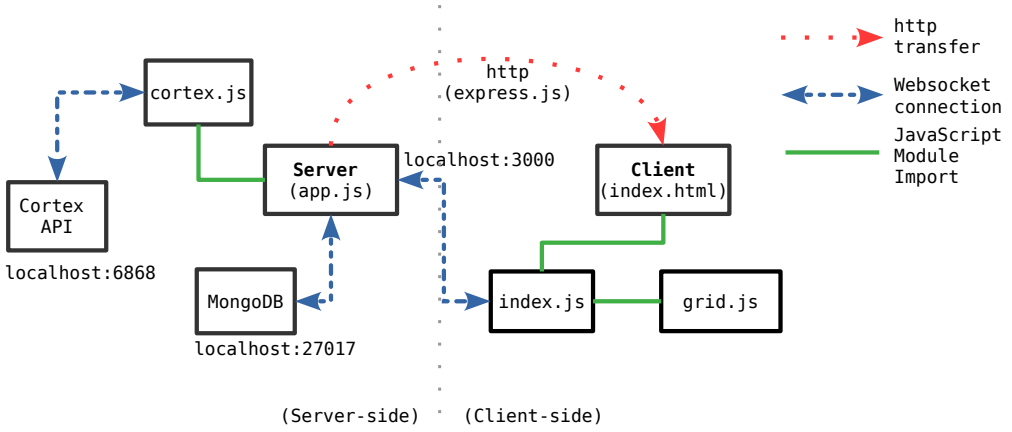

Figure 3.7: A schematic diagram of the authentication application showing relations between the major server-side and client-side components. The application server is responsible for serving the application client when a user connects as well as coordinating the activities of the database and hardware API. The application client is responsible for creating a websocket connection to communicate back to the server as well as all of the logic for drawing and interacting with the interface.

their current one). If no match is found in the database, the user can only create a new password associated with the provided ID.

In both cases, the grid interface (described in Section 3.4.4) is rendered and the connection is established between the server and Cortex API. At this point the Cortex training profile associated with the ID is initialized as well. The user is then able to issue movement commands by pressing a button which causes the server to initiate a Command Block (see Section 3.4.2) and begin receiving data from Cortex. After a specified duration (4 seconds by default), data collection ends and the collected data is processed to determine the final command output for the block, which is sent back to the client-side where the command is executed by moving the user's position on the grid. The user's position in the grid is always indicated by an orange circle the covers the currently occupied grid point (see Figure 3.9), and an orange *trail* shows the path that they have travelled from the

starting position. Movement in the grid is limited to moving by one grid unit at a time in one of four directions (*up, down, left,* or *right*), and it is not possible to visit a previously-visited node (i.e., the path cannot overlap itself). This constraint was added to ensure that the visual feedback of the trail would remain simple and clear.

If the user chooses to create a new password, a password is randomly generated consisting of a starting location and a series of directional commands. A guide is rendered on the grid (Figure 3.9) showing the correct sequence of moves from the starting location. The user must then practise entering their password twice with the guide, after which the guide is hidden and the user must enter the password twice without it in order to ensure memorization. Password entry is accomplished by entering a series of BCI mental commands and then clicking a *Submit* button, which causes the entered sequence to be compared against the correct one to determine whether the user has successfully authenticated. If they are successful, their newly created password is stored in the password database along with their unique ID. If the user chooses to try to enter a previously-created password, the interface is the same except that there is no guide. The user can enter commands and then click *Submit* to check whether they have entered the correct password, which is indicated by a text message that appears in the interface as well as a change of the colour of the primary position indicator (blue for correct, red for incorrect). After a brief delay, the grid is automatically reset to the initial state.

3.4.2 Command training and input.

Emotiv[57] provides an application, EmotivBCI, which is used to train mental commands. The main interface of EmotivBCI is shown in Figure 3.6. A user can select up to four commands to train in addition to the *Neutral* state. The training interface is shown in Figure 3.8. The user must decide on a reproducible mental

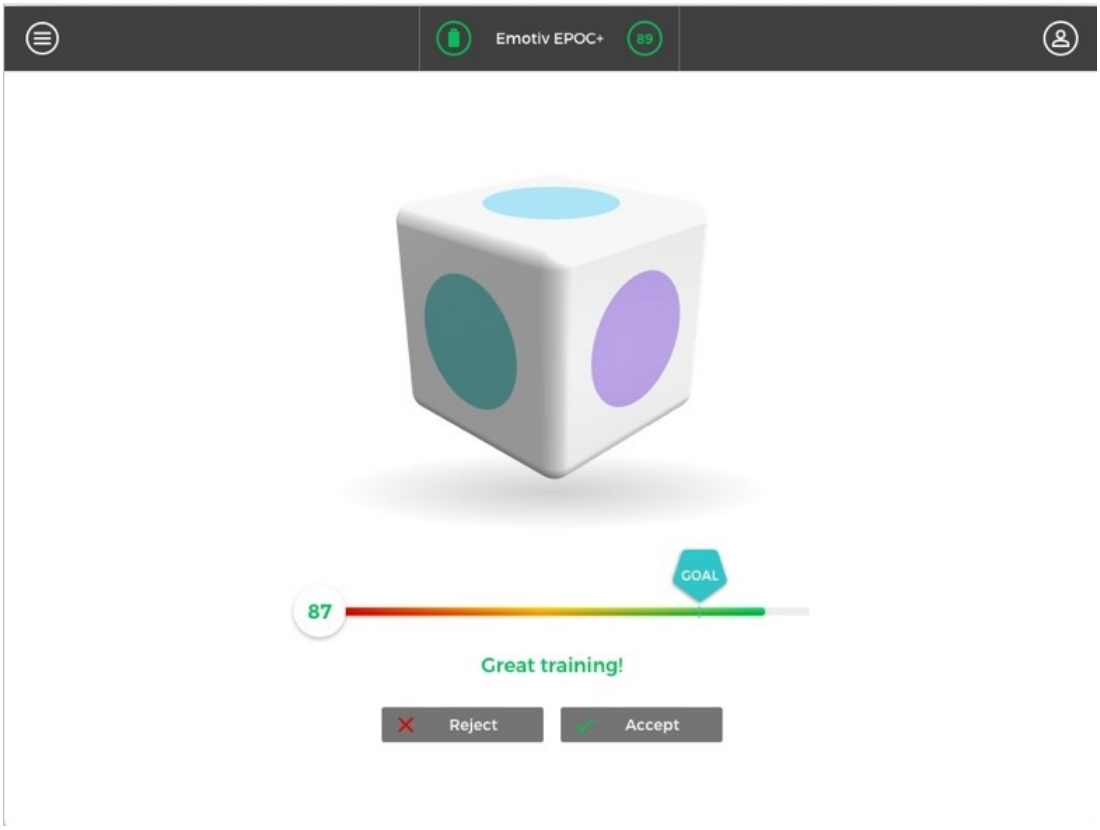

Figure 3.8: Command training interface of the EmotivBCI application. The cube in the center moves during training to indicate the strength of the detected command. A numeric score is given at the end of each training, based on which the user is asked to accept the session and use it to train the classifier or to reject the session and discard the data. Reproduced from Emotiv Inc.[57]

task to associate with each command. The EmotivBCI application is essentially a graphical wrapper around the mental command training API methods available through Cortex.

During training, users are asked to engage in this mental activity continuously for 8 seconds, during which feedback is provided by the cube moving according to the command (e.g., moving up in the case of the *lift* command). At the end of the training block, a score is given for the session indicating the quality of training and the user must choose to accept or reject the session. A *Goal* value is shown and the user is encouraged to only accept training sessions that score above the threshold. The Goal value is lowered as the user adds additional commands to their profile. A collection of trained commands is stored as a *training profile* which can be imported through the Cortex API to be used in external applications.

Thirteen commands are available and can be trained using the Cortex API, however only four of these are used in our application: *left*, *right*, *lift* (which is interpreted as an "up" command), and *drop* (which is interpreted as "down"). The mental task to associate with each command and does not need to be related to the movement direction or command in any way; it needs only to be reproducible.

In my BCI authenticator application, movement commands are issued in discrete steps called *Command Blocks*. A user initiates a Command Block by pressing the *Spacebar* key. This begins a period of data collection from the headset for a specified duration (which defaults to 4 seconds), after which the collected data is processed to determine a final output command for the block which is executed in the interface.

In order to read data from the headset, a Cortex[171] `session` is created. This begins a period of data collection, however no data is transmitted until a `stream` is added to the `session` using the `subscribe` API method. A number of data

streams are available that can be accessed using `subscribe` such as raw EEG values, frequency band power, or motion sensors. In this case, the application subscribes to the `com` stream to receive mental command events,which begin streaming over the websocket. Mental command events consist of a JavaScript object with two attributes `act` and `pow` which correspond to the name of a mental command and the *power* at which it is detected, respectively. The cumulative power associated with each command is tracked during the command block and stored in a JavaScript object. At the end of the command block, the accumulated data is processed to determine the command with the highest total power which is then designated as the final output for the block and passed back to the client-side to be executed in the user interface.

3.4.3 Cortex API.

The Emotiv Cortex API[171] exposes a websocket on the local system. Communication over the socket takes for form of JSON-RPC messages passed as requests and responses as well as streams that send continuous data from the device. The Cortex API is asynchronous; however, for many operations a strict sequence must be followed. For example, to read a data stream from the device, the following steps must be followed in order: (1) open the websocket connection, (2) authenticate using an API key, (3) receive and store an API token, (4) create a session to initialize a data stream from the device, (5) subscribe to the EEG stream. Each step relies on the result of the previous (e.g., the API token which is returned from the authentication step is required in order to open a session; the session ID is then required to open a stream). In order to handle asynchronous API communication while maintaining, when needed, strict control of the order of events, the API wrapper class (`Cortex`) makes heavy use of JavaScript `Promises`[178] and `Promise` chaining.

The `Cortex` class is built around one method, `call`, which accepts as arguments `method`: the name of a Cortex API method (a string), and `params`: a set of parameters for the method (a JavaScript object) and returns a `Promise`.[178] Within the `Promise`, the `call` method constructs a JSON-RPC object with the `method` and `params` data as well as some metadata and sends it to the API over the websocket. A listener is added to the websocket which will capture the response to the request and pass the result back to the calling scope by resolving the `Promise`. Wrappers for various API functions are implemented as special cases of `call`. For example, the class method `authorize` essentially constructs a `params` argument with the appropriate credentials and passes it to `call` along with `method = ‘‘authorize’’`.

3.4.4 Grid interface.

The user interface is shown in Figure 3.9 and consists of the following components:

- A backdrop canvas with a grid of black dots.
- An orange circle overlaying one of the grid points indicating the user's current position in the grid.
- An orange *trail* beginning at the start position and following the path that the user has moved through the grid.
- A grey *guide* which indicates the correct path to follow (only in password creation mode)
- Instructions which are presented at the top of the interface above the grid.
- Clickable UI buttons for various functions such as “Submit Password”, “Undo Move”, “Reset”, “Quit”.

The client-side user interface is implemented using the `Snap.svg` NodeJS library[179] for vector graphics. A `Grid` JavaScript class is defined that handles rendering and animating the grid interface, as well as providing helper functions for various calculations including the generation of random passwords.

The `Grid` class accepts a variety of arguments to modify aspects of the interface. The width and height of the grid (in pixels), number of nodes on the X and Y axes, duration of command blocks, and animation delay can be set explicitly by providing appropriate arguments to the class constructor. These variables have reasonable default values if no arguments are provided.

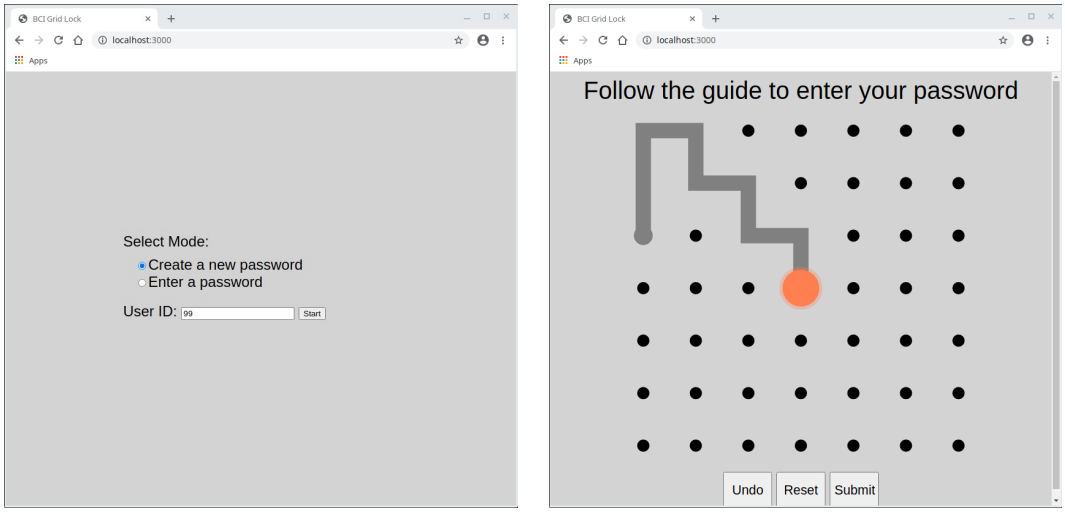

Figure 3.9: The main menu interface of the authenticator (*left*) and the *Create mode* interface (*right*). In the main menu, the user is asked to enter a unique ID which corresponds to a particular password. The user can choose to enter Create mode, creating a new password to associated with the ID or overwriting an old one, or Enter mode, where they can practise entering their previously enrolled password. The Create mode interface presents a system-generated password (shown as a grey line) which the user is asked to enter using Command Blocks with the BCI device. Enrolment is complete once the user has entered the password correctly twice with the guide and twice with the guide hidden. The interface for *Enter mode* is identical to that of Create mode except that the grey guide line is always hidden.

When the interface is initialized, a setup function renders the static components of the interface which comprise the backdrop and the nodes of the grid, as well as the static UI buttons. As the nodes are generated, their exact pixel locations are stored in a two-dimensional matrix such that their index in the matrix corresponds to their coordinate position on the grid (i.e., to find the pixel coordinates of the node located at $X = 2$ and $Y = 3$, access the node matrix at index `[2, 3]`). Next, the dynamic components are rendered including the coloured circle that represents the user's current position, the path trail, guide, and instructions. At this point control is given to the user who can begin issuing movement commands.

The password generation function is implemented as a two-dimensional random walk with the constraint that a given node cannot be visited more than once. A two-dimensional matrix is initialized with the same dimensions as the grid. The starting node is determined by an argument to the function: *random*, which selects a point on the grid at random; *center*, which selects the point closest to the center of the grid; or a custom start location in the form of an array of two integers corresponding to X and Y. From a given node, the four movement directions are checked to determine whether they would result in a valid position, i.e., that the node has not previously been visited and does not exceed the bounds of X or Y. In the case that no movement options are valid, the current node will be designated a *dead-end* and the position will backtrack by one step to take a different movement option. A counter tracks the number of steps (and decrements according to backtracking) until the desired password length is reached (the default length is 8 steps).

Assuming the starting position is not adjacent to an edge, there are four possible choices for the first step. For every step thereafter, there are at most 3 choices because the previous position cannot be repeated. The password space is therefore at most $4 \times 3^{n-1}$, but this is idealized given the constraint that the path

cannot overlap itself. A sequence of length 8 would allow at most 8748 unique paths, which is slightly less than a 4 digit PIN at 10^4 or 10,000. If Command Blocks were to take 4 seconds each, it would take 32 seconds to enter, assuming no mistakes. On its own, the pattern component of the passthought system offers an abysmal value in terms of both usability and security. The password space of the system is a significant limitation, but one I considered acceptable for this prototype because the focus of the design was on the multifactorial element of passthought authentication. If this iteration of the prototype were to demonstrate that the mental command graphical password idea is feasible, it would be worth revisiting this part of the implementation.

3.4.5 Using the application.

The process for setting up the application, enroling, and entering a mental command password are illustrated in Figure 3.10. The local webserver that provides the application must be started beforehand. The user can connect to the server with a web browser on the local network. The main page of the application is then loaded, which contains a field in which to enter a numeric ID and a menu to select whether to create a new password to associate with the ID (*Create* mode) or to attempt to enter a previously created password (*Enter* mode). The user is not able to initialize *Enter* mode if a matching ID is not found in the database.

To enrol in the system, the user enters their numeric ID and selects the "Create a new password" option. The main interface is rendered (right side in Figure 3.9) and a generated password sequence is drawn over the grid indicating the user's assigned password. At this point the user can begin issuing BCI movement commands using *Command Blocks* (described in Section 3.4.2) to move their position indicator through the grid. In order to complete enrolment, the user must successfully navigate through the assigned path (and press the *Submit* button) twice

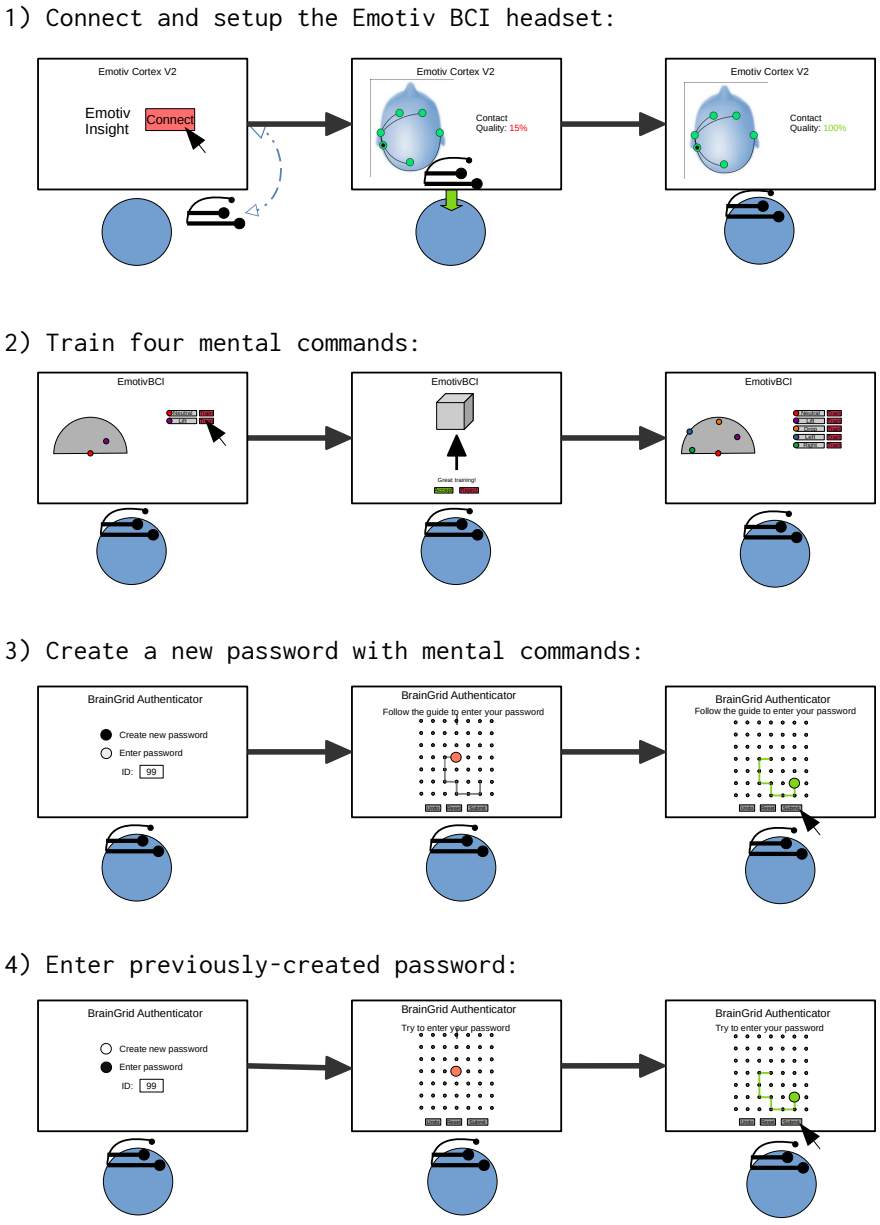

Figure 3.10: A walkthrough of the usage of the application, including the initial setup and training of a mental command profile in EmotivBCI.[171]

with the guide, and twice again with the guide hidden to ensure memorization. In addition to the *Submit* button, the user can use the *Undo* button to undo their last movement command or the *Reset* button to reinitialize the interface to its initial state.

To enter a password, the user enters their ID and selects the "Enter a password" option. The interface is identical to that of *Create* mode except that no guide is available and only one session is performed. The user can issue movement commands and attempt to enter their password. If the user submits the correct password, the indicator circle and trail turn green momentarily to signal success and the application returns to the main menu. If the password is incorrect, the indicator and trail turn momentarily red and control is returned to the user. Currently there is no limit on the number of incorrect attempts allowed or amount of time taken, so the user may continue attempting to enter their password until they succeed or close the application.

3.5 System Evaluation

I designed a simple evaluation study to evaluate the feasibility of the authenticator prototype using motor-imagery-based mental commands with BCI-naïve participants. The usability study as described below was approved by the Carleton University Research Ethics Board (CUREB File No. 111922, see Appendix A for details), but was delayed and ultimately not completed due to various complications described below (Section 3.5.3). The rationale and methodology of the proposed study are discussed next, followed by a description of the obstacles that were encountered and the outcome of the project.

3.5.1 Feasibility Study Design

The primary objective of this study would be to determine whether the authenticator fulfilled the requirement of usability. In other words, would it be possible for someone who has not used the application before to train a command profile,[171] enrol in the system with a new password, and then successfully authenticate with their password after some amount of time? Therefore the proposed study would be meant to assess the memorability and *enterability* of passthoughts based on mental commands.

To answer this question, I would have participants enrol in the system with three fictitious accounts and then attempt to enter them after being briefly distracted by a mental rotation task.[180]

Participants

The participants for the proposed study would comprise at most 40 students from the Carleton University community who are over the age of 18, have normal or corrected-to-normal vision, and are comfortable wearing a lightweight ($<$ 1 kg) device on the head for one hour. Participants would be recruited using posters placed around the university campus as well as postings to student social media groups. The expected duration of the study would be 60–90 minutes, and participants would be compensated with $15, even if they withdraw without completion.

Procedure

Participants would be given a consent form (see Appendix A) prior to beginning any study procedures which would explain the goal of the study, what to expect, and that they may choose to end the study at any time without loss of compensation. As BCI devices are not common among the general public, participants

would be given an opportunity to familiarize themselves by asking questions and handling the device, and they would be informed that they may pause the study to ask questions or for help at any time. The experimenter would remain in the room with the participant through the duration of the study.

A brief demographic questionnaire (see Appendix A) would be used to learn about the general traits of the sample including age, education level, field of study/work, frequency of computer use, whether they have used a BCI before, and whether they have been previously advised of any significant neurological conditions. The demographic questionnaire would be implemented as a web form running on a local laboratory server.

After completing the consent and demographic questionnaire forms, the participant would be asked to place the BCI device (an Emotiv Insight[57]) onto their head and follow the on-screen instructions in the EmotivBCI training app (Figure 3.6) to position the headset correctly and with good contact quality. If there is any difficulty during this stage, the experimenter would ask the participant whether they are comfortable with the experimenter adjusting the device on their head and, if so, proceed to do so; otherwise the experimenter would attempt to provide guidance and instructions to aid the participant in finding the ideal positioning. It is anticipated that some sessions would not progress past this phase as some types of hair can present significant difficulty in establishing good contact.

Training: Once contact had been established, the participant would be asked to train four mental commands using EmotivBCI[171] (*left, right, lift (up)*, and *drop (down)*) as described in Section 3.4.2. The four commands and the neutral state would be trained according to Emotiv's recommended procedure,[171] which suggests beginning with a single command and adding additional ones to the profile only when all currently-trained commands can be produced reliably. The training

phase would continue until one of the following conditions are met: the participant has achieved reliable control of the four movement commands, each command has been trained more than 20 times, or 45 minutes has passed. Ample time is alloted in this step to afford the participant taking breaks and as a precaution against complications such as losing signal quality and having to adjust the headset. It is expected that some participants would be unable to complete the training stage within the alloted time.

Enrolment: Participants would be asked to create three passwords for fictitious online accounts (*Social Media, Online Shopping, Online Banking*). Three account IDs would be provided to each participant which correspond to the accounts in a text file; the participant would not be required to memorize the account IDs but would be asked not to write their passwords down in any way. To create a new password for an account, the participant must enter the corresponding ID on the main menu of the authenticator and select *Create a new password.* The interface is initialized and a new password is randomly generated consisting of a series of eight commands which is overlaid as a *guide* over the grid (Section 3.4.4, Figure 3.9). Enrolment of a password is complete when the participant successfully uses BCI commands to enter the password twice with the guide and twice without it.

Mental Rotation Distractor Task: Participants would be asked to complete a mental rotation task[180] as a distraction. This is done to prevent the participant being able to rehearse their password between the enrolment and authentication stages.

The mental rotation task would be conducted using an implementation in PsyToolkit[181] on the same computer as the rest of the experiment. Briefly, a white target shape is presented in the top half of the interface and two potentially

matching shapes are shown in red below (shown in Figure 3.11). One of the target shapes is a rotated version of the target and the other is a similar but non-identical shape. The participant is asked to click on the shape that matches the target and are given feedback about whether they are correct or incorrect. The PsyToolkit mental rotation implementation outputs a data file containing the results for each trial, but this data would not be retained or used as the results are not of interest for the assessment of the authentication system.

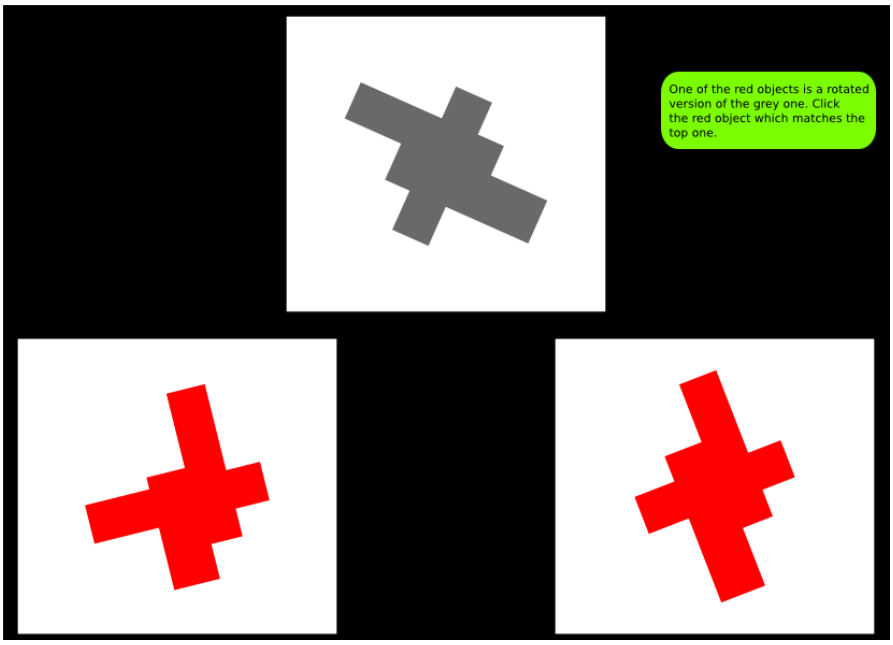

Figure 3.11: An example of the mental rotation task used as a distractor task in the evaluation study. The participant is asked to decide which of the red shapes are a rotated *match* of the grey shape. Reproduced from PsyToolkit.[181]

Authentication: After the distractor task, recall of the mental command passwords would be tested by having participants input their passwords without a guide. Participants would enter each of their previously-created passwords by entering the ID associated with the account and selecting the *Enter password* option on the main menu. The order in which they enter the passwords would be unconstrained. The password entry process is described in greater detail in Section 3.4.1.

The system would be instrumented to record events to a log file including commands, *undo* actions, correct and incorrect submissions for later analysis.

Analysis: The primary outcome of interest is whether password entry is successful, the amount of time taken, and the number of mistakes (i.e., issuing the wrong command either due to misremembering the sequence or the system misterpreting the user's intent) that occur during the password entry session. The study design does not include any conditions or groups, so the data analysis would be straightforward. Due to the exploratory nature of the study, no concrete hypotheses were generated. An ideal outcome would have all or nearly all participants able to enter their three passwords with something like 80% or greater accuracy, but it is unlikely that the system would achieve such a result without significant testing and refinement. Results would be examined to identify problems and barriers, and to determine areas for improvement for the application.

3.5.2 Pilot and Obstacles

The evaluation experiment began with a pilot in order to ensure that it could be completed in its entirety. Five members of the HotSoft lab group volunteered to go through the experimental procedure without compensation. Despite our best efforts and numerous attempts, no participants were able to progress past the training phase by successfully training four mental commands in the EmotivBCI application. Training sessions lasted between 30 and 90 minutes, and several of the participants volunteered for multiple of these sessions over several days to experiment with different approaches.

First Approaches:

For the initial attempts, participants were instructed to use motor imagery tasks as their directional commands with movement with *up* associated with movements of the face, mouth, or tongue, *down* with movements of the feet, and *left*, and *right* with movements of the left and right hand respectively. All participants were able to successfully train and use one command (demonstrated by issuing the command reliably in EmotivBCI *live mode*[171]), but significant problems arose when the system was required to discriminate between multiple commands. After training a second command, the previously trained one would become very difficult or impossible for the user to produce. It was noted with several participants that when testing commands in EmotivBCI's *live mode*, the application would strongly detect the most recently added command even when the participant was not intending to issue a command at all.

A number of slight modifications to the approach were tried but yielded similar results, described here:

- Stepwise training. Rather than training a single command until proficiency before moving on to another, participants tried training commands in sequence starting with *neutral state* training followed by one training session for each of the four directional commands and then beginning again with neutral (e.g., neutral, left, up, right, down, back to neutral and repeat).

- Covert spatial attention. Deviating from the motor-imagery paradigm, participants were instructed to use covert spatial attention,[182] in which they focus their spatial attention up, down, left, or right relative to a central point without moving their visual focus. This method has been reported as a viable alternative for those who are unsuccessful with the motor imagery approach.[182]

- Open-ended mental tasks. Participants were instructed to try any mental activity of their choosing to associate with a mental command. Some of the strategies that were used included imagining sensations of taste or temperature, recalling a specific visual scene or the tune of a song, and imagining complex motor activities such as swimming or playing a musical instrument.

- Body movement. Instead of a purely cognitive task, participants were instructed to engage in real (i.e., not just imagined) movement of their limbs to the extent possible without disturbing the EEG signal.

- Combinations of the above approaches, e.g., body movement for *up* and *down* commands and covert spatial attention for *left* and *right*.

- Accepting *bad* training sessions. Rather than rejecting all training sessions that do not meet the recommended threshold (see Figure 3.8), participants chose to accept or reject sessions based on their own perception of how well they were able to hold their command task in mind.

- Upgrading to the Epoc. Given the lack of success using the Insight, the training procedure (including many of the modifications discussed here) was attempted again using the Emotiv Epoc,[57] a BCI headset with 14 EEG electrodes in contrast to the Insight's five. The Epoc offers a performance—usability trade-off, as the setup process takes significantly longer and the additional sensors offer increased points for potential failure.

- Alternative sensor placement. Using the Epoc, the headset was adjusted such that the cluster of sensors that normally sits over the frontal part of the skull were instead positioned rearward, over the sensorimotor cortex. This was aimed at improving detection of sensorimotor rhythms associated with motor imagery.

These approaches had mixed results across participants. For example, imagining the movements and feelings associated with swimming in cold water worked particularly well for one participant, whereas another was successful by miming a piano melody with their hand against the desk. Regardless of the level of success achieved in training individual commands, all of the approaches that were tried suffered from the same failure when attempting to train more than one or—at best—two commands.

Mental fatigue and signal stability seemed to have significant impacts on performance in our sessions. In particular, all participants noted that issuing mental commands became significantly more difficult over the course of longer sessions (i.e., 30 minutes to 1 hour). Taking breaks, however, was also problematic as longer breaks of several hours or a day were associated with increased difficulty issuing commands when returning. A further difficulty stemmed from the fact that Emotiv's API[171] and other applications are closed-source and many critical internal components are not documented. For example, Emotiv does not provide significant detail regarding their classification algorithm, it's class and structure, or how data are pre-processed before being fed into the classifier. This fact made it difficult to understand how to go about altering the training protocol to achieve better results. The training feedback that is provided at the end of each training session is vague (e.g., *Great training!*, or *Not so great, maybe try again?*) and is difficult to interpret in terms of how to improve training or even the metric that is being assessed.

Also, anecdotally, the semi-circular display in EmotivBCI which is meant to show the distinctiveness of each trained command (see Figure 3.6) was found to be unhelpful because it is not clear how this metric is computed, and it did not appear to correspond with the observed performance of the classifier. In other words, the classifier would still fail to detect to correct command even when the

visualization suggested they were sufficiently distinct from one another and from the neutral state.

Reimagining the evaluation study

After having spent three weeks attempting to achieve satisfactory command discrimination using the approaches described above, it was clear that the system was not workable as implemented. I began considering how to work around this limitation in the next iteration of the prototype.

Notably, while the four-command classifier required by the prototype appeared to be out of reach, it seemed relatively more feasible to establish a reliable two-command classifier, which raised the possibility of a mental command password system based on two commands. Indeed, I confirmed that it is possible to use only two mental commands (such as *up* and *left*) to draw a simple pattern on the grid interface in a sort of *staircase* pattern. However, using only two movement directions with an interface designed to support up to four is unintuitive and not particularly parsimonious; it would be reasonable to give some thought to an alternative front-end interface that be more appropriate for a two-command system. For example, a visual metaphor based on leftward and rightward rotation, perhaps resembling a combination padlock, might be suitable.

Another consideration for a two-command system is that of the sequence length. In order to achieve a similar possibility space to a four-command sequence of length 8 (approximately 13 bits), a two-command system would require 13 steps. It is possible that the duration of command blocks in the two-command system could be shorter than in the four-command system, which could possibly offset the increased number of steps required.

Another possibility was to salvage the experiment by *spoofing* the BCI input, bypassing the problematic training phase altogether. Training would be faked by

disabling feedback for a set number of training sessions. A modification was made to the authentication software to accommodate faked *Command Blocks* which will output either a correct or incorrect movement step based on an experimenter-chosen selection function. This process would allow investigation of the role of error-rates in determining user perceptions of the usability of passthoughts based on mental commands. This approach would enable evaluation of passthoughts that is unaffected by the actual performance of BCI systems.

3.5.3 Outcome

In mid-March of 2020, on-site research activities at Carleton University were suspended due to the ongoing COVID-19 global health crisis. This situation has made it impossible to pursue further testing with study participants or lab volunteers for the foreseeable future. Work on the in-person component of project has been indefinitely postponed pending a return to normal research activities.

A few lessons were learned while conducting the system evaluation study and are described here. Firstly, the difficulty of developing applications to interface with consumer BCI devices is compounded when important details of the internal functioning of the hardware are undocumented or obscured, such as the structure of the mental command classifier or data preprocessing steps that are used in the Emotiv devices. In hindsight, a more flexible solution such as OpenBCI[58] seems like a better approach. Additional effort would be required to develop some of the tools that are available out-of-the-box with Emotiv BCIs (such as a machine learning classifier for mental commands), but this cost may be offset by greater insight and a more accurate mental model of the behind-the-scenes functioning of the application, as well as the ability to modify it as needed.

Further, mental command training is complicated by the interplay of two factors: cognitive fatigue and EEG signal stability. Training mental commands in

EmotivBCI is a cognitively demanding task which requires sustained focus over long periods of time. As participants train commands, they gradually become more fatigued (and potentially frustrated), making it progressively more difficult to reproduce the specific EEG patterns required to generate commands. Cognitive fatigue acts as a sort of *soft ceiling* for the duration of mental command training sessions. A further complication is that EEG patterns are not stable over time, meaning that a user could load a mental command profile that they had successfully trained days or weeks ago to find that their commands are no longer recognized. These factors suggest that an ideal training paradigm would involve sessions that are short (ending before the onset of fatigue), but frequent (without opportunity for non-stationarity of EEG to significantly degrade peformance). The downside of this approach in a research settings is that we usually have access to participants for an hour or two at a time, and having them return over subsequent days is probematic for a number of reasons.

3.5.4 Future Directions

A number of possibilities exist to continue or extend this work. A great deal of the difficulties experienced in this project were due to the restrictive nature of the proprietary Emotiv ecosystem. Ideally the authenticator would be hardware-agnostic and be able to support any of the major BCI hardware/software stacks in a modular fashion. In the short term, adding support for OpenBCI[58] seems like a good first step as it is the most open and configurable BCI platform that I'm aware of.

The fact that the authenticator uses live visual feedback compromises the *unobservability* quality of passthoughts. An observer could simply watch the computer screen and easily capture the sequence of directional commands that comprises the

user's password. Practically speaking, the multifactorial nature of the authenticator should prevent this being a significant issue, since knowledge of the command sequence alone is not sufficient to authenticate: the attacker would also need to be capable of producing the appropriate EEG states that are recognized by the classifier, which are biometrically specific to the victim and based on specific mental activities which are themselves unobservable. Still, this is a vulnerability which could be remedied by adding a feedback-less mode that enables authentication without revealing the passthought sequence. I envision a system whereby novice users of the system can gradually reduce their reliance on visual feedback as they gain experience and practise with the system, eventually removing the feedback altogether once they achieve some degree of proficiency.

It is clear from attempting the evaluation study that mental command training is a much more difficult and time-consuming process than was initially assumed. Moving forward, a new solution for training study participants for with Emotiv mental commands must be developed. The niche nature of BCIs makes it very difficult—if not impossible—to locate potential participants with any prior BCI experience for in-person studies. The simplest solution would be to have participants return to the lab over subsequent days to engage in extended training sessions, allowing sufficient time for them to become proficient with mental commands. However, even disregarding cost and participant attrition, the level of time and effort required to arrive at a trained mental command classifier is a substantial blow to the usability of the system.

It may also be worth addressing the context in which the passthought system might be used. Based on the findings presented here, it seems that mental command passthoughts cannot hope to achieve rapid entry comparable to other authentication methods like text passwords or fingerprint biometrics, which usually take a few seconds at most. Therefore, this type of passthought system doesn't

seem well suited for authentications that are frequent and/or trivial, such as unlocking one's mobile phone or entering an administrator password on a computer. The theoretical high-security but slow entry of mental command passthoughts seems most appropriate for infrequent but high-value authentication situations, such as taking out a substantial bank loan or altering one's last will and testament.

Chapter 4

Brain-Computer Interface Expert Interview Study

The usability of passthought authentication has received only a little attention[18–20,134,183] relative to that of BCIs in general. Chapters 4 and 5 describe my attempts to elucidate factors relating to the acceptance of BCIs and passthoughts using qualitative (Ch. 4) and quantitative (Ch. 5) methods.

In order to qualitatively assess these questions, I conducted semi-structured interviews with BCI enthusiasts and BCI researchers recruited through online BCI-related forums and via direct email. For this study, I defined the research questions as follows: *What are the main barriers preventing adoption of BCIs and passthoughts for the general population?* A reflexive thematic analysis[184,185] (RTA) approach was used to analyze the interview data and derive general themes related to the research question, which led to the identification of three general areas for improvement: the perceived safety of BCI devices, usability of BCI devices (including difficulty with use as well as physical and psychosocial comfort), and the need for continued research and development to identify viable use-cases for BCIs.

4.1 Background

Chuang et al. [18] conducted, to my knowledge, the first passthought system study with an explicit emphasis on usability. In addition to minimizing the hardware burden by using a single-channel EEG-based BCI headset, the authors had participants use a series of seven different mental tasks (e.g., simulated finger movement,

song recitation, focus on breathing) for authentication. Participants were asked to rate the tasks according to difficulty and enjoyment, as well as to indicate which task that they would most likely be willing to use on a daily basis. Results of the study supported the proposal that strong authentication could be achieved with a minimal (single-channel) BCI, and also indicated that users have heterogenous preferences for passthought tasks in terms of both enjoyment and perceived difficulty. Other passthought usability studies are limited in that they either do not directly assess usability[134,183] or are focused on specific populations with special needs, such as users with visual impairments.[19,20]

Yang and Deravi [186] conducted a survey of EEG-based passthought systems and attempted to compare usability across studies based on four factors: the number of users that the system is meant to be used for, number of electrodes, duration of enrolment, and duration of authentication. Unfortunately, it is not clear how these factors were derived (they appear to reflect the authors' assumptions about what constitutes a usable passthought system rather than having an empirical basis), and none of the assessed studies included actual reports of usability involving the participants. Therefore it is difficult to determine whether the four factors described by Yang and Deravi [186] truly relate to the end-user's perception of usability in any meaningful way.

The present study takes a significantly different approach relative to other passthought authentication studies. Rather than BCI-naïve participants or individuals with specific impairments that are recruited in other studies, I targeted an expert population—BCI researchers and enthusiasts—who have significant knowledge and firsthand experience with BCIs. Especially given the finding that typical consumers hold incorrect beliefs about biosensors, particularly around neurological data,[157] it is of interest to learn to opinions of individuals who have a more accurate view of the technology and its applications.

4.2 Methods

4.2.1 Participants and Recruitment

I conducted an online search to identify BCI-focused online communities using Google search engine, as well as the community-based content aggregation and discussion platform Reddit. Few such communities were found, which was unsurprising due to the uncommonality of BCIs among the general population. I identified the NeuroBB[187] forum and the Reddit page *r/bci*[188] as suitably active communities with somewhat large user bases that could be used for recruitment. I made accounts on both sites and started threads with the following text:

> My name is Josh Carr and I'm a researcher at Carleton University in Ottawa, Canada studying BCIs. For my Master's thesis I'm conducting a study about BCI authentication. As part of this, I'm hoping to conduct interviews with some users and/or researchers about their thoughts and opinions about privacy, cybersecurity, and authentication with regard to BCIs. In particular I'm interested in discussing non-invasive commercial BCI devices (i.e., Emotiv, OpenBCI, Neurosky, Muse) that are used in a non-medical context.
>
> The interview would be done over the phone or via Skype and would last approximately 1 hour. All data collected from the interview will be anonymized and stripped of any information that could potentially be used to identify you. You must be over the age of 18 to participate. If you are interested in participating, please contact me by email at josh.carr@carleton.ca or send me a private message through [Reddit/NeuroBB].

> The ethics protocol for this study has been reviewed and cleared by the Carleton University Research Ethics Board [CUREB-B Clearance # 111922].
>
> Thanks for reading!

Overall, only three participants were recruited using this method, two of whom reported that they found the study through NeuroBB and the other from Reddit. After two weeks with little interest, a different approach was devised. A demographic group that would have experience with BCIs and would likely be willing to discuss their experiences is BCI researchers. I identified a number of researchers who had published studies on topics related to BCIs, BCI usability, and BCI authentication. Details of the researchers and the works I reviewed to identify them are not presented here to preserve anonymity. Emails to researchers were semi-personalized, specifically referencing their related work, in order to increase the likelihood of a positive response. I was able to recruit four additional participants using this direct-contact approach, for a total of seven interviewees. For anonymity, participants were assigned an ID based on the order in which the interviews were conducted, i.e., *P1, P2, ... P7*.

4.2.2 Interview Guide

Interview question were developed using a bottom-up approach starting with brainstorming sessions. The goal was to develop a series of high-level topic questions to get interviewees talking, and a series of potential follow-up questions for each topic that could be used to elicit more information. The interview guide is not meant to be exhaustive; the interviews are semi-structured and are meant to permit deviation from the interview guide to follow any interesting threads that

may emerge. Not all of the items would necessarily be asked for each interview depending on the flow of conversation.

Candidate questions were developed in a brainstorming session based around the research question. No topic structure was defined beforehand so as not to bias the brainstorm. A number of items were derived, several of which were then removed and combined with others to reduce redundancy. The questions were then arranged into groups based on common themes, from which five main topics emerged: basic information about the interviewee and their experience with BCIs, usability of BCIs, physical and social comfort of BCIs, privacy concerns about BCIs, and the use of BCIs for authentication. With the topic structure defined, a second round of brainstorming was conducted to determine additional follow-up questions for each topic. The finalized list of interview questions is presented in Table 4.1.

Table 4.1: The finalized interview guide with 24 question items grouped into five topics.

#	Topic	Question
1	Basic Information	In what capacity do you have experience with BCIs? As a researcher, a casual user, or something else?
2		What types/brands of commercial BCIs do you have experience with? (e.g., Emotiv, Muse, OpenBCI, Neurosky)
3	Usability	Generally speaking, how do you feel about the performance of BCIs? Do they live up to your expectations?
4		Do [you/users] ever become frustrated when using BCIs? Why?
5		Do you have any experience training mental commands (e.g., with motor imagery)? Were you successful? What challenges did you encounter?

6		Have you successfully used a BCI to accomplish a task? Describe your experience.
7		Are BCIs usable enough for real-world applications? What are the most significant barriers? Will they become usable enough at some point in the future?
8	Comfort	What do you think about the physical comfort of wearing BCI devices?
9		Does the comfort of wearing a BCI change over the course of a session?
10		Is it necessary to take breaks and remove the device due to discomfort or fatigue? How frequently?
11		What about the appearance of the device?
12		Would you feel comfortable using a BCI in public or in the presence of strangers?
13	Privacy	What do you think about the privacy implications of using BCIs?
14		Concerning the BCI devices that you have used, are you familiar with the manufacturers' privacy policies?
15		Do you think that someone with access to BCI data could use it to learn private information about the user? What sort of information do you think they could learn?
16		Do you take any precautions to protect [your/users'] BCI data? What kind of precautions? How effective do you think they are?
17		Would you be willing to allow the BCI manufacturer or a third-party company to collect data from your BCI device in exchange for additional features or services?

18		Should BCIs be considered a major privacy concern relative to other new or emerging technologies?
20	Authentication	Have you ever tried to use any type of authentication (e.g., entering a password) using a BCI?
21		What do you think about BCI biometric authentication, similar to using your fingerprint or iris?
22		Would you feel comfortable with the level of security offered by such a system? Why/why not?
23		Given our incomplete understanding of neurophysiology, do you think there are likely to be as-yet-unknown security vulnerabilities associated with passthoughts?

4.2.3 Procedure

Interviews were arranged over email and conducted remotely using videoconferencing software. Each participant received an email containing a consent form which outlined the goals and procedure for the study, and were asked to reply to that email explicitly stating that they have read the consent form and whether they agree to participate. The videoconferencing software was not the same for all interviewees, and was decided based on the interviewee's preference and convenience. All interviews used one of Skype, Discord, Zoom, or Microsoft Teams. Participants chose whether to enable video for the call but no video was recorded or retained. The length of interviews was between 30–50 minutes. The audio from each interview was recorded and then later used to take detailed notes which would be used for thematic analysis (see Section 4.2.4). After each interview, the participant received an email with a debriefing document which reiterated the

goals of the study and provided contact information for the researcher and research supervisor.

4.2.4 Analysis

Reflexive thematic analysis (RTA) was used to interpret the interview data as described in Braun et al. [185]. The process is described here, but specific results (i.e., the generated codes and themes) are discussed in Section 4.3. Firstly, data familiarization and transcription took place in a single step. Rather than fully transcribing the interviews, extensive notes were taken which included verbatim quotes as appropriate. During this phase, a few ideas for codes were generated which were recorded to use as a starting point for the next phase, code generation.

During code generation, I reviewed participants' responses to each of the interview questions and assigned codes based on similar meanings in order to define a basic structure for the data. New codes were added liberally in order to fully capture the relevant meanings in the answers. Initially, codes were added to a list in a text file, without considering redundancy or sorting. After reviewing all of the interviews, the list of codes was reviewed, roughly sorted into categories, and reduced by combining or eliminating redundant items. This category structure became the basis for the construction of themes. The code generation process was repeated several times until no new codes emerged, indicating code saturation.

Themes were constructed out of codes with similar meanings by attempting to identify a central concept that would organize and contextualize the codes with respect to the research question. Firstly, the list of codes was reorganized such that similar items were grouped together in the list. This process yielded several groupings of items, which were then analyzed in order to define the theme that the grouped codes had in common. Theme construction was done iteratively: many ideas for themes were *tested out* against the codes before being disregarded

or refined into something else. The process of reducing and combining themes continued until a manageable number of themes remained (i.e., fewer than five).

4.3 Results

Five of the seven interviewees reported having a background in BCI research, and the remaining two were BCI enthusiasts with significant hands-on experience in a non-research capacity. Each participant listed the types of commercial BCI devices with which they'd had experience, shown in Table 4.2. All participants had experience with at least two brands of commercial BCIs. The Muse and OpenBCI devices were the most commonly used, followed by the Neurosky Mindwave and Emotiv devices. Three interviewees had experience using research-grade equipment (e.g., clinical EEG caps), and two had experience using custom or *do-it-yourself* devices.

Table 4.2: Frequency table showing the number of interviewees who reported having experience using each of several commercially-available BCI devices.

Device	n
Neurosky Mindwave	4
InteraXon Muse	5
Emotiv Epoc	4
OpenBCI	5
Research-grade	3
Other/Custom	2

After transcription and familiarization with the interview data, three iterations of code generation were conducted in order to fully extract the relevant meaning in the data. The complete list of unsorted codes is presented in Table 4.3. Note that the codes were intended to capture a specific view stated by the interviewees, and are somewhat conversational in tone.

Table 4.3: The unsorted list of codes generated from three iterations of the code generation procedure described in Section 4.2.4.

Code	
– BCI data is potentially more sensitive than other personal data.	– BCIs are less of a privacy concern than other types of data collection.
– BCI data can be aggregated with other personal data.	– Privacy paradox. (claim concern about privacy but engage in privacy-compromising behaviours)
– I don't care about BCI data being collected.	– BCIs will be used to marketing in the future.
– BCIs will probably be common in the future.	– BCIs aren't powerful now but will be one day.
– Privacy/security issues should be addressed before wider adoption, rather than later	– Performance of BCIs is disappointing
– Non-stationarity of EEG as a benefit	– Non-stationarity of EEG as a barrier
– Passthoughts could lock people out if they're not in the right mental state.	– BCI hardware is difficult to use
– BCI software is difficult to use	– Usability-performance trade-off
– The more usable BCIs can't do much.	– Muse has good user experience.
– OpenBCI is difficult, cumbersome.	– BCI device gets uncomfortable over time.
– Social stigma/aesthetics of BCIs.	– BCI engineering is impressive.
– Researchers have lower expectations of BCIs.	– BCIs could be used for surveillance of thoughts.
– BCIs could be abused by companies/governments to control employees/citizens.	– Military BCIs probably much more advanced that commercial ones.
– Average consumer can't make an informed decision.	– People have incorrect beliefs/expectations about neurological data.
– Comfort with BCIs requires strong privacy policies, data ownership.	– Lack of general understanding of neurological data (we don't know enough to know what the risks are)

– BCIs need to be perceived as less "creepy."	– Passthoughts for high-value (non-trivial) authentications
– BCIs have value and serve a purpose.	– We are in the early stages of BCI development.
– EEG data quality is low.	– The capabilities of BCIs are overstated.
– Low information-transfer rate.	– BCIs need a compelling use-case.
– BCIs are useful for neurofeedback/meditation training.	– BCIs are a novelty.
– Passthoughts are impractical for real-world use.	– BCI data could be used in a cyber attack.
– Haven't read privacy policy.	– Invasive BCIs are more impressive than noninvasive ones.

The first round of theme constructions yielded eight themes: data privacy, usability/difficulty, comfort, consumer protection, surveillance, performance, the future of BCIs, and BCI applications. Ideally, the number of themes would be further reduced; however, these eight themes do appear to reflect an important structure of the data. Rather than completely collapse the eight initial themes, I instead grouped them into three *meta-themes*: safety (comprising data privacy, surveillance, and consumer protection relating to BCIs), usability (including both technical difficulties as well as physical and psychosocial comfort of using BCIs), and development (comprising BCI applications, the future of BCIs, and BCI performance). These meta-themes are discussed in greater detail next.

4.3.1 Safety

Interviewees indicated that potential BCI users would worry that using a BCI might put them at risk in some way. Average technology consumers are not equipped to make informed decisions about BCI use and associated data collection, making them vulnerable to privacy violations or other abuses. In addition,

Table 4.4: The structure of the *Safety* meta-theme, including its three sub-themes and their respective codes.

#	Theme	Code
1	Data Privacy	BCI data is potentially more sensitive than other personal data.
2		Current BCIs are less of a privacy concern than other types of data collection.
3		BCI data can be aggregated with other personal data.
4		Privacy paradox. (claim concern about privacy but engage in privacy-compromising behaviours)
5		BCIs will be used for marketing in the future.
6		BCI data could be used to facilitate a cyber-attack.
7		I haven't read the privacy policy.
1	Surveillance	BCIs could be used for surveillance of thoughts.
2		BCIs could be abused by companies or governments to control employees/citizens.
3		Military BCIs are probably much more advanced than commercial ones.
4		BCIs need to be perceived as less "creepy".
1	Consumer Protection	Average consumers can't make an informed decision about BCIs.
2		People have incorrect beliefs and expectations about neurological data.
3		Researchers have lower expectations of BCIs than laypeople.
4		An average consumer doesn't know that you can't read thoughts with EEG.
5		Comfort with BCIs requires strong privacy policies, end-user data ownership.
6		The capabilities of BCIs are overstated.
7		BCI manufacturers restrict user access to data, including raw EEG data.

the complexity of neurological data and its proximity to inner thoughts and feelings is a source of uncertainty and discomfort. A number of these concerns were directly related to corporate data collection practises and associated risks of data breaches, selling of personal information, and data aggregation:

> P1: *"We can see where the trend is going . . . with big corporations and social media companies. And we are trying to build an alternative which is privacy-aware, because we can really see how this technology can be used to invade people's privacy at a mental level."*
>
> P4: *"I would treat BCI devices with utmost privacy. We must be very careful with any data related to people's genetics. The consequences of a privacy incident could be irreparable."*
>
> P6: *"Based on how everything works on the internet, I wouldn't be surprised if they record some level of data on you and sell something to someone. I'm very sceptical about companies that record data like that."*

In particular, it was emphasized that the privacy threats of data aggregation are largely unknown until long after the data have been collected. This could be the case to an even greater extent with BCIs than other forms of personal data collection due to the complexity and high-dimensionality of EEG data. The implication is that extra care should be taken with neurological data because we cannot expect to know in advance the degree of privacy-compromise that could occur in the event of a breach:

> P2: *"I think that Muse, with all the data they have of my brain, could probably profile me in some way."*

P3: *"It's not just neural data–all data! We don't know what it reveals until we've already collected it in aggregate. So it's an epistemic problem: we don't know what we don't know. What really concerns me is that there could be sources of bias that slip into the signal that we don't know about . . . gender or racial biases. I don't think anyone knows."*

P7: *"Like with other biomedical data, we don't know the significance of it when initially giving it out; the impact comes afterward, once it has been aggregated."*

Conversely, a number of interviewees made note that, despite the potential for privacy violations from neurological data being unknown, current BCI devices and data processing techniques are not sufficiently powerful to be a significant threat right now. Interviewees drew comparisons to other types of personal data that are commonly collected, such as GPS location data and photos of a user's face, suggesting that these are more significant and urgent privacy issue than BCI data, at least for the time being:

P3: *"Relative to all security threats that are out there and all the stuff you could solicit from my devices . . . I would put BCI maybe at the bottom of the list."*

P5: *"People are considerably more concerned about brain data than they are about, say, face recognition data. In practical terms, face recognition is a real privacy problem and BCI is a hypothetical privacy problem."*

P6: *"It's definitely a privacy concern, but it's not on the scale of giving someone a camera and allowing them to access the internet with it. You can't complain about privacy on one thing and then take pictures*

of everything you do and post it somewhere else. BCIs have potential to be a serious concern at some point in the future, maybe."

An interesting perspective on this topic was given by participant P2, who acknowledged privacy concerns associated with BCI data collection, but chose not to focus on it in favour of prioritizing research:

P2: *"I don't care, in the sense that this isn't where my focus is. It's more important to me to do some research . . . to democratize the technology and contribute to this process . . . than not doing it because of privacy concern. In some sense I'm sacrificing myself, sacrificing my privacy, in order to do some research in this."*

The potential for BCIs to be abused by authorities, governments, or corporate entities was also mentioned. Although this seems like a distant problem in terms of the technical capabilities of BCI devices, the fact that it was brought up by multiple interviewees suggests that this perception may be a barrier to public acceptance of BCIs irrespective of the actual likelihood of the threat:

P1: *"I fear that there will be even greater power for advertising companies and anybody who wanted to exercise some type of control over the population. I do expect this to go very dystopian very quickly in the case that there are no alternatives."*

P2: *"Let's say I'm working on a secret project for a company . . . the company may want to have my thoughts monitored to check my loyalty toward the project. This could be used and abused by companies and governments."*

All of the interviewees suggested that consumer protections should be a priority in the continuing development of commercial BCI technologies, including

encryption of all neurological data, comprehensive anonymization, and end-user data-ownership:

> P3: *"Everything should be encrypted. Data should be encrypted in transit and at rest. Ideally you would use some kind of homomorphic encryption so that you can even do computations on encrypted data when that's feasible. Certainly, there should be a pre-existing toolkit to make sure that data is properly anonymized."*
>
> P4: *"With these devices, we have chance to fix things and do them differently than with mobile phones. With mobile phones, in some sense privacy was an afterthought. By the time it became clear to the public what was happening, it was in some sense too late to do anything about it. [with BCIs] I want to start with a good use paradigm from the beginning."*
>
> P5: *"If you want people to use the device and feel comfortable enough to purchase a BCI device, the way to do that is to have a very strict privacy policy with end-user ownership of data, and give them the opportunity to have their data completely deleted from the database upon request."*

With respect to consumer protection, it was also stressed by participants P3 and P5 that typical consumers tend to have incorrect or inaccurate beliefs about BCIs and neurological data more generally, which prevents them being able to make informed decisions about BCI use:

> P3: *"We all make these trade-offs but—and this is not specific to BCI—but consumers generally don't know what they're trading off specifically, so they can't make that econometric judgement. My general comment*

here is that BCI data is not necessarily special. I think that's it's special insofar as people believe that it's special, because people have particular beliefs about the brain."

P3: *"I could see myself making some kind of trade-off, but I would be very contextually aware of it . . . I would imagine that the average consumer wouldn't know how to be contextually aware of the privacy value of their data. That latter part is what concerns me mostly: we can't expect an average consumer to know what they're revealing about themselves, necessarily."*

P5: *"Most BCI manufacturer privacy policies are designed around standard tech privacy policies. Where it goes beyond that, it's due to recognition that people are more concerned about brain data than other data due to rational or irrational fears about what you might be doing with it . . . The average user doesn't even know that you can't read minds with EEG."*

For the Safety meta-theme, it should be noted that what is important here is not necessarily whether these safety concerns are likely or even feasible. Rather, it is the *perception* of risk that has a significant bearing on the acceptance of BCIs. BCI designers should therefore be aware not just of actual risks to users' privacy and security, but of perceived risks as well, and make efforts to adequately inform users of the difference.

In summary, concerns about the safety of BCIs comprises the three interrelated dimensions of privacy, surveillance, and consumer protection. In terms of privacy, there is concern that neurological data from BCI users could be used to violate user privacy, either in the form of malicious cyber-attacks or more mundane corporate marketing. There is a general awareness that corporate data collection

from BCIs is leading to the accumulation of massive amounts of EEG data from consumers, which is troubling because the limits of what can be inferred from aggregated neurological data are not known. For the topic of surveillance, there is concern about authoritative entities like governments or employers leveraging BCI data at scale to monitor the mental states of individuals. Simultaneously, there is scepticism about the ability of current privacy regulations to protect BCI users, as well as users' ability to understand these issues and make informed decisions about BCI use.

4.3.2 Usability

Table 4.5: The structure of the *Usability* meta-theme, including its two sub-themes and their respective codes.

#	Theme	Code
1	Difficulty	BCI hardware is difficult to use.
2		BCI software is difficult to use.
3		Usability-performance trade-off.
4		The most usable BCIs have limited capabilities.
5		Muse, Neurosky have good user experience.
6		OpenBCI is difficult, cumbersome, too technical.
7		Ease-of-setup is important for BCI devices.
1	Comfort	BCI devices become uncomfortable over time.
2		Social stigma/aesthetics of BCIs.
3		User becomes habituated to the presence of the BCI device on their head.
4		Comfort-performance trade-off.
5		BCIs need to be perceived as less "creepy."

The use of BCIs is not straightforward, even for experts, and devices with better usability characteristics tend to have restricted capabilities. Technical difficulties as well as social and physical discomfort are barriers in the way of BCI and passthought acceptance.

A common theme was around the general difficulty associated with the basic setup and usage of BCI devices. Interviewees made a number of comparisons between different devices that they had used in terms of their difficulty and usability characteristics, highlighting a trade-off between usability and performance.

> P2: *"Muse has good use experience, because the device is comfortable, it's comfortable to wear it, you switch it on, off, and it works out of the box."*
>
> P2: *"With OpenBCI, I struggle a bit to get the signal into the computer . . . and the setup was unclear at the beginning . . . I had to follow some tutorials . . . the software was failing and it wasn't clear how to set up a working environment . . . There was not a linear procedure to follow."*
>
> P4: *"Even when recording signals is made easy, extracting information from those signals is not."*
>
> P6: *"It's usable for things that don't involve movement. For example, the Muse, sitting still doing meditation, it's fine. It's much better for that than for anything to do with movement. Even blinking is problematic."*

In addition to difficulty, the comfort of wearing a BCI device was an important dimension of usability. Interviewees remarked that wearing a BCI device for an extended period of time can cause it to become uncomfortable or painful, or can even cause a headache in the case of participant P1.

> P1: *"[The OpenBCI headset] becomes transparent after a few minutes. So you kind of get used to it. I notice this lasts for about 10–15 minutes and then it becomes uncomfortable, it can cause a headache."*

P2: *"A couple of red spots appear where they [the sensors] are. If I'm wearing it for a long time I do have to take them off."*

P6: *"The Muse is definitely more comfortable than the Epoc. For the first 30 minutes, wearing the Epoc is not bad. Over time the reference sensors that sit behind the ears on the Epoc start to become uncomfortable or painful."*

However, P3 stated that all of the devices they had tried were a significant improvement over the EEG caps commonly used in medical and research contexts.

P3: *"I'm impressed by all of the cheaper commercial devices in terms of their comfort. It's certainly better than wearing a cap, and also they don't require gel."*

In particular, the Muse and Neurosky Mindwave devices were regarded as very comfortable to wear, but offered a least in terms of performance and capabilities, as described by participants P1 and P3:

P1: *"I would say Muse . . . no, Neurosky was the most comfortable . . . but also the least meaningful. The Muse was surely easier to have on in terms of fashion and wearability . . . it's easier to go around with as well . . . whereas OpenBCI is at the bottom of the list."*

P3: *"We've used everything from OpenBCI to the Mindwave . . . there were obviously differing levels of success . . . our best results were with the OpenBCI device."*

The appearance of BCI devices was a common point of discussion, particularly around the sociocultural ramifications of wearing a BCI in the presence of other people, which could be viewed as stigmatizing.

P3: *"In terms of usability, what I think of a lot is how awkwardly visible these devices are, especially for people with disabilities."*

P4: *"In some sense you can see it like a bicycle helmet. Would you be willing to go around wearing a bicycle helmet everywhere you go?"*

P6: *"I wouldn't wear it outside because people would think it's weird."*

P2: *"OpenBCI, some work could be done on the sensors. And they provide really raw boards, there's no box that contains it. So that lacks a bit of design."*

Participants P3 and P5 suggested that these issues could be remedied by incorporating a BCI into a device that people already use, such as earphones, in order to make it less conspicuous:

P5: *"A couple of people have designed headphone-based BCIs, which is a good use-case . . . you and I are wearing headphones right now, and people will do that basically all day."*

P3: *"Something like an Apple Airpod that can record EEG signals . . . I think that's the frontier for usability."*

The idea of *trade-offs* was present throughout the discussion of usability, both explicitly and implicitly. The basic idea is that getting good performance out of a BCI device is very difficult and beyond the capabilities of laypeople who don't have a significant understanding of the neurophysiology, machine learning, and computer systems that underlie BCI technologies. Simpler, more comfortable, and easier-to-use devices have been developed and marketed with some success (e.g., the Muse BCI headset), but this has come at the expense of performance and capability of those devices. Throughout these discussions, no particular device stood out as being more usable than others without a significant loss in performance.

Indeed, the OpenBCI devices, which were considered by most interviewees to be the most flexible and powerful consumer-oriented devices available, were regarded as very difficult to use, uncomfortable, and visually unappealing.

To summarize: a number of usability issues are apparent when discussing the use of BCIs for average users. On the technical side, these devices can be difficult to setup and use, and the setup process can be time-consuming if the sensors require the application of a saline solution or conductive gel. In terms of comfort, many BCI devices are physically uncomfortable to wear for extended periods of time, significantly reducing their viability for real-world applications. Finally, the visibility of BCI devices can be awkward or stigmatizing, especially if a user is using a BCI to compensate for a disability. The latter two problems can be mitigated with smaller, less obtrusive devices such as BCIs integrated into earphones, as suggested by P3 and P5, but it is unclear to what extent this would limit their capabilities.

4.3.3 Development

BCI technology is immature and lacking broad applicability, and doesn't offer enough value to be an everyday-use device. A common sentiment was that the current use-cases for BCIs are not sufficient to entice a typical consumer to spend the required amount of money and time to purchase and learn to use a BCI system. Despite the very limited capabilities of current BCIs, experts generally believe that they have significant potential that can be achieved with continued research and development. The essence of the Development meta-theme is that we are in the early days of BCI development and significant work is needed to move the technology forward to a state where normal people would want to use it.

Table 4.6: The structure of the *Development* meta-theme, including its three sub-themes and their respective codes.

#	Theme	Code
1	Applications	BCIs need a compelling primary use-case.
2		BCIs have value and serve a purpose.
3		Passthoughts for high-value authentications but not trivial ones.
4		BCIs are useful for meditation/neurofeedback training.
5		BCIs are a novelty.
6		Existing methods of interaction are easier and better for average users than BCI.
7		Passthoughts are impractical for real-world use.
1	Future	We are in the early stages of BCI development.
2		BCIs will probably be common in the future.
3		BCIs aren't powerful now but will be one day.
4		Privacy and security issues should be addressed before wider adoption, rather than later.
5		Lack of general understanding of neurological data (we don't know enough to know what the risks are).
1	Performance	Performance of BCIs is disappointing.
2		Low information-transfer rate (bitrate).
3		Non-stationarity of EEG as a benefit.
4		Non-stationarity of EEG as a barrier.
5		Passthoughts could lock people out if they're not in the right mental state.
6		Ambient electrical interference.
7		EEG data quality is low.
8		Invasive BCIs are more impressive than non-invasive ones.
9		Commercial BCI engineering is impressive.

P5: *"There's this idea that you're going to put this thing on your head and then quickly learn to control something. The reality is very different. Even mental imagery BCIs take weeks of training to learn to use effectively."*

P5: *"Widespread adoption needs something that people will wear on their heads anyway, like a VR set or earphones. The success of Muse is in giving people a reason to put the BCI on their head on a regular basis."*

P6: *"Based on my experiences with the Emotiv Epoc and Muse . . . at this point it sounds like a marketing thing. There's no way you could just use these things out in the world. It's too finicky, requires too much setup . . . there's too many things that just get in the way of casual use . . . It's just not practical yet."*

P4: *"If the only use cases are the ones we have right now, I have a hard time imagining that BCIs will be common in the future. Then again, as big tech companies are entering the space and talking about advanced use cases, anything can happen. I think we are a couple of years out."*

P5's comments are particularly relevant for the case of authentication; a user is not likely to carry around a cumbersome BCI device if it is useful only for authentication. Authentication with BCIs for healthy people only makes sense if they have some compelling reason to own and use a BCI in the first place, or in a context where the security demands warrant use of passthoughts. P5 and P3 made additional comments to this effect:

P5: *"In some sense I think authentication could work, but then people have to have a BCI just for authentication. To put it on, authenticate,*

and then take it off, because there's no other reason to have it on your head."

P3: *"It depends on the context: are you using this to unlock your cellphone? or are you using it to withdraw twenty thousand dollars from the bank? I've always envisioned passthoughts as more of a 'change your last will and testament' type of authentication mechanism, as opposed to unlocking your cellphone."*

Another recurring topic related to the theme of development stressed that existing methods of human-computer interaction are generally superior for healthy users in terms of usability and performance, encapsulated in these comments from P4 and P5:

P4: *"The information transfer rate that we can get from these devices is still rather low, nowhere near to what a typical person can do on their smartphone using their fingers. Given the stage of the technology, for most able-bodied people BCIs would be a step back."*

P5: *"The consistent result is that . . . people think it's really cool for 10 minutes, then ask for the mouse and keyboard back, take the BCI off, and never put it on again."*

To summarize the Development meta-theme: in many ways it is not clear what commercial BCIs *are for*. Medical BCIs have much more defined objectives and use-cases: controlling a wheelchair, enabling communication, and so on. With commercial BCI devices, the objectives are much less clear. In some sense it appears that, rather than developing a new technology to solve a problem, BCI developers have created a technology without a use-case and are now scrambling to find applications for it. The overall performance of BCI devices is an area

of concern, with many interviewees remarking that BCIs don't live up to their expectations or the claims made by BCI manufacturers. Many of the suggested use-cases for BCIs are simply not possible with the current generation of commercial BCI devices because of their restricted capabilities. There was a general consensus among interviewees that we are in the very early stages of BCI development, and that there is significant potential for BCIs to improve, pending further refinement of existing neuroimaging technologies or the emergence of wholly novel methods.

4.4 Interpretation

This interview study began with the objective of answering the question: *What are the main barriers preventing adoption of BCIs and passthoughts for the general population?* Through qualitative semi-structured interviews with BCI expert users and a reflexive approach to thematic analysis, I identified three meta-themes which captured the interviewees' beliefs and opinions about the public acceptance and adoption of BCIs and BCI-based authentication. Based on this work, the main barriers affecting perceptions and beliefs about BCIs are related to perceived threats to safety or uncertainty about the safety of BCIs, problems with usability, and a need for further development and refinement of the technology.

The *Safety* meta-theme suggests that people are sceptical or at least uncertain about the safety of using BCI devices. There is a perception of risk associated with the collection of neurological data by BCI manufacturers, as well as aversion to the idea that BCI data could be abused by governments or employers to monitor individuals' mental states. Further, there is a general sentiment that laws governing privacy and corporate data collection are not sufficient to protect BCI users from these perceived threats. The perception of risk is a barrier to public acceptance of BCIs, irrespective of whether the risks are credible or realistic. To

make potential users more comfortable with BCIs, BCI designers should be aware of this and attempt to mitigate the real risks associated with BCI use as well as the misplaced perception of risk arising due to uncertainty or misinformation.

The takeaway message behind the *Usability* meta-theme is the BCI devices are not usable for normal people due to a combination of technical difficulty in setup and use, physical discomfort, and social stigma due to the obvious and awkward appearance of BCI devices, especially for people who would use a BCI to compensate for a disability. In the domain of commercial BCI devices, there is a tension between usability and performance. It is not clear how BCI designers might approach making their devices smaller, less obtrusive, and easier to use without compromising their capabilities.

The *Development* meta-theme stresses that non-medical BCIs lack a compelling use-case that would encourage non-enthusiasts to become interested in BCIs devices. While a number of studies have demonstrated impressive capabilities of BCIs in a laboratory environment, these have not translated into the real world, and there is scepticism about whether real users would opt to use a BCI when traditional methods of HCI like mice, keyboard, and touchscreens can facilitate a much greater information transfer rate with significantly better accuracy and reliability. Rather than trying to make BCIs perform well in tasks that can be trivially accomplished with other interaction methods, the BCI community may benefit from asking *"What types of interaction can BCIs enable that other modalities cannot?"* Authentication with BCIs has been investigated as a potential answer to this question, but these reports from interviewees alongside the disappointing results of my BCI authenticator in Chapter 3 seem not to support this use-case.

A unifying concept that spans across all three meta-themes is that of uncertainty. The interdisciplinary field of BCI devices involves a number of domains

which, despite extensive study, remain largely mysterious and poorly understood. The most obvious example of this is the domain of neurophysiology, but the *black-box* problem of machine learning (i.e., that many machine learning models do not specify the relationship between the input and output values) applies here as well, since virtually all BCI applications involve machine learning in some way. Feeding poorly-understood EEG data into a black-box machine learning classifier is a recipe for inscrutability, and it should therefore be unsurprising that even experts struggle with these systems.

4.4.1 Limitations

A significant limitation of this study is its small sample size of only seven interviewees. Unfortunately, due to the relative uncommonality of BCI devices, it is not easy to access significant numbers of BCI experts. In this study I had better results recruiting BCI experts by directly cold-emailing researchers in the field as opposed to the initial approach of posting to online BCI forums. This approach may be useful for other BCI studies that intend to address an expert (or at least *experienced*) sample.

Additionally, while the interviews were intended to primarily address views about passthought authentication, most of the interviews (and therefore the derived codes and themes) ended up being about the usability of BCIs in general. I propose two possible interpretations of this: firstly, it may be that the interview guide prepared for this study was not specific enough to capture the emphasis on authentication. The second interpretation is that the relationship between passthoughts and BCI usability is such that one cannot be addressed in the absence of the other. In other words, passthought usability depends critically on the usability of BCIs in general, which tends to be poor, so any discussion about passthoughts will necessarily center around the topic of BCI usability. This would

also suggest that the most significant barriers to passthought acceptance and adoption are those of BCIs in general. The latter interpretation seems more interesting from a theoretical standpoint, though it is difficult to discount the first without further study.

4.4.2 Conclusion

In summary, the usability of passthought authentication is tightly connected to the usability and acceptance factors of BCI devices in general, which can broadly be categorized as those relating to perceived safety of BCI devices, their usability, and the need to continued development of BCI applications and technologies. Underpinning these factors is a general lack of fundamental knowledge about the brain which impedes development as well as understanding of BCI technologies. Despite these factors, BCI experts share the belief that continuing advancement of neuroscience, biosensing technologies, and machine learning will one day lead to significantly wider adoption and everyday use of BCIs for by the general population.

Chapter 5

Mechanical Turk BCI Questionnaire Study

5.1 Introduction and Background

The topic of BCI usability has been of considerable interest in recent years.[189–191] Only a few studies, however, have addressed usability in the context of BCI authentication or *passthoughts*.[18,20,192] A general consensus in the research literature is that although BCIs have become significantly more accessible to the public, substantial usability burdens such as long setup times and poor or unreliable signal quality[143,190] have prevented adoption outside the enthusiast community. Additionally, the social discomfort arising from wearing a strange device on one's head may be a significant barrier.[143] The potential for adoption by the general population is of interest because all potential BCI applications, including authentication, are contingent upon people's willingness to purchase and use a BCI device.

This study is aimed at identifying factors that underlie BCI-naïve respondents' perceptions of the usability and security of BCIs, with the broader goal of understanding how these relate to their comfort and acceptance of BCIs generally. Specifically, it is expected that security related behaviours[193] and Big 5 personality dimensions[194] will be associated with individuals' acceptance and security concerns about BCIs.

5.2 Methods

5.2.1 Instruments

An exploratory questionnaire was developed which comprises four instruments designed to capture security-related behaviours, general personality dimensions, perceptions of BCIs and BCI security, and demographic information. Demographic information included age in years, education (*Primary/Elementary School, High-School, Vocational/Trade School, Bachelor's Degree, Graduate/Professional School,* or *Other* with a text field), and gender identity (*Female, Male, Prefer not to answer,* and *Self-describe* with a text field).

The *Ten Item Personality Inventory* (TIPI[195]) is an abbreviated measure of Big 5 personality dimensions (*Agreeableness, Openness to Experience, Extraversion, Emotional Stability,* and *Conscientiousness*[194]). For each dimension, the TIPI contains two items with opposing valence where each item is a pair of adjectives and respondents are asked to rate the extent to which the adjectives apply to them. For example, the TIPI subscale for Agreeableness comprises a positive item (*Sympathetic, warm*) and a negative item (*Critical, quarrelsome*). Respondents rate each TIPI item on a 7-point Likert scale (*Disagree strongly (1), Disagree moderately (2), Disagree a little (3), Neither agree nor disagree (4), Agree a little (5), Agree moderately (6), Agree strongly (7)*). The score for each subscale is calculated by taking the average ratings of the positive item and the reverse-scored negative item.

The TIPI was included because a number of prior studies have found significant relationships between the Big 5 personality dimensions and wearable technology acceptance,[196–201] and because the TIPI is trivially easy and fast for a respondent to complete, making it an ideal candidate for this exploratory study.

The *Security Behaviour Intentions Scale* (SeBIS[193]) is a 16-item scale which measures cybersecurity behaviours on four dimensions: *Device Securement, Password Generation, Proactive Awareness,* and *Updating,* with higher scores in these reflecting more secure behaviours. The SeBIS[193] has respondents rate statements about security behaviours such as "I manually lock my computer screen when I step away from it." on a five-point scale according to the frequency with which they engage in that behaviour (*Never (1), Rarely (2), Sometimes (3), Often (4), Always (5)*). Subscale scores for the SeBIS[193] are computed by taking the average of the items assigned to each subscale after reverse-scoring some items as described in Egelman and Peer.[193]

Figure 5.1: The images of the Emotiv Insight[57] that were presented to respondents alongside the following description: "A brain-computer interface, or BCI, is a system that allows a user to control a computer system with their mind. At it's simplest, a BCI reads signals coming from the brain and then does something based on the signals it receives, such as moving a mouse cursor on a screen or controlling a robotic arm. There are several BCI devices on the market which measure the electrical activity of parts of the brain using sensors placed on the scalp. Below are a few images of a wearable BCI device called the Emotiv Insight (www.emotiv.com). Please look at them and try to imagine what it would be like to wear the device. In the next section you will be asked about your thoughts about the device."

The *Comfort Rating Scale* (CRS) was adapted from Knight and Baber's[202] assessment tool for the comfort of wearable devices which asks respondents to rate a series of statements about a wearable device according to the extent to which

#	Dimension	Text
1	Appearance*	I would be worried about how I looked wearing the device and what others would think.**
2	Attachment	I would be constantly aware of the device's presence on my head.
3		After some time I would get used to the presence of the device on my head.**
4	Harm	The device would be safe, and unable to cause me any physical harm.
5	Perceived Change	The device would make me feel physically different. I would feel strange wearing it.
6		I would feel normal wearing the device. It wouldn't make me feel physically different.**
7	Movement	The device would affect the way that I move. It would inhibit or restrict my movement.
8		My movement would be unaffected by wearing the device.**
9	Anxiety	I would feel at-risk while wearing the device. Wearing the device would make me anxious.

Table 5.1: The final items used for the modified Comfort Rating Scale used in this study. Reversed items are used for response validation.

* The *Appearance* dimension was originally called *Emotion* and was not reversed in Knight and Baber's[202] paper describing the CRS.
** Reverse-scored items.

they agree with them on a 21-point scale, with higher scores indicating greater agreement. The CRS measures six dimensions of comfort: *Emotion*: emotions concerns about appearance of the device; *Attachment*: physical feel of the device on the body; *Harm*: the device causing damage or harm to the body; *Perceived Change*: feeling different or strange while wearing the device; *Movement*: the feeling that the device affects movement; and *Anxiety*: worry about the safety and reliability of the device.

As the present study was to be conducted online, the precise wording of the items described in Knight and Baber[202] were altered to adjust for the fact that respondents will not have worn or used the device. Instead, a brief description of BCI devices is presented alongside photos of a BCI device (Figure 5.1; Emotiv Insight[57]) and the respondent is asked to imagine what it would be like to wear the device. The survey items were altered to reflect a hypothetical scenario. For example, "I am worried about how I look when I wear this device." is changed to "I would be worried about how I looked wearing the device." Photos of the Emotiv Insight were used for consistency and easier contrast between the present study and the BCI authentication study described in Chapter 3. For easier interpretation, the *Emotion* dimension was reverse-scored and renamed to *Appearance*. Additional items were added that had opposing valence to the original items in order to determine whether participants were not paying attention to the task (i.e., the difference between the rating on the original item and the reversed rating on the opposing item is greater than some threshold). Reversed items were added for the Attachment, Perceived Change, and Movement dimensions. The score for these dimensions is the average of the original and opposing items after reverse-scoring the opposing one. Finally, the scale on which respondents are asked to rate the items is reduced from Knight and Baber's'.[202] The final set of items for the CRS in this study is presented in Table 5.1.

#	Subscale	Survey Item
1	Knowledge	Please rate your level of knowledge about brain-computer interfaces (BCIs):
2	Future	In the future, wearable BCI devices will become mainstream and most people will use them.
3		BCI devices will probably never become popular.**
4		Wearable BCI devices will be vulnerable to previously-unknown types of security challenges.
5		In the future, companies like Google and Facebook will use BCI devices to learn about users for the purpose of advertisement targeting.
6		In the future, governments will use wearable BCI devices for surveillance.
7	Consumer	There should be special protections or regulations about the collection and use of data from wearable BCI devices.
8		Current privacy regulations are sufficient to protect BCI users.**
9		Companies that collect data from wearable BCI devices should be required to disclose how the data will be used.
10		Companies that collect data from wearable BCI devices should be required to ask for consent before collecting any data.
11		BCI manufacturers should be able to collect and use data from BCI devices without explicit permission.**
12		Users should not have the right to force companies to delete data collected from them.**
13		Please select "Agree" as your answer for this question.
14	Security	Data from BCI devices is more sensitive than that of other wearable devices (e.g., smartwatch).
15		Current security practices like encryption are not sufficient to protect data generated by BCIs.
16		It would be impossible for a hacker to cause physical harm or damage by taking control of the device.**
17_a		A hacker could use data intercepted from a BCI device to infer private information about the user.
17_b		What sort of information might they be able to learn (select all that apply)?*

Table 5.2: Survey items for the BCI Acceptance Scale (BAS) grouped by subscales.

* Item 17_b is only shown to respondents who select "Agree" or "Strongly agree" as their answer for Item 17_a.
** Reverse-scored items.

#	Survey Item
17_{b1}	Gender
17_{b2}	Sexual Orientation
17_{b3}	Ethnicity
17_{b4}	Political or religious beliefs
17_{b5}	Emotional state
17_{b6}	Passwords for online accounts
17_{b7}	Medical or health-related information (including mental health)
17_{b8}	Whether the user is being truthful or lying.

Table 5.3: The possible answers to item 17_b ("What sort of information might they be able to learn (select all that apply)?"), which is presented only to those who respond "Agree" or "Strongly agree" to the preceding item 17_a ("A hacker could use data intercepted from a BCI device to infer private information about the user.")

The *BCI Acceptance Scale* (BAS) was developed for this study as an exploratory measure to assess general opinions about BCIs for people who do not necessarily have experience using them. Scale items were generated in a brainstorming session which was guided in part by experience and knowledge obtained while conducting qualitative interviews with BCI users, as described in Chapter 4. A set of 26 candidate items were generated which were then grouped into categories according to topic and redundant items were dropped or combined. As with the CRS, validation items were added corresponding to several of the BAS items and were worded to have the opposite valence. This process yielded a total of 18 items which were grouped into three categories: *Future:* the belief that BCI devices are likely to be commonplace at some point in the future; *Consumer:* concern about regulation and consumer protections regarding BCIs; and *Security:* concern about the safety and security of BCIs, sensitivity of BCI data. A fourth dimension, *Knowledge* consists of one item which asks the respondent to rate their level of knowledge on the topic of BCIs on a five-point scale.

All of the BAS items are presented as statements (see Table 5.2) to which the respondent is asked to rate their level of agreement on a five-point Likert scale with higher scores indicating greater agreement (or knowledge, in the case of the BCI knowledge question). The valence of the items is mixed and some must be reverse-scored before computing the subscale values. A flag question was added to the *Consumer* subscale (Item 13 in Table 5.2) instructing the respondent to select a particular answer. This item is used for validation by detecting respondents who do not read the items. If respondents select a positive response (Agree or Strongly agree) to the item "A hacker could use data intercepted from a BCI device to infer private information about the user." (Security subscale) they are given the followup question "What sort of information might they be able to learn (select all that apply)?" and a list of eight different types of information which can be selected using checkboxes (Table 5.3).

The questionnaire was implemented using LimeSurvey,[203] an open-source software platform for developing and hosting web-based surveys, and hosted on a local laboratory server. The consent form, demographic questions, SeBIS,[193] TIPI,[195] modified CRS,[202] and BAS were created in the LimeSurvey dashboard application as Question Groups. The question groups were presented in a particular order (Consent, demographics, TIPI, SeBIS, CRS, BAS), however, the ordering of items within each group was set to be randomized, as was the order of answer items for multiple-choice type questions (e.g., the items in Table 5.3). Finally, settings were enabled in the LimeSurvey page to record the MTurk (see 5.2.2) Worker ID of the respondent as well as the amount of time spent on each question group and the survey overall to avoid duplicate submissions and for response validation.

5.2.2 Participants and Recruitment

The participants for this study were recruited through Amazon Mechanical Turk, (MTurk) an online crowdsourcing platform for human-intelligence tasks (HITs) that is commonly used to gather survey data for research studies.[21] MTurk workers volunteer to complete HITs through the MTurk platform in exchange for typically modest monetary compensation. Rather than interacting with MTurk directly, the HIT was created through CloudResearch (formerly TurkPrime[204])–a service which facilitates easier management of research studies (as opposed to other types of HITs) on MTurk for a small fee.

The CloudResearch[204] study was set to limit participants to those with at least a 98% HIT approval rating who had completed at least 100 HITs, and to those located in Canada or the United States only. The geographic constraint was included to ensure consistency in understanding the research context. The estimated completion time of 15 minutes was displayed on the HIT post as well as the compensation of $2. When a worker accepted the HIT, they were directed to the LimeSurvey page hosting the questionnaire. A consent form was presented which explains the objective and nature of the study, and the worker could choose to proceed having accepted the conditions of the study or decline and withdraw from the study. At the end of the questionnaire, a code was provided which the worker can enter back on the MTurk HIT page to prove their completion and receive compensation. A pilot HIT was posted with a quota of 25 responses which were validated before posting another with a quota of 100 for a total of 125 expected responses.

5.2.3 Data Analysis

Data preparation and analysis were conducted using the R statistical computing language.[205] R scripts containing the code used for preparation and analysis of these data can be found in Appendix B. Plots are generated using the R packages `ggplot2, ggExtra,` and `ggpubr`. Data tables are constructed as dataframes and exported using `xtable`.

Data were downloaded in `.csv` format from LimeSurvey and loaded into an R session. Firstly, respondents who did not accept the consent form were removed from the data frame. Data were validated by computing difference scores between the opposing-valence items on the CRS and BAS (after reverse-scoring as appropriate); large differences indicate inconsistent answers and suggest that the respondent may be providing spurious answers or not paying attention. Cases with a difference score greater than 4 on any of the three validation items from the CRS (7-point scale) or greater than 3 on any of the BAS items (5-point scale) were removed. Similarly, any respondents who failed to select the correct answer for the flag question (Item 13 in Table 5.2) were removed from the dataset. Subscale scores for the SeBIS, TIPI, CRS, and BAS were calculated by taking the mean of the items of each subscale after reverse-scoring as appropriate.

Hypotheses

The main relationships of interest are between personal factors (SeBIS, TIPI) and BCI factors (CRS, BAS), which can be viewed as independent and dependent variables (IVs and DVs), respectively. Broadly, it is hypothesized that personality factors will be significantly associated with respondents' acceptance, perceived comfort, and beliefs about the future prospects of BCIs, and that security behaviour factors will be related to views about BCI security and future. Twelve

hypotheses were generated that correspond to the SeBIS and TIPI measures. The hypotheses relating to the SeBIS (HS_{1-4}) are as follows:

HS_1 Device securement behaviours ($SeBIS_{Securement}$) will be positively associated with concerns about the security of BCIs ($BAS_{Security}$).

HS_2 Device securement behaviours ($SeBIS_{Securement}$) will be negatively associated with beliefs that BCIs will become common in the future (BAS_{Future}).

HS_3 Awareness of security practices ($SeBIS_{ProactiveAwareness}$) will be positively associated with concerns about the security of BCIs ($BAS_{Security}$).

HS_4 Awareness of security practices ($SeBIS_{ProactiveAwareness}$) will be negatively associated with beliefs that BCIs will become common in the future (BAS_{Future}).

And the hypotheses relating to the TIPI (HP_{1-8}) are:

HP_1 Agreeableness will be negatively associated with feelings of anxiety about the BCI device ($CRS_{Anxiety}$).

HP_2 Emotional Stability will be positively associated with comfort regarding the appearance of the BCI device ($CRS_{Appearance}$).

HP_3 Emotional Stability will be will be negatively associated with the belief that the BCI device could cause harm (CRS_{Harm}).

HP_4 Emotional stability will be negatively associated with feelings of anxiety about the BCI device ($CRS_{Anxiety}$).

HP_5 Openness to Experience will be positively associated with beliefs that BCIs will become common in the future (BAS_{Future}).

HP_6 Openness to Experience will be positively associated with comfort regarding the appearance of the BCI device ($CRS_{Appearance}$).

HP_7 Openness to Experience will be negatively associated with feelings of anxiety about the BCI device ($CRS_{Anxiety}$).

HP_8 Extraversion will be positively associated with comfort regarding the appearance of the BCI device ($CRS_{Appearance}$).

Two tests were conducted for each hypothesis. First, a one-tailed Spearman rank correlation coefficient is computed between the two variables using the `cor` function in base R with `method = ‘‘spearman’’` as an argument. As a secondary test, the IV (SeBIS or TIPI) is split into two groups at the median value and a Wilcoxon rank sum test is computed between the two groups on the DV (CRS or BAS) using `wilcox.test`.

5.3 Results

5.3.1 Descriptive Statistics

Demographics and Time

A total of 126 respondents started the HIT but 2 did not complete it. All respondents selected the correct answer for the flag question (Item 13 in Table 5.2), but 15 participants had inconsistent answers to the opposing-valence questions used for validation and were excluded from further analysis. The final total of responses included in subsequent analysis is 109.

One respondent did not disclose their gender and all other respondents indicated their gender as either *male* or *female*. In the initial responses there were

79 male-identifying and 46 female-identifying respondents. After cases were removed, there remained 63 male-identifying, 45 female-identifying respondents, and one respondent with undisclosed gender. A bias toward more male respondents is a relatively common trend in MTurk studies[206] and not unexpected.

Education	n
High-school	21
Trade/Vocational	15
Bachelor's	60
Graduate/Professional	11
(Missing)	2

Table 5.4: Frequency table of levels of education for the sample.

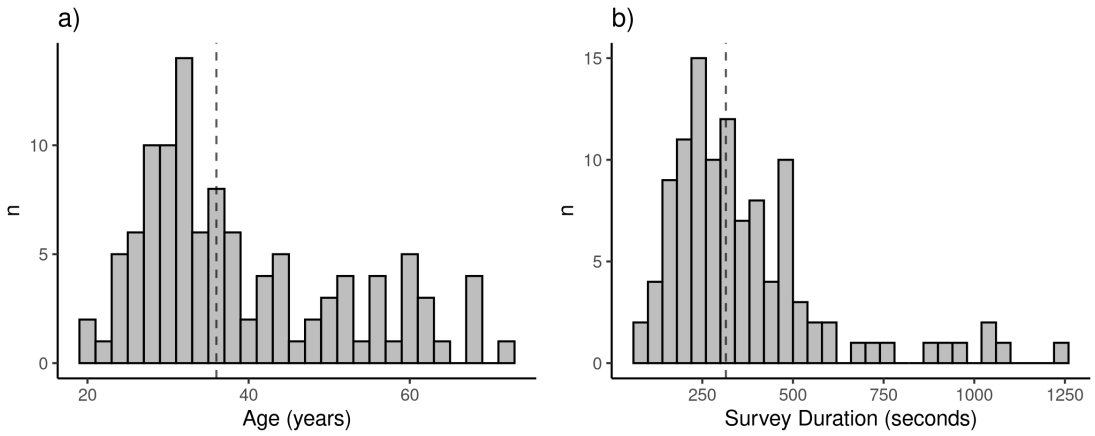

Figure 5.2: Distribution of ages (a) and survey completion times (b) for the sample. Dashed lines represent median values.

The median age of the sample was 36, and the mean is 39.85 ($SD = 12.94$). A histogram showing the distribution of ages in the sample is shown in Figure 5.2 (a). The skew toward younger respondents is another common feature of MTurk studies.[206]

The median completion time for the survey was 315 seconds. The distribution of completion times is represented in Figure 5.2 (b). A significant skew is apparent with the majority of respondents completing the survey in under 10 minutes but a few taking up to twice as long.

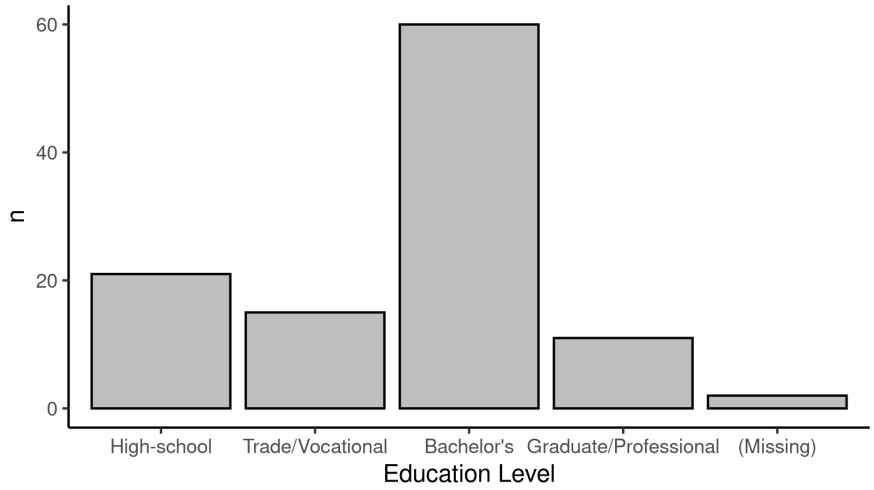

Figure 5.3: Histogram of levels of education for the sample.

Education data from the sample is shown in Table 5.4 and graphically in Figure 5.3. More than half of respondents report having a Bachelor's degree, which is significantly more than in the general population but typical for MTurk workers.[207]

Scales

Descriptive statistics of the TIPI responses are shown in Table 5.5 alongside populations norms.[208] Histograms of the five subscales of the TIPI are shown in Figure 5.4. Each of the subscales demonstrate a significant skew, all of which are negative except for Extraversion.

Scale	Median	Mean	SD	Population Mean
Agreeableness	5.50	5.35	1.33	4.91
Conscientiousness	6.00	5.68	1.16	4.94
Emotional Stability	5.50	5.35	1.41	4.56
Extraversion	3.00	3.35	1.81	3.98
Openness to Experience	5.00	5.00	1.45	5.46

Table 5.5: Descriptive statistics for the subscales of the TIPI. Scores on each subscale are calculated by taking the average of the subscale items after reverse-scoring as appropriate. Population mean values are from Gosling, Rentfrow, and Potter[208]. Scores on each subscale can range from 0 to 7.

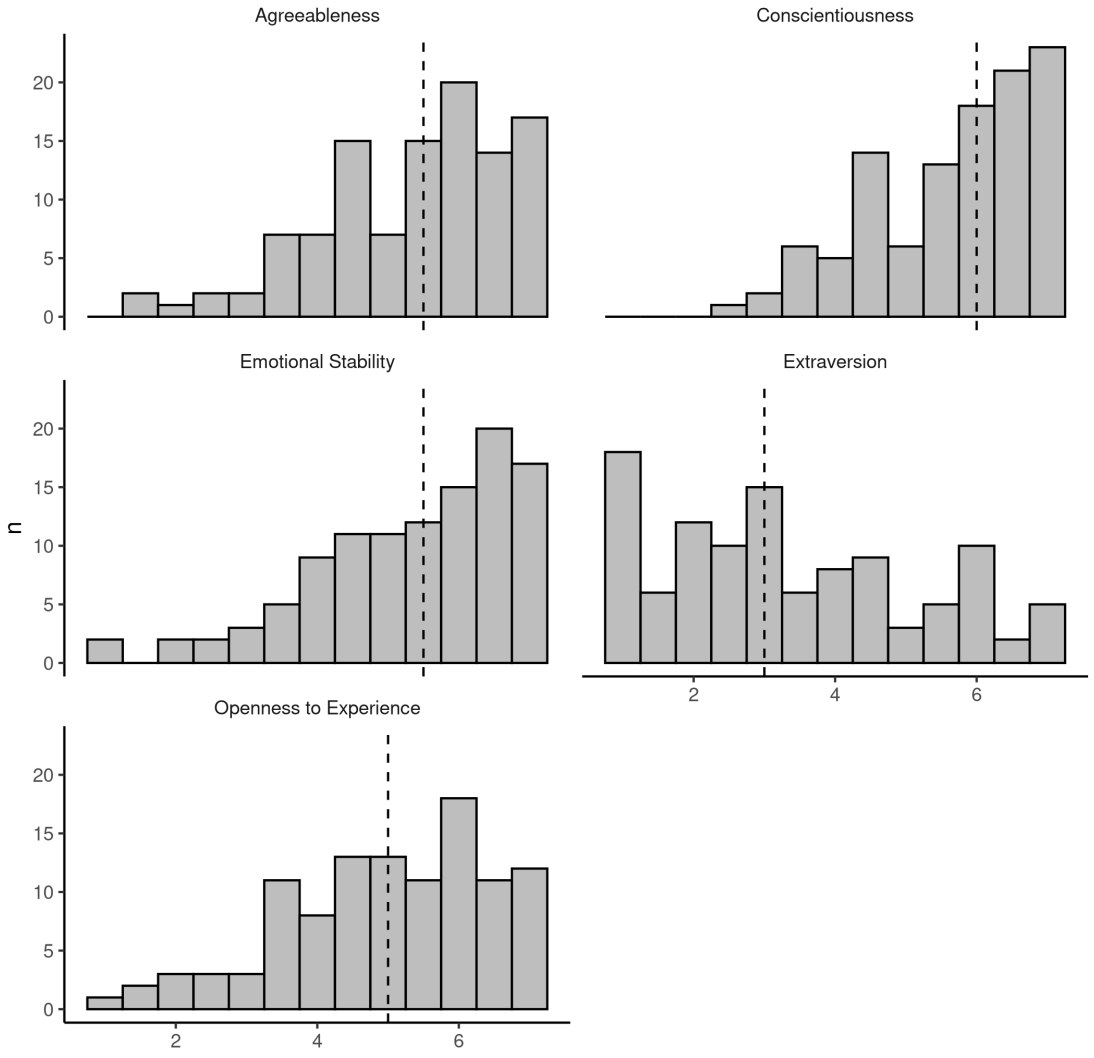

Figure 5.4: Histograms of the Big 5 personality dimensions as assessed using the Ten Item Personality Inventory (TIPI) subscales. Scores on each subscale are calculated by taking the average of the subscale items after reverse-scoring as appropriate. Dashed lines represent the median values.

The descriptive statistics for the SeBIS subscales are shown in Table 5.6 and distributions in Figure 5.5. For all four subscales of the SeBIS there is a significant negative skew, with the majority of respondents scoring above the neutral midpoint (i.e., an average score of 3 on the 5-point rating scale), suggesting that this sample demonstrate reasonably high security behaviours.

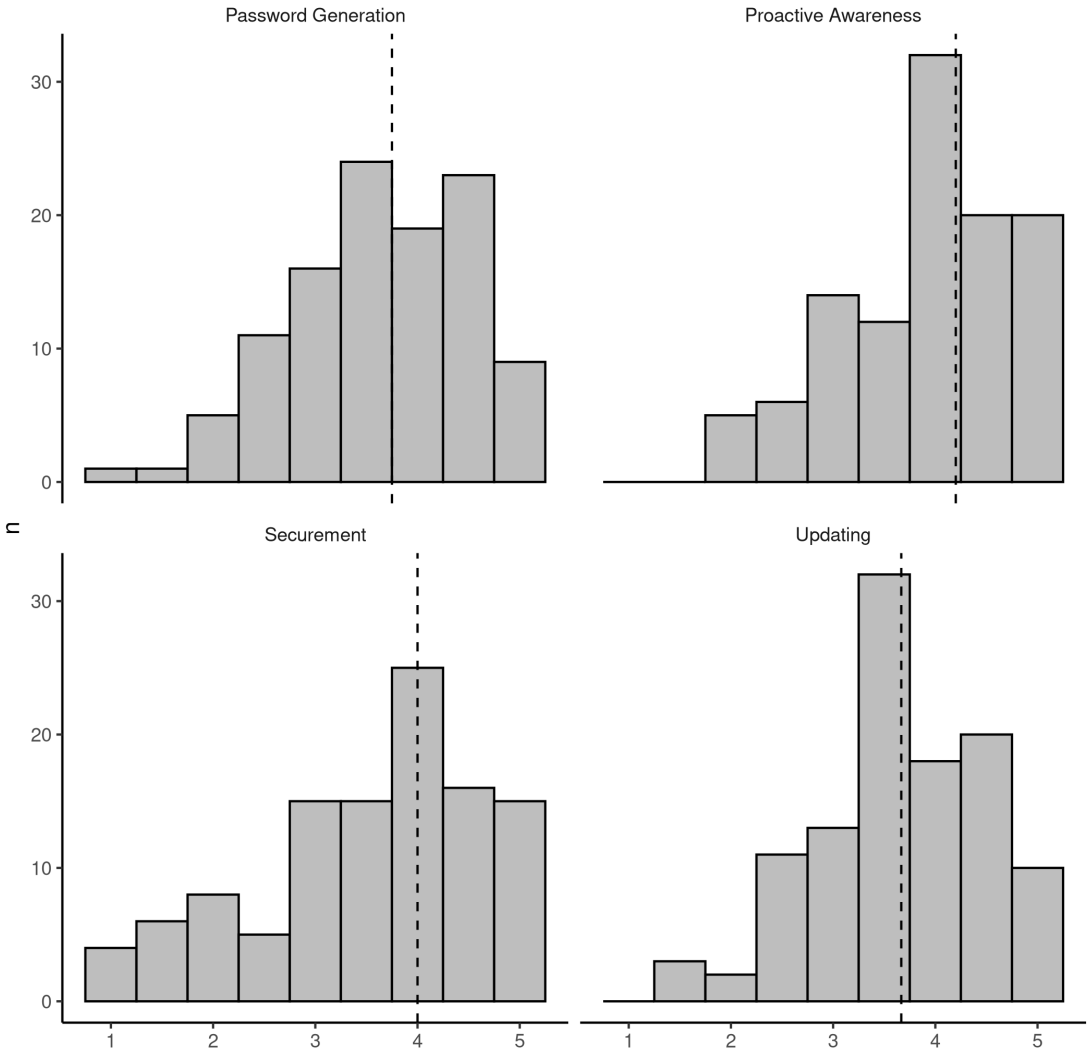

Figure 5.5: Histograms of the four subscales of the Security Behaviour Intentions Scale (SeBIS). Scores on each subscale are calculated by taking the average of the subscale items after reverse-scoring as appropriate. Dashed lines represent the median values.

The descriptive statistics for the CRS dimensions are shown in Table 5.7 and histograms of their distributions are depicted in Figure 5.6. Of interest are the dimensions of Anxiety, Harm, and Movement, which demonstrate some skewness in their distribution. Scores on the Anxiety dimension are mostly low, demonstrating a positive skew, indicating that the respondents mostly did not feel that wearing the device would cause feelings of anxiety. Correspondingly, respondents rated

Scale	Median	Mean	SD
Password Generation	3.75	3.73	0.87
Proactive Awareness	4.20	3.92	0.82
Securement	4.00	3.64	1.11
Updating	3.67	3.67	0.81

Table 5.6: Descriptive statistics of the subscales of the SeBIS. Scores on each subscale are calculated by taking the average of the subscale items after reverse-scoring as appropriate. Scores on each subscale can range from 0 to 5.

their belief that the device could cause harm as relatively low. The majority of the sample also indicated that they did not believe the device would significantly affect their movement. The remaining dimensions appear to follow a relatively normal distribution, though the Appearance dimension may be biased to more extreme answers given the low instances of the neutral response.

Scale	Median	Mean	SD
Anxiety	3.00	3.26	1.79
Appearance	4.00	4.15	1.81
Attachment	4.00	3.70	1.30
Change	4.00	4.17	1.65
Harm	3.00	3.14	1.61
Movement	3.00	3.29	1.46

Table 5.7: Descriptive statistics of the six dimensions measured by the CRS. Scores on each subscale are calculated by taking the average of the subscale items after reverse-scoring as appropriate. Scores on each subscale can range from 0 to 7.

Scale	Median	Mean	SD
BCI Knowledge	2.00	1.80	0.95
BCI Security	3.50	3.58	0.66
Consumer Protection	4.50	4.26	0.72
Future of BCIs	3.60	3.50	0.58

Table 5.8: Descriptive statistics for the four subscales of the BIS. Scores on each subscale are calculated by taking the average of the subscale items after reverse-scoring as appropriate. Scores on each subscale can range from 0 to 5.

Descriptive statistics for the BAS subscales are shown in Table 5.8 and histograms of their distributions are depicted in Figure 5.7. The sample reported

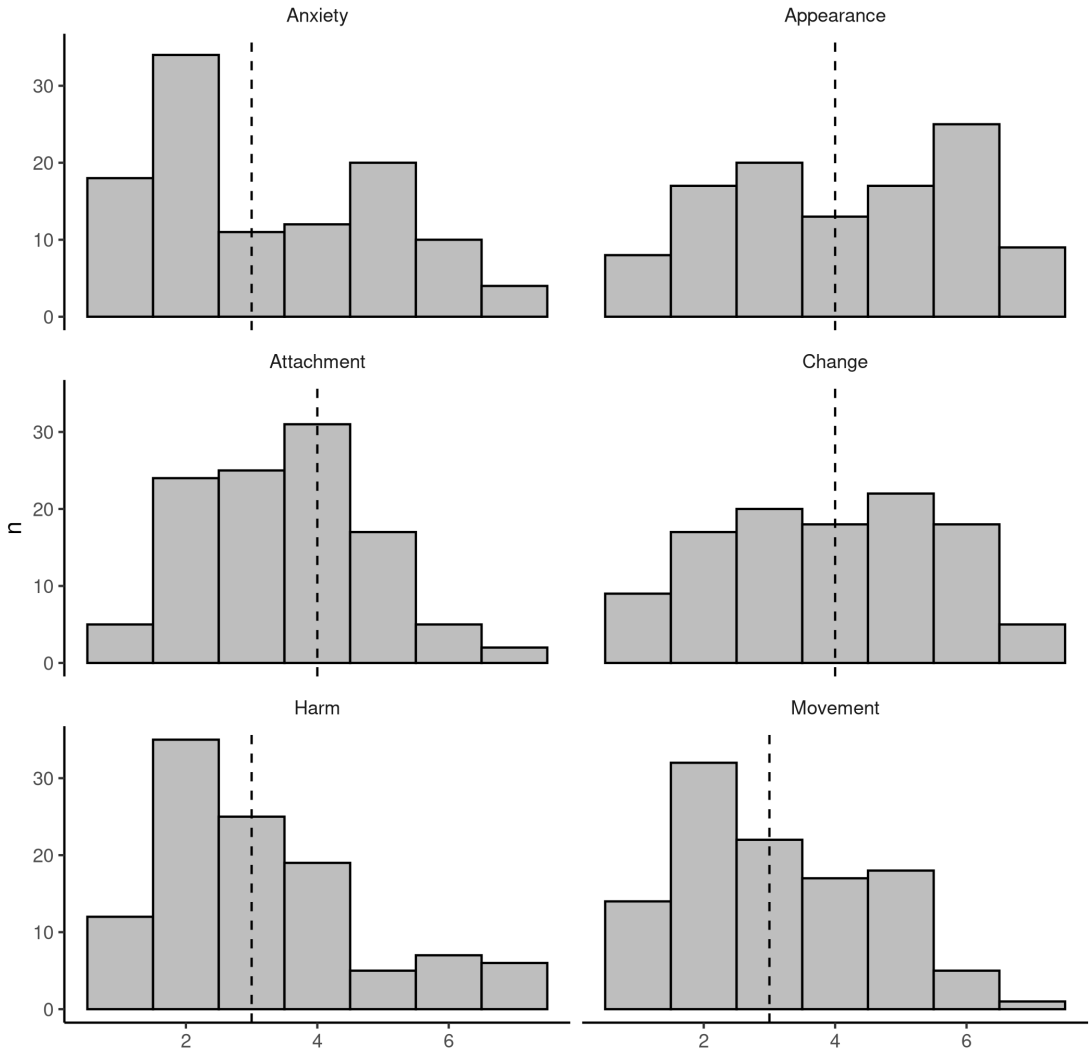

Figure 5.6: Histograms of the six comfort dimensions assessed using the Comfort Rating Scale (CRS). Scores on each subscale are calculated by taking the average of the subscale items after reverse-scoring as appropriate. Dashed lines represent the median values.

generally quite low prior knowledge of BCIs, although 8 respondents rated themselves *Moderately knowledgeable* and one *Very knowledgeable* about BCIs. On the Security subscale, very few respondents were unconcerned, while a majority were either neutral or moderately concerned. The respondents in this sample showed strong support for regulations and protections around the collection and use of

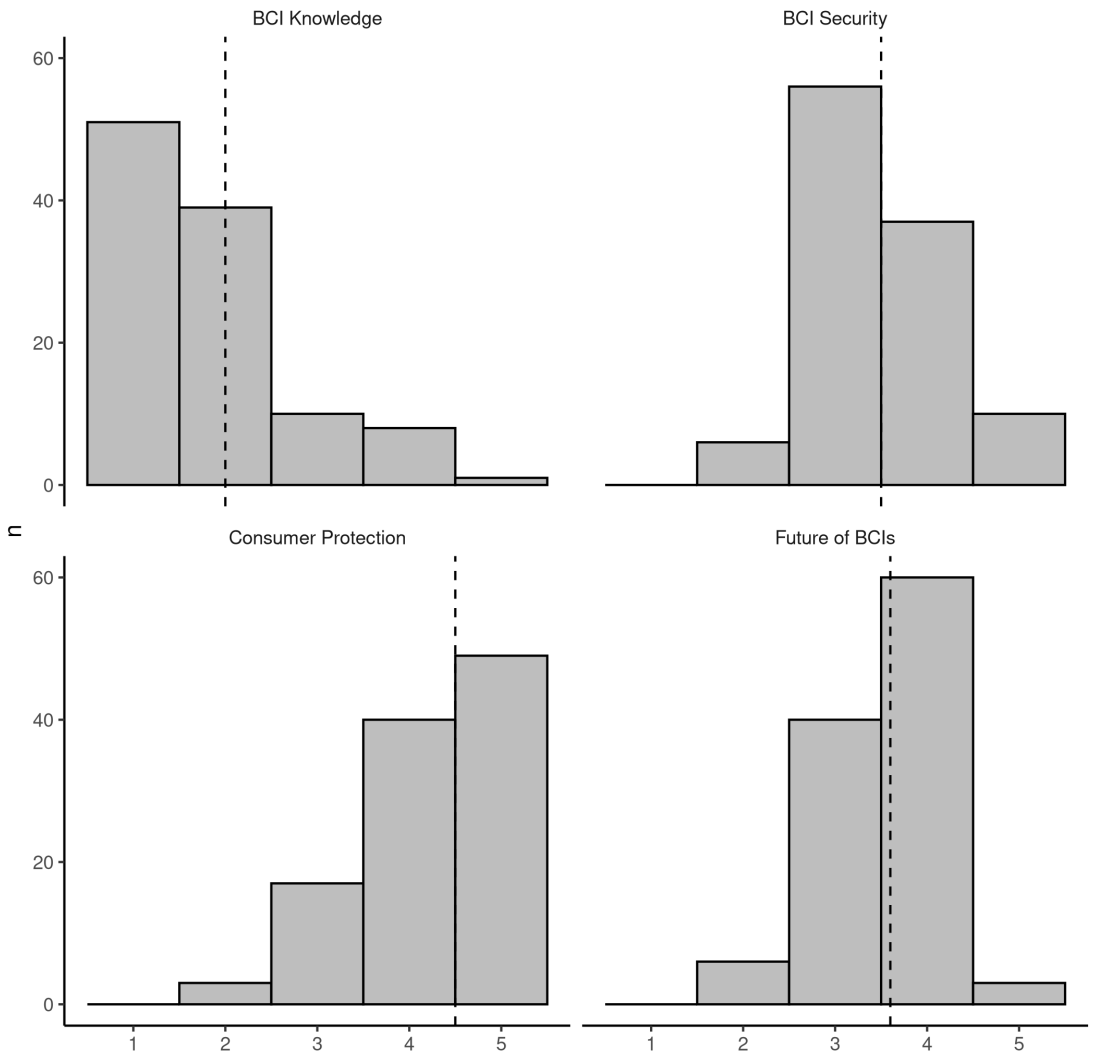

Figure 5.7: Histograms of the four subscales assessed using the BCI Acceptance Scale (BAS). Scores on each subscale are calculated by taking the average of the subscale items after reverse-scoring as appropriate. Dashed lines represent the median values.

data from BCIs as assessed by the Consumer Protection subscale. In general, respondents tended to believe that BCIs would become more common and relevant in the future.

When asked to respond to the statement "A hacker could use data intercepted from a BCI device to infer private information about the user.", a majority of respondents indicated that they agreed ($n = 52$) or strongly agreed ($n = 26$; see

Answer	n
Strongly disagree	4
Disagree	4
Neutral	23
Agree	52
Strongly agree	26

Table 5.9: Frequency table of the responses to the BIS:Security item "A hacker could use data intercepted from a BCI device to infer private information about the user."

Info type	n
Emotional State	59.00
Medical/Health	59.00
Passwords	52.00
Truthfulness	44.00
Gender	43.00
Religious/Political Beliefs	36.00
Sexual Orientation	32.00
Ethnicity	30.00

Table 5.10: Frequency table of the responses to the followup question "What sort of information might they be able to learn (select all that apply)?", shown to respondents who selected *Agree* or *Strongly agree* as their answer to the question in 5.9.

Table 5.9). These participants were asked a followup question: "What sort of information might they be able to learn (select all that apply)?" Responses to the followup question are shown in Table 5.10. The most common types of vulnerable information identified by respondents were Emotional State ($n = 59$) and Medical/Health-related information ($n = 59$), while the least common included Religious/Political Beliefs ($n = 36$), Sexual Orientation ($n = 32$), and Ethnicity ($n = 30$).

5.3.2 Hypothesis Tests

Data were analyzed as described in Section 5.2.3. The median-split Wilcoxon test yields fewer statistically significant results relative to the Spearman test, and

there are no hypotheses for which the Wilcoxon is statistically significant but the Spearman is not.

SeBIS Hypotheses (HS)

Test	Spearman ρ	Spearman p-value	Wilcoxon W	Wilcoxon p-value
HS_1	0.05	0.60	1514.00	0.60
HS_2	0.20	0.04	1780.50	0.03
HS_3	0.27	0.01	1636.00	0.10
HS_4	0.17	0.07	1594.00	0.18

Table 5.11: Results and p-values of Spearman correlation tests and Wilcoxon rank sum test for the SeBIS hypotheses. Wilcoxon tests were conducting by performing a median split on the data based on the relevant SeBIS dimension and testing for a difference between the two groups on the other variable.

The test statistics and p-values of the hypothesis tests on the SeBIS subscales are presented in Table 5.11 and pairwise scatterplots for each hypothesized relationship can be seen in Figure 5.8. Based on the Spearman tests, only HS_2 and HS_3 were associated with statistically significant p values (i.e., $p < 0.05$). Wilcoxon tests also supported HS_2 but did not support any of the others.

$HS_1 : SeBIS_{Securement} \propto BAS_{Security}$ The lack of a significant association between device securement behaviours and concerns about BCI security ($\rho = 0.05, p = 0.6$) suggests, somewhat surprisingly, that respondents' views about BCI security are unrelated to the degree to which they proactively protect their own devices.

$HS_2 : SeBIS_{Securement} \propto \frac{1}{BAS_{Future}}$ The correlation between device securement behaviours and views about the future of BCIs ($\rho = 0.2, p = 0.038$) is statistically significant but in the opposite direction to the hypothesized relationship, suggesting that those who are more concerned with device security are in fact more optimistic about the future of BCIs.

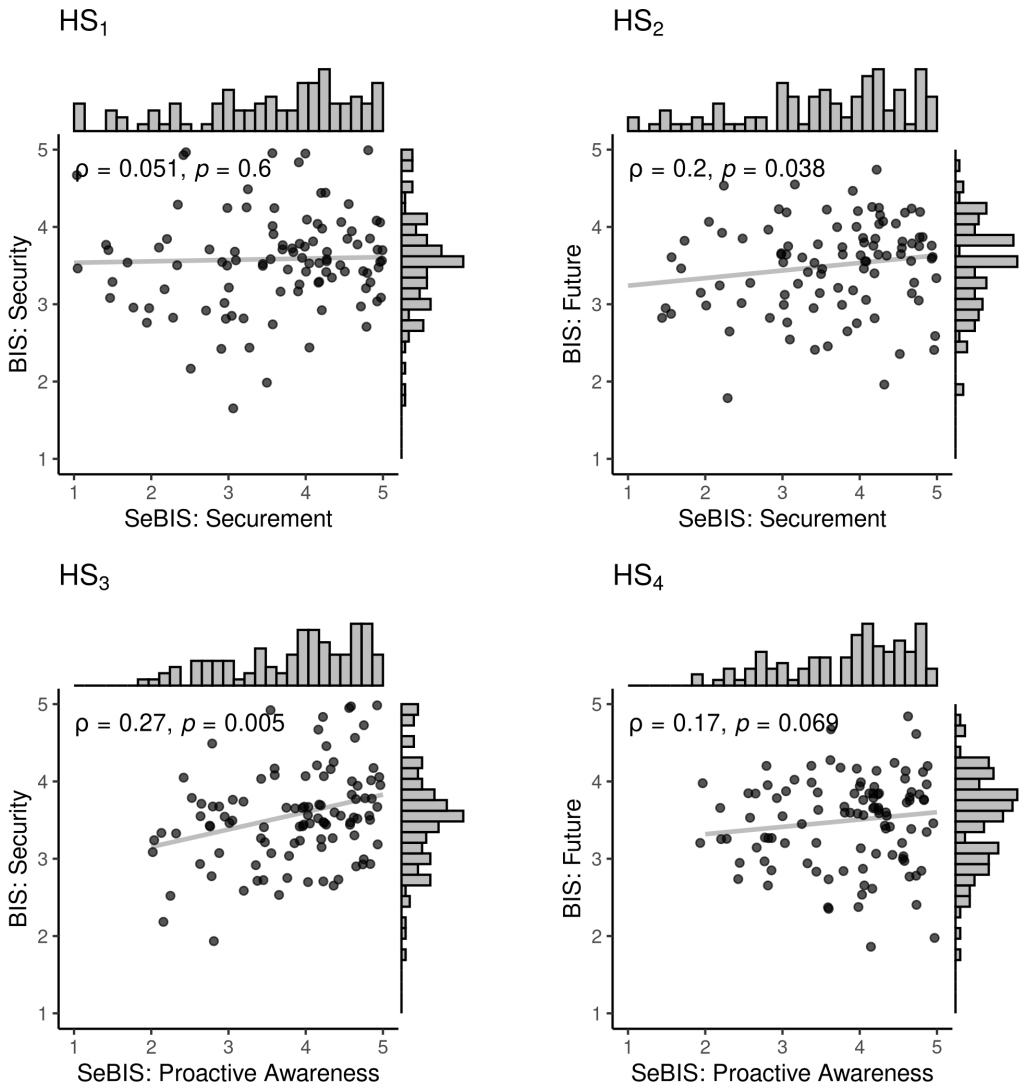

Figure 5.8: Pairwise scatterplots for the SeBIS hypotheses. Spearman ρ and corresponding p-values for each pair of variables is shown in the upper left corner of each plot.

$HS_3 : SeBIS_{ProactiveAwareness} \propto BAS_{Security}$ Of the SeBIS hypotheses, only the relationship between proactive awareness about security practices and concerns about BCI security was supported in the predicted direction by the Spearman test ($\rho = 0.27, p = 0.01$). This result suggests that those who are more proactively aware of security practices are more concerned about the security of BCI devices.

Notably, the Wilcoxon test for this hypothesis was not statistically significant at $p = 0.1$.

$HS_4 : SeBIS_{ProactiveAwareness} \propto \frac{1}{BAS_{Future}}$ The predicted negative relationship between proactive awareness about security practices and the belief that BCIs will be common in the future was not supported. In fact, there appears to be a trend toward a positive association between the two ($\rho = 0.17$), although this is not statistically significant according to the Spearman ($p = 0.07$) or Wilcoxon ($p = 0.18$) tests.

TIPI Hypotheses (HP)

Test	Spearman ρ	Spearman p-value	Wilcoxon W	Wilcoxon p-value
HP_1	-0.12	0.21	1190.50	0.07
HP_2	0.26	0.01	1735.00	0.12
HP_3	0.06	0.55	1591.50	0.50
HP_4	-0.23	0.02	1085.50	0.01
HP_5	0.09	0.35	1585.00	0.53
HP_6	0.20	0.04	1740.00	0.11
HP_7	-0.27	0.01	1162.00	0.05
HP_8	0.20	0.04	1646.00	0.26

Table 5.12: Results and p-values of Spearman correlation tests and Wilcoxon rank sum test for the TIPI hypotheses. Wilcoxon tests were conducting by performing a median split on the data based on the relevant SeBIS dimension and testing for a difference between the two groups on the other variable.

Spearman and Wilcoxon test statistics for the TIPI hypotheses are presented in Table 5.12, and corresponding pairwise scatterplots are shown in Figure 5.9 (HP_{1-4}) and Figure 5.10 (HP_{5-8}).

$HP_1 : TIPI_{Agreeableness} \propto \frac{1}{CRS_{Anxiety}}$ The association between Agreeableness and the Anxiety dimension of the CRS was not statistically significant according to the Spearman ($\rho = -0.12, p = 0.21$) or Wilcoxon tests ($W = 1190.5, p = 0.07$),

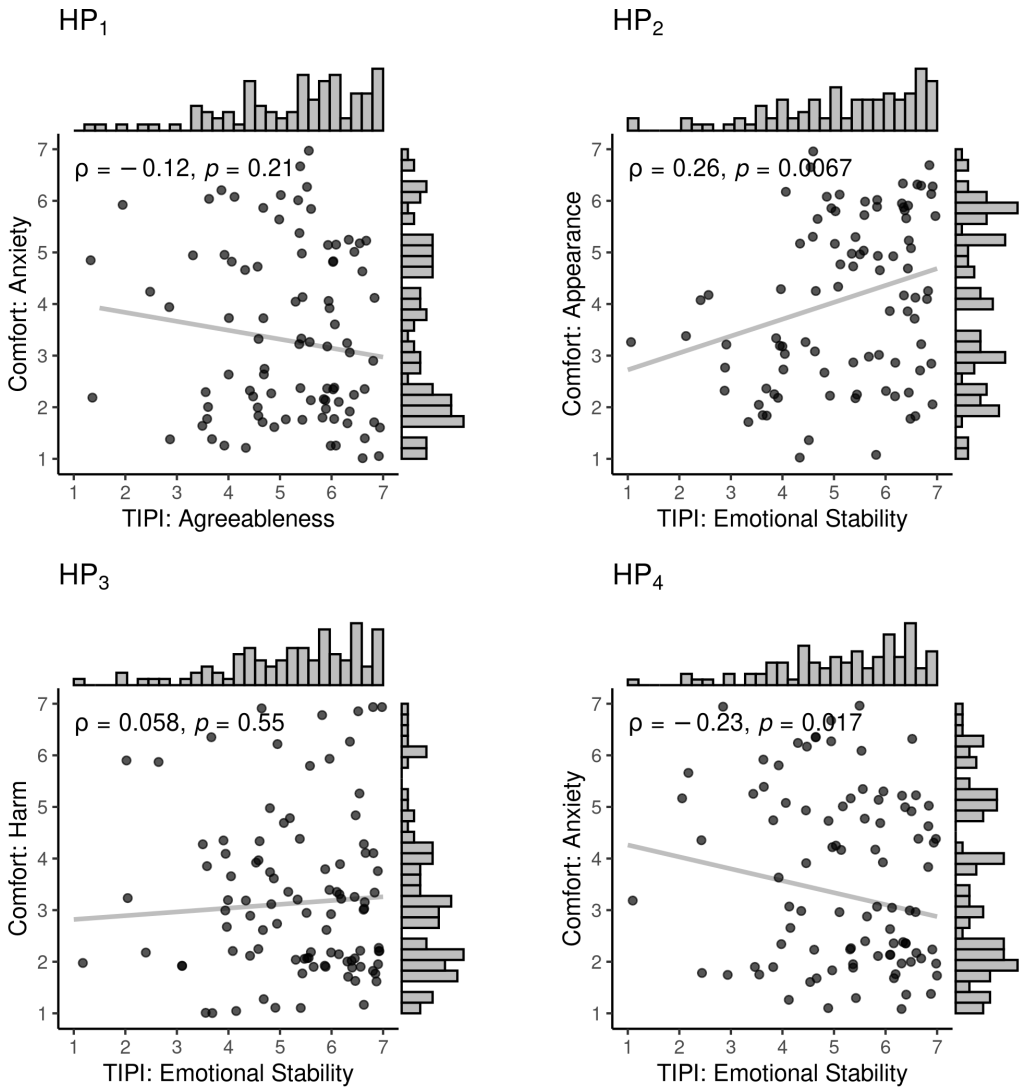

Figure 5.9: Pairwise scatterplots for the first four TIPI hypotheses (HP_{1-4}). Spearman ρ and corresponding p-values for each pair of variables is shown in the upper left corner of each plot.

suggesting that respondents' perceived anxiety associated with the idea of wearing the device is not related to their degree of agreeableness.

$HP_2 : TIPI_{EmotionalStability} \propto CRS_{Appearance}$ The Spearman rank correlation coefficient between Emotional Stability and comfort regarding the appearance of the BCI device revealed a statistically significant positive association of $\rho = 0.26, p < 0.01$, which supports HP_2 that more emotionally stable respondents

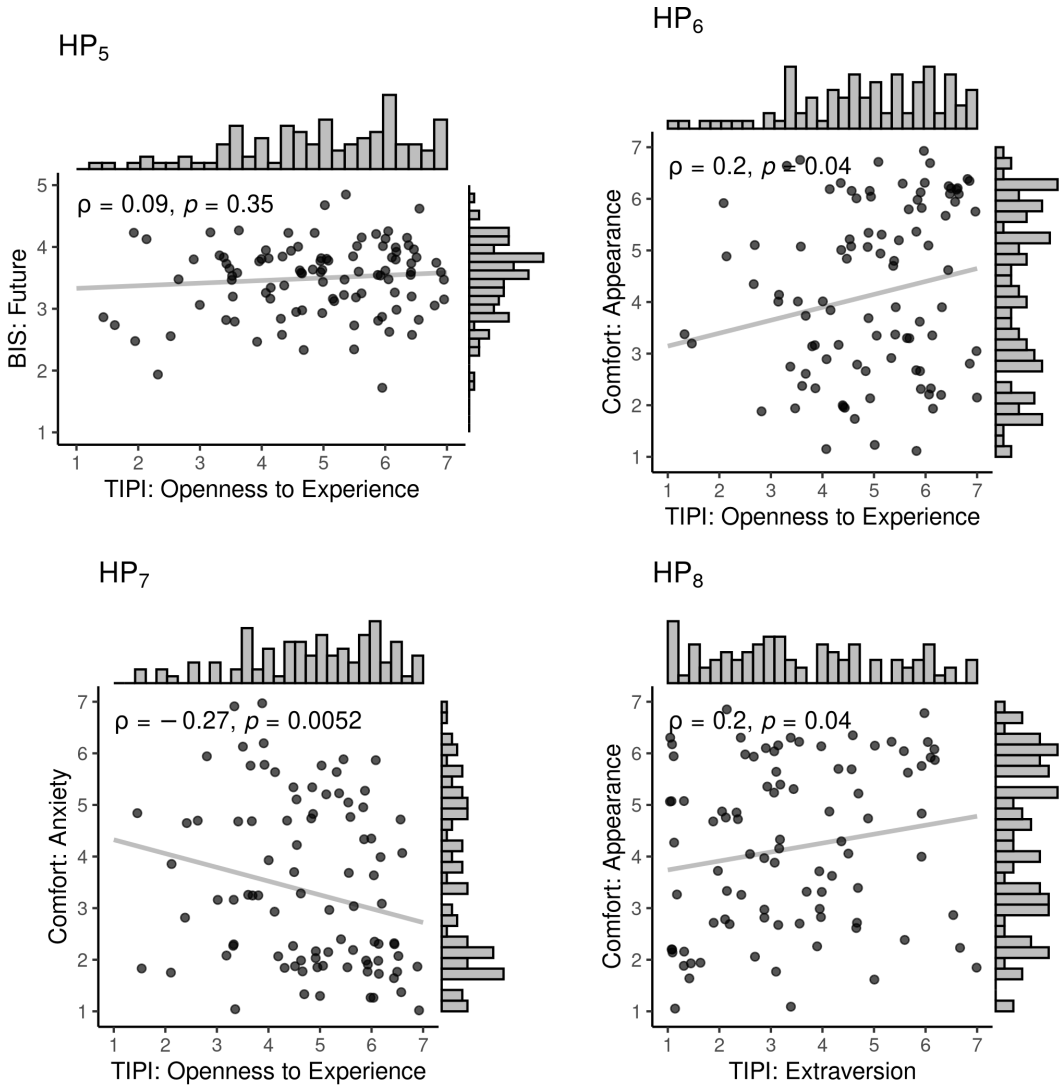

Figure 5.10: Pairwise scatterplots for the last four TIPI hypotheses (HP_{5-8}). Spearman ρ and corresponding p-values for each pair of variables is shown in the upper left corner of each plot.

will be less uncomfortable about the appearance of the device and being seen by others. The Wilcoxon test for this HP_2 did not reach statistical significance ($W = 1735, p = 0.12$).

$HP_3 : TIPI_{EmotionalStability} \propto \frac{1}{CRS_{Harm}}$ Both the Spearman ($\rho = 0.06, p = 0.55$) and Wilcoxon ($W = 1591.50, p = 0.5$) statistics failed to support HP_3 that Emotional Stability is negatively correlated with the belief that the BCI device could

cause harm, suggesting that beliefs about whether the BCI device could cause harm are not related to respondents' degree of Emotional Stability.

$HP_4 : TIPI_{EmotionalStability} \propto \frac{1}{CRS_{Anxiety}}$ The hypothesis that Emotional Stability will be negatively associated with the anxiety dimension of the CRS was supported by both the Spearman ($\rho = -0.23, p = 0.02$) and Wilcoxon ($W = 1085.5, p = 0.01$) tests, indicating that those who are high in Emotional Stability tend to have less anxiety associated with the idea of wearing the BCI device.

$HP_5 : TIPI_{OpennessToExperience} \propto BAS_{Future}$ The hypothesis that Openness to Experience will be positively correlated with the belief that BCIs will be common in the future was not supported by the Spearman ($\rho = 0.09, p = 0.35$) or Wilcoxon ($W = 1585, p = 0.53$) statistics.

$HP_6 : TIPI_{OpennessToExperience} \propto CRS_{Appearance}$ The positive association between Openness to Experience and comfort regarding the appearance of the BCI device was statistically significant according to the Spearman statistic ($\rho = 0.20, p = 0.04$). This result indicates that those who score highly on Openness to Experience are more comfortable with the appearance of the device and what others might think. The Wilcoxon statistic for this hypothesis was not statistically significant ($p = 0.11$).

$HP_7 : TIPI_{OpennessToExperience} \propto \frac{1}{CRS_{Anxiety}}$ Both the Spearman ($\rho = -0.27, p < 0.01$) and Wilcoxon ($W = 1162, p = 0.05$) tests supported HP_7 that Openness to Experience would be negatively associated with anxiety about the idea of wearing the BCI device, suggesting that those higher in this dimension have less anxiety toward the BCI device.

$HP_8 : TIPI_{Extraversion} \propto CRS_{Appearance}$ The hypothesis of a positive association between Extraversion and comfort regarding the appearance of the BCI device was supported by the result of the Spearman test ($\rho = 0.2, p = 0.04$). This result indicates that more extraverted respondents are more comfortable with the appearance of the device and what others might think.

#	Hypothesis	Direction	Supported
HS_1	$SeBIS_{Securement} \sim BAS_{Security}$	Positive	N
HS_2	$SeBIS_{Securement} \sim BAS_{Future}$	Negative	N*
HS_3	$SeBIS_{ProactiveAwareness} \sim BAS_{Security}$	Positive	Y
HS_4	$SeBIS_{ProactiveAwareness} \sim BAS_{Future}$	Negative	N
HP_1	$TIPI_{Agreeableness} \sim CRS_{Anxiety}$	Negative	N
HP_2	$TIPI_{EmotionalStability} \sim CRS_{Appearance}$	Positive	Y**
HP_3	$TIPI_{EmotionalStability} \sim CRS_{Harm}$	Negative	N
HP_4	$TIPI_{EmotionalStability} \sim CRS_{Anxiety}$	Negative	Y
HP_5	$TIPI_{OpennessToExperience} \sim BAS_{Future}$	Positive	N
HP_6	$TIPI_{OpennessToExperience} \sim CRS_{Appearance}$	Positive	Y**
HP_7	$TIPI_{OpennessToExperience} \sim CRS_{Anxiety}$	Negative	Y
HP_8	$TIPI_{Extraversion} \sim CRS_{Appearance}$	Positive	Y**

Table 5.13: Summary of the results of the hypothesis tests indicating whether they were supported by the collected data.

* The relationship described in HS_2 was statistically significant in the opposite (i.e., positive) direction.

** Some hypotheses were supported by the result of the Spearman test but not the Wilcoxon.

5.4 Interpretation

5.4.1 Summary

The aim of this research was to identify and learn about factors that influence or mediate individuals' acceptance of BCIs and concerns about their security. Data were gathered from an online sample of MTurk workers regarding their general personality traits (TIPI), security behaviours (SeBIS), comfort with various dimensions of wearing a BCI (CRS), and opinions on BCIs, their potential role in

society, security concerns, and concerns about data collection/handling (BAS). Based on these data, several trends and relationships emerged, revealing factors that significantly influence acceptance, comfort, and perceived security of BCIs.

Descriptive statistics obtained from the sample indicate that respondents trended toward higher values in all personality dimensions except for Extraversion and had better-than-neutral security practices on all subscales of the SeBIS. In terms of the perceived comfort of a BCI device, respondents tended to report low feelings of anxiety about the device, and were unlikely to endorse the belief that the BCI device could cause harm to the user. The slightly bimodal distribution of the Appearance dimension of the CRS in Figure 5.6 indicates that opinions about the appearance of the BCI device are somewhat polarized.

The sample overall reported quite low prior knowledge of BCIs (Figure 5.7), however 8 respondents rated themselves as *Moderately knowledgeable* and 1 rated themself as *Very knowledgeable*. The remaining BAS subscales (*Future, Consumer, Security*) showed a positive trend, indicating that respondents in this sample generally believed that BCIs would be more relevant in the future, but were concerned about the security of these devices and regulations that govern the collection and use of data.

Hypothesis test results are summarized in Table 5.13. Hypothesis tests related to security behaviours (SeBIS) generated some surprising findings. Contrary to our expectations, there was no evidence of an association between the extent to which respondents protect and secure their own devices and their level of concern about the security of BCIs. It seemed reasonable to assume that this level of concern for the security of one's devices would generalize to hypothetical use of BCI devices as well, but it appears that this is not the case. It was also predicted that device securement behaviours would be negatively associated with optimistic views about the future of BCIs in society. However, these data suggest the opposite, that in

fact those who are more diligent about securing their own devices appear to be more likely to believe that BCIs will be common in the future. While no significant relationship was found between proactive awareness about security practices and views about the future of BCIs, proactive awareness was significantly positively associated with concerns about the security of BCIs. This indicates, somewhat intuitively, that those who are more security-aware are more concerned about the security of BCI devices.

Similarly, significant relationships were discovered between Big 5 personality dimensions (TIPI) and factors relating to comfort and acceptance of BCIs. Emotional Stability, Openness to Experience, and Extraversion were all significantly positively correlated with comfort regarding the appearance of the device and being seen by others, indicating that those who are higher in these traits tend to be more comfortable. Both Openness to Experience and Emotional stability were negatively associated with the Anxiety dimension of the CRS, suggesting that those who are high in these personality traits believe that they would not experience significant anxiety due to using or wearing the device.

These findings demonstrate that personality factors play a role in determining potential users' acceptance and comfort regarding BCIs. Those who are high in openness to experience, extraversion, and emotional stability appear to have fewer barriers to adoption of BCIs. Since BCIs are novel and uncommon, there are significant social acceptance barriers[143] and a high likelihood of drawing attention to oneself if worn in public. With this in mind, it is not particularly surprising that more extraverted, emotionally stable, and adventurous people would be more comfortable with unfamiliar BCI devices than those who are introverted, less emotionally stable, and less open to experiences.

The relationship between security behaviours and perceptions of BCIs appears to be more complicated. The lack of a relationship between device securement

behaviours and concerns about BCI security despite the latter being significantly correlated with proactive awareness about security suggests that respondents base their views of BCI security on their broader understanding of security practices rather than on the way in which they interact with their own devices.

The association between increased device securement behaviours and the belief that BCIs will be more common in the future is of interest for the case of authentication; this may suggest that establishment of robust authentication protocols for BCIs will be an important step in increasing their viability for adoption among the general public.

A substantial majority of respondents indicated that they believe it would be possible for a hacker to infer private information about a user based on BCI data. Some studies[158,159] have indicated the ability of attackers to infer limited personal information about a BCI, such as whether a particular face is familiar, but only if the attacker also has the ability to present stimuli in the user's visual field. This suggests a misunderstanding of the capabilities of current BCI devices, as these attacks are not feasible for real-world use. The types of information that respondents felt were vulnerable are largely consistent with other studies regarding perceptions of biosensor data[157]

5.4.2 Limitations

There is a significant limitation inherent in asking members of the general public to comment and make specific judgements about a complex technology with which they have no prior knowledge or experience. Indeed, the few pictures of one type of BCI device and brief description that were shown to respondents are certainly not sufficient to enable them to give well-informed opinions about, for example, the security of BCI devices overall and their potential to be hacked. The general lack of understanding and prevalence of misinformation with respect to BCIs among

the general population was a known limitation from the beginning of this study, but nonetheless constrains the interpretation. The goal and findings of this study should be interpreted with the understanding that the measures reported here are not intended as an empirical investigation of the usability of BCIs *per se*, but rather an investigation of the *perception of usability* in the context of barriers to acceptance and adoption of BCIs.

Another limiting factor is the restriction of responses to those from Canada and the United States only. This was done to aid interpretability of the findings, especially given that regulations around as well as attitudes toward digital privacy differ significantly across regions, but are relatively similar between the US and Canada. Therefore some additional investigation would be required before these results could be generalized to, for example, the European Union which has significantly more stringent privacy regulations.

5.4.3 Conclusion

The key findings of this study are as follows:

- Despite the majority of respondents having post-secondary education, very reported having any significant amount of knowledge about BCIs.
- Respondents' ratings of the perceived comfort of a BCI device were varied but not particularly negative. The majority of respondents indicated low feelings of anxiety and were unlikely to view the device as potentially harmful. With respect to the appearance of the device, responses were somewhat polarized with roughly the same number of participants reporting negative perceptions as positive ones.
- Respondents tended to indicate that they thought BCIs would be more common in the future. Many were also concerned about the security of BCI

devices, and there was strong support for consumer protection regulations to protect BCI devices and the data derived from them.

- The majority of respondents believed that an attacker with access to BCI data could use that data to learn private information about the user. Physiological factors such as emotional state and health-related information were the most likely to be viewed as vulnerable to this type of attack, where as sociocultural information like religious/political beliefs, gender, sexual orientation, and ethnicity were were less likely.

- Respondents who reported greater proactive awareness about cybersecurity were more likely to be concerned about the security of BCI devices. Counterintuitively, the degree to which respondents reported securing their own devices was not significantly related to their views about the security of BCIs. In fact, those who were more diligent in securing their own devices were more likely to believe that BCIs would become commonplace in the future than those who report low device securement behaviours.

- Personality characteristics were found to be associated with factors related to BCI acceptance. In particular, being high in emotional stability, extraversion, and openness to experience was associated with more positive views about the appearance of the BCI device and lower reported anxiety.

BCIs have been applied with reasonable success in a number of domains, including authentication. However, BCIs have not yet achieved any significant level of adoption among the general population. Significant attention has been given to understanding the usability factors that affect BCI adoption, such as poor reliability and long set-up times, whereas the role of security and privacy concerns in BCI adoption have not been significantly addressed.

The present study was intended to explore relationships between factors related to personality traits, security behaviours, and perceptions of BCIs among an online sample of mostly BCI-naïve MTurk workers. It was expected that relationships would emerge between personal factors (Big 5 personality dimensions, security behaviours) and factors related to BCI acceptance and adoption (CRS and BAS measures). Specific hypothesis tests between the various measures yielded mixed results, but broadly these findings support the notion that security factors as well as personality dimensions influence people's acceptance and comfort with BCIs.

Chapter 6

Conclusions

6.1 Summary

Authentication remains an open problem in cybersecurity. Despite numerous attempts to develop a system to replace text-based passwords as the *de facto* standard for authentication, none have yet emerged as a clear candidate. An ideal authentication system is not only robust against impersonation and other attacks, but also easy to use and minimizes the burden placed on the end-user. Additionally, an ideal authentication system should be easy and cost-effective to deploy in the wild. As described by Bonneau et al. [1] in 2012, all proposed alternative systems fail on at least one of these dimensions. The cybersecurity landscape has changed considerably since 2012, but the general problem of authentication has not.

Emerging technologies may offer novel and unique solutions to the authentication problem. One such technology is brain-computer interfaces (BCIs), which have a number of qualities that are of interest to cybersecurity researchers working on authentication. In particular, BCI-based authentication (or *passthoughts*) has the potential to combine multiple authentication factors into a single step, achieving the security of multi-factor authentication without the added usability burden of the user having to do a separate task for each factor. Passthoughts also have the ability to be revoked or changed in the event of compromise, and can be implemented in such a way as to be unobservable by would-be attackers.

However, much remains unknown about the real-world feasibility of passthoughts, especially with regard to usability. Only a few studies have explicitly addressed the usability of passthought authentication, all of which have significant limitations of either not directly assessing usability or focusing on specific populations with unique needs that do not necessarily reflect the experience of using passthoughts for an average consumer.

The goal of this thesis was to comprehensively explore the usability issues surrounding BCIs and passthoughts, especially in relation to the perception and adoption of these technologies by the wider public. To this end, I applied a variety of HCI research methods including software prototyping, qualitative semi-structured interviews, and quantitative surveys to gain insight into the potential role for BCIs and passthoughts in society.

6.1.1 Timeline of Studies

The studies described in this thesis are presented in the order that they were conducted, beginning with the prototype mental command graphical password system described in Chapter 3. The interview study described in Chapter 4 began during the last stages of attempted usability testing of the prototype when it became clear that further in-person usability testing would not be possible. The interview study and the online survey study from Chapter 5 overlapped significantly in time; the interview study began first, but only three out of the seven total interviews had been conducted at the time that the MTurk survey was launched. As MTurk data collection took only a few hours, the data analysis presented in Chapter 5 was conducted before the conclusion of interviews and analysis of the interview data.

Some of the knowledge gained from the first sessions of the interview study was incorporated into the MTurk study, primarily in the development of the BCI

Acceptance Scale (BAS), of which a number of items were based on interviewee responses. However, this was before data from the interview study had been formally analyzed according to thematic analysis procedures, and as a result the categories that make up the BAS (*Knowledge, Future, Consumer Protection, Security*) are not similar but not identical to the themes derived from thematic analysis of the interview Data (*Safety, Usability, Development*).

6.2 Contributions

In Chapter 3, I describe my design and development of a prototype BCI authentication system which uses directional mental commands to enter a graphical password, similar to the *pattern unlock* paradigm commonly seen in mobile phones. The system works by a user training a classifier to associate particular EEG patterns with discrete commands, and then entering those commands in a specific sequence in order to authenticate. This authenticator provides inherent two-factor authentication because a user must demonstrate knowledge of the command sequence as well as the ability to consistently reproduce the correct EEG states in order to generate the commands. Additionally, it enables changeable biometric authentication because both the command sequence and the association between mental states and commands can be revoked or altered. In the current implementation, the system does not provide full unobservability because the pattern is drawn on a screen; however, the mental states used to generate the commands are unobservable, so the system could be described as *pseudo-unobservable.* The use of mental commands as a passthought-entry mechanism is, to my knowledge, novel and distinct from other passthought systems that have been described in the research literature.

My attempts to conduct a usability study of the prototype were unsuccessful due to technical issues with the Emotiv mental command training process as well as

external factors. In general, the Emotiv system did not meet the expectations set by the company's claims, especially regarding its reliability and the amount of time and effort required to train the classifier. Nonetheless, the process of attempting to train mental commands was informative. A number of strategies were employed in attempts to arrive at a trained classifier, including guidelines suggested by the device manufacturer, Emotiv. These strategies resulted in differential success, but at best were only able to distinguish two commands with limited reliability and a notable bias toward the most recently trained command. In a research context, the proprietary and closed-source nature of the Emotiv system makes it difficult to use optimally. A number of possibilities exist to extend and improve this project.

Chapter 4 describes a qualitative semi-structured interview study that I conducted with a sample of expert BCI users and researchers. An issue which complicates the study of public opinions toward BCIs is the fact that the public is generally poorly informed—or misinformed—about the technology. By talking to BCI experts, I was able to better differentiate between BCI issues that are genuine versus those that are based on poor understanding of the technology or misinformation.

Interviews were conducted with the goal of answering the question *"What are the main barriers preventing adoption of BCIs and passthoughts for the general population?"* Using reflexive thematic analysis,[184,185] I identified three categories of barriers relevant to the research question: perceptions about the safety of BCIs, their usability characteristics, and the need for continued research and development into the technology and its applications. These findings may provide insight and direction for the future development of BCI devices.

Chapter 5 discusses an online survey study I conducted to solicit opinions about BCIs and passthoughts from a population of Amazon Mechanical Turk workers with no prior experience of BCIs. The survey consisted of measures of Big 5

personality traits, security-related behaviours, perceived comfort of BCI devices, and a novel exploratory instrument designed to capture thoughts and impressions about BCI devices. It was hypothesized that the independent factors of personality dimensions and security behaviours would be significantly correlated with outcome measures related to acceptance of BCIs.

Analysis of the survey data revealed associations between the independent and dependent variables. Specifically, it was found that respondents who scored highly in the dimensions of openness to experience, extraversion, and emotional stability were more likely to report more positive impressions and fewer barriers related to BCI use. Additionally, proactive awareness about security was associated with increased concern about the security of BCI devices. Broadly, these findings indicate that individual characteristics affect general perceptions about and openness toward BCI technologies.

6.3 Limitations

Clearly, the most significant limitation of the mental command graphical password authenticator was the lack of success in using it with participants. The failure of the system was due to an inability to train the required number of mental commands such that they could be reliably recognized by the Emotiv mental command classifier. The principal limitation here is the reliance on a proprietary, closed-source platform which impaired the ability to understand the internal workings of the system and to make modifications where needed. Additionally, the participant training protocol is not optimal for training mental commands, and could be improved by having multiple training sessions across several days.

The interview study involved a trade-off of having better-informed participants at the expense of generalizability. This was done in order to circumvent the fact that typical consumers are not aware of or have inaccurate or misinformed beliefs

about BCI technologies; recruiting experts makes it easier to differentiate real issues affecting BCI devices from *perceived* issues based on misunderstanding of the technology. However, since the goal of this study is to understand barriers to BCI and passthought acceptance among the general population, some care should be taken in extrapolating these results.

Another limitation of the interview study is the emphasis of the respondents on the usability of BCIs in general rather than that of passthought authentication. An interesting possibility is that the usability of BCIs is one of the most significant barriers to the specific case of passthoughts, suggesting that research into the usability of passthoughts is perhaps premature. A follow-up interview study could address this question directly.

The interview study suffers from a further limitation stemming from the low number of interviewees ($n = 7$) who were recruited to give interviews. This seems to be an inherent and unavoidable limitation given that the purpose of the study was to interview BCI experts, and very few people have any experience with BCIs whatsoever. In retrospect, the approach of cold-emailing BCI researchers based on their contributions to the BCI research literature was more successful than posting recruitment materials on online BCI-oriented forums (such as *neurobb.com* and *reddit.com/r/bci*), which tend to have very low traffic and activity.

The main limitation of the online questionnaire survey is the lack of knowledge or experience of the sample regarding BCIs. In this case it is important to be very clear in the interpretation of these findings that they are based on respondents *first impressions* of a very basic description and depiction of a BCI device. In particular, it is worth emphasizing that this study is assessing *perceived usability*, which is likely more related to more abstract concepts such as technology acceptance than it is to the actual usability criteria of the device.

Another limiting factor of the Mechanical Turk BCI questionnaire study is the fact that responses were limited to individuals located in Canada or the United States only. This approach was chosen to improve interpretability, especially given that attitudes and regulations regarding privacy vary significantly across regions. It may be of interest in future studies to compare responses from regions with different regulatory landscape, such as the European Union.

Additionally, while the population of MTurk workers is relatively diverse, they tend to differ from the general population in significant ways, such as having above-average educational attainment. It is possible that the knowledge, opinions, and attitudes toward BCIs represented in the MTurk sample could be different from those of the general population in potentially significant ways.

Finally, hypothesis testing of the MTurk study data was limited to twelve *a priori* hypotheses only; a number of potentially interesting relationships were not directly addressed. For example, no tests were conducted to assess the relationship of age, education level, or level of knowledge about BCIs with other variables of interest. There remains the possibility of revisiting these data to conduct a more comprehensive exploratory analysis.

6.4 Future Work

A significant amount of work could be done to improve the mental command authenticator prototype. A priority would be to extend the application to support additional hardware, starting with OpenBCI as it would be the most flexible. Doing so would also require the development of other tools such as a mental command classifier and training platform, which would require the application as a whole to be modularized. Also worth considering is the general format of the application; the prototype presented in Chapter 3 was implemented as a web

application mostly for convenience and the ability to iterate development rapidly and flexibly, but a web app may not be the best solution overall.

The data collected from the online MTurk survey have not been fully exhausted; the analysis described in Chapter 5 was limited to descriptive statistics and testing *a priori* hypotheses. It would likely be worthwhile to explore some of the other potential relationships within the data. For example, it would be interesting to see whether the few individuals in the sample who rated themselves as moderately knowledgeable or very knowledgeable about BCIs scored differently on the outcome measures than those who rated themselves less knowledgeable. A full exploratory analysis of the dataset seems warranted.

6.5 Final Thoughts

The current state of BCI technologies leaves much to be desired. We are certainly in the early days of BCI development and there is a great deal left to learn. Nonetheless, the recent emergence of low cost consumer-oriented BCI devices is a major step forward and has led to an improved understanding of what BCI devices can do and what their place in society might be. Furthermore, while the general public has been slow to adopt BCIs, there are a number of promising and meaningful use-cases for BCIs to improve the lives of individuals living with various disabilities. Looking to the future, the impressive capabilities demonstrated by invasive BCI systems gives a general idea of what may be possible with non-invasive commercial systems as neuroimaging technologies improve and become more accessible.

Concerning passthoughts, the main takeaway is that more development is needed into the general usefulness and applicability of BCIs in other domains before passthought authentication would be feasible for average consumers. The consensus of BCI experts in the interview study (Chapter 4) is that BCI-based

interaction is too error-prone and has too low of an information transfer rate to be practically useful in the real world, and people would not be willing to buy and use a BCI device for the purpose of authentication only. Taking all three studies into account, my overarching conclusion is that passthoughts can only be as usable as the BCI systems that they rely on.

Bibliography

[1] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes". In: *2012 IEEE Symposium on Security and Privacy*. May 2012. DOI: 10.1109/sp.2012.44. URL: https://doi.org/10.1109/sp.2012.44.

[2] J. Bonneau. "The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords". In: *2012 IEEE Symposium on Security and Privacy*. 2012, pp. 538–552.

[3] Sonia Chiasson and P. van Oorschot. "Quantifying the security advantage of password expiration policies". In: *Designs, Codes and Cryptography* 77 (Dec. 2015). DOI: 10.1007/s10623-015-0071-9.

[4] Eiji Hayashi and Jason Hong. "A diary study of password usage in daily life". In: *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*. 2011. DOI: 10.1145/1978942.1979326. URL: https://doi.org/10.1145/1978942.1979326.

[5] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. "The Tangled Web of Password Reuse". In: *Proceedings 2014 Network and Distributed System Security Symposium*. 2014. DOI: 10.14722/ndss.2014.23357. URL: https://doi.org/10.14722/ndss.2014.23357.

[6] Zhang Rui and Zheng Yan. "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification". In: *IEEE Access* 7 (2019), pp. 5994–6009. DOI: 10.1109/access.2018.2889996. URL: https://doi.org/10.1109/access.2018.2889996.

[7] Ruud M. Bolle, Jonathan H. Connell, and Nalini K. Ratha. "Biometric Perils and Patches". In: *Pattern Recognition* 35.12 (2002), pp. 2727–2738. DOI: 10.1016/s0031-3203(01)00247-3. URL: https://doi.org/10.1016/s0031-3203(01)00247-3.

[8] MinYi Jeong, Chulhan Lee, Jongsun Kim, Jeung-Yoon Choi, Kar-Ann Toh, and Jaihie Kim. "Changeable Biometrics for Appearance Based Face Recognition". In: *2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference*. Sept. 2006. DOI: 10.1109/bcc.2006.4341629. URL: https://doi.org/10.1109/bcc.2006.4341629.

[9] S. Chaudhari, S. S. Tomar, and A. Rawat. "Design, implementation and analysis of multi layer, Multi Factor Authentication (MFA) setup for webmail access in multi trust networks". In: *2011 International Conference*

on Emerging Trends in Networks and Computer Communications (ETNCC). Apr. 2011. DOI: 10.1109/etncc.2011.5958480. URL: https://doi.org/10.1109/etncc.2011.5958480.

[10] Nancie Gunson, Diarmid Marshall, Hazel Morton, and Mervyn Jack. "User Perceptions of Security and Usability of Single-Factor and Two-Factor Authentication in Automated Telephone Banking". In: *Computers & Security* 30.4 (2011), pp. 208–220. DOI: 10.1016/j.cose.2010.12.001. URL: https://doi.org/10.1016/j.cose.2010.12.001.

[11] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and M. Angela Sasse. ""They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking". In: *Proceedings 2015 Workshop on Usable Security*. 2015. DOI: 10.14722/usec.2015.23001. URL: https://doi.org/10.14722/usec.2015.23001.

[12] Sanchari Das, Andrew Dingman, and L. Jean Camp. "Why Johnny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key". In: *Financial Cryptography and Data Security*. Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2018, pp. 160–179. DOI: 10.1007/978-3-662-58387-6_9. URL: https://doi.org/10.1007/978-3-662-58387-6_9.

[13] Sanchari Das, Bingxi Wang, Zachary Tingle, and L. Jean Camp. "Evaluating User Perception of Multi-Factor Authentication: A Systematic Review". In: *HAISA*. 2019.

[14] Julie Thorpe, P. C. van Oorschot, and Anil Somayaji. "Pass-Thoughts : Authenticating With Our Minds". In: *Proceedings of the 2005 workshop on New security paradigm* (2005), pp. 45–56. ISSN: 1475-2859. DOI: 10/dt5ht4. URL: https://doi.org/10/dt5ht4.

[15] Nick Merrill, Max T. Curran, Swapan Gandhi, and John Chuang. "One-Step, Three-Factor Passthought Authentication With Custom-Fit, In-Ear Eeg". In: *Frontiers in Neuroscience* 13 (2019). DOI: 10.3389/fnins.2019.00354. URL: https://doi.org/10.3389/fnins.2019.00354.

[16] M. Sasse, S. Brostoff, and D. Weirich. "Transforming the 'Weakest Link' - a Human-Computer Interaction Approach to Usable and Effective security". In: *Internet and Wireless Security*. Internet and Wireless Security. IET, pp. 243–262. DOI: 10.1049/pbbt004e_ch15. URL: https://doi.org/10.1049/pbbt004e_ch15.

[17] Catherine S. Weir, G. Douglas, Martin Carruthers, and M. Jack. "User perceptions of security, convenience and usability for ebanking authentication tokens". In: *Comput. Secur.* 28 (2009), pp. 47–62.

[18] John Chuang, Hamilton Nguyen, Charles Wang, and Benjamin Johnson. "I Think, Therefore I Am: Usability and Security of Authentication Using Brainwaves". In: *Financial Cryptography and Data Security*. Ed. by Andrew A. Adams, Michael Brenner, and Matthew Smith. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 1–16. ISBN: 978-3-642-41320-9.

[19] Sidas Saulynas and Ravi Kuber. "Towards Brain-Computer Interface (BCI) and Gestural-Based Authentication for Individuals Who Are Blind". In: *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility*. ASSETS '17. Baltimore, Maryland, USA: Association for Computing Machinery, 2017, pp. 403–404. ISBN: 9781450349260. DOI: 10.1145/3132525.3134785. URL: https://doi.org/10.1145/3132525.3134785.

[20] Sidas Saulynas, Charles Lechner, and Ravi Kuber. "Towards the Use of Brain-Computer Interface and Gestural Technologies As a Potential Alternative To Pin Authentication". In: *International Journal of Human-Computer Interaction* 34.5 (2018), pp. 433–444. DOI: 10.1080/10447318.2017.1357905. eprint: https://doi.org/10.1080/10447318.2017.1357905. URL: https://doi.org/10.1080/10447318.2017.1357905.

[21] Kevin Crowston. "Amazon Mechanical Turk: A Research Tool for Organizations and Information Systems Scholars". In: *Shaping the Future of ICT Research. Methods and Approaches*. Ed. by Anol Bhattacherjee and Brian Fitzgerald. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 210–221. ISBN: 978-3-642-35142-6.

[22] Leigh R. Hochberg, Daniel Bacher, Beata Jarosiewicz, Nicolas Y. Masse, John D. Simeral, Joern Vogel, Sami Haddadin, Jie Liu, Sydney S. Cash, Patrick van der Smagt, and John P. Donoghue. "Reach and Grasp By People With Tetraplegia Using a Neurally Controlled Robotic Arm". In: *Nature* 485.7398 (2012), pp. 372–375. DOI: 10.1038/nature11076. URL: https://doi.org/10.1038/nature11076.

[23] Takufumi Yanagisawa, Masayuki Hirata, Youichi Saitoh, Haruhiko Kishima, Kojiro Matsushita, Tetsu Goto, Ryohei Fukuma, Hiroshi Yokoi, Yukiyasu Kamitani, and Toshiki Yoshimine. "Electrocorticographic Control of a Prosthetic Arm in Paralyzed Patients". In: *Annals of Neurology* 71.3 (2011), pp. 353–361. DOI: 10.1002/ana.22613. URL: https://doi.org/10.1002/ana.22613.

[24] Alexander J. Doud, John P. Lucas, Marc T. Pisansky, and Bin He. "Continuous Three-Dimensional Control of a Virtual Helicopter Using a Motor Imagery Based Brain-Computer Interface". In: *PLoS ONE* 6.10 (2011), e26322. DOI: 10.1371/journal.pone.0026322. URL: https://doi.org/10.1371/journal.pone.0026322.

[25] Gert Pfurtscheller, Bernhard Graimann, and Christa Neuper. "EEG-Based Brain-Computer Interface System". In: *Wiley Encyclopedia of Biomedical Engineering*. Wiley Encyclopedia of Biomedical Engineering. John Wiley & Sons, Inc., 2006. DOI: 10.1002/9780471740360.ebs1309. URL: https://doi.org/10.1002/9780471740360.ebs1309.

[26] Noman Naseer and Keum-Shik Hong. "Fnirs-Based Brain-Computer Interfaces: a Review". In: *Frontiers in Human Neuroscience* 9 (2015). DOI: 10.3389/fnhum.2015.00003. URL: https://doi.org/10.3389/fnhum.2015.00003.

[27] Abidemi B. Ajiboye and Robert F. Kirsch. "Invasive Brain-Computer Interfaces for Functional Restoration". In: *Neuromodulation*. Neuromodulation. Elsevier, 2018, pp. 379–391. DOI: 10.1016/b978-0-12-805353-9.00027-9. URL: https://doi.org/10.1016/b978-0-12-805353-9.00027-9.

[28] Renishaw plc. *Renishaw promotes robotic stereoelectroencephalography (SEEG) at ILAE*. 2020. URL: https://www.renishaw.com/ (visited on 06/26/2020).

[29] Pedro Amaral, Francisco Sales, João Paulo Cunha, Paulo Dias, and Jose Maria Fernandes. "Multimodal application for visualization and manipulation of Electrocorticography data". In: Jan. 2007.

[30] Blackrock Microsystems. *Utah Array: The benchmark for multichannel, high-density neural recording*. URL: https://www.blackrockmicro.com/electrode-types/utah-array/ (visited on 06/26/2020).

[31] Peter A. Crosby. "Cochlear Implant System for an Auditory Prosthesis". In: *The Journal of the Acoustical Society of America* 79.4 (1986), pp. 1197–1197. DOI: 10.1121/1.393367. URL: https://doi.org/10.1121/1.393367.

[32] Eric C Leuthardt, Gerwin Schalk, Jonathan R Wolpaw, Jeffrey G Ojemann, and Daniel W Moran. "A Brain-Computer Interface Using Electrocorticographic Signals in Humans". In: *Journal of Neural Engineering* 1.2 (2004), pp. 63–71. DOI: 10.1088/1741-2560/1/2/001. URL: https://doi.org/10.1088/1741-2560/1/2/001.

[33] Leigh R. Hochberg, Mijail D. Serruya, Gerhard M. Friehs, Jon A. Mukand, Maryam Saleh, Abraham H. Caplan, Almut Branner, David Chen, Richard D. Penn, and John P. Donoghue. "Neuronal Ensemble Control of Prosthetic Devices By a Human With Tetraplegia". In: *Nature* 442.7099 (2006), pp. 164–171. DOI: 10.1038/nature04970. URL: https://doi.org/10.1038/nature04970.

[34] G Schalk, K J Miller, N R Anderson, J A Wilson, M D Smyth, J G Ojemann, D W Moran, J R Wolpaw, and E C Leuthardt. "Two-Dimensional Movement Control Using Electrocorticographic Signals in Humans". In: *Journal of Neural Engineering* 5.1 (2008), pp. 75–84. DOI: 10.1088/1741-2560/5/1/008. URL: https://doi.org/10.1088/1741-2560/5/1/008.

[35] Gerwin Schalk and Eric C. Leuthardt. "Brain-Computer Interfaces Using Electrocorticographic Signals". In: *IEEE Reviews in Biomedical Engineering* 4 (2011), pp. 140–154. DOI: 10.1109/rbme.2011.2172408. URL: https://doi.org/10.1109/rbme.2011.2172408.

[36] Sumeet Vadera, Amar R. Marathe, Jorge Gonzalez-Martinez, and Dawn M. Taylor. "Stereoelectroencephalography for Continuous Two-Dimensional Cursor Control in a Brain-Machine Interface". In: *Neurosurgical Focus* 34.6 (2013), E3. DOI: 10.3171/2013.3.focus1373. URL: https://doi.org/10.3171/2013.3.focus1373.

[37] Wei Wang, Jennifer L. Collinger, Alan D. Degenhart, Elizabeth C. Tyler-Kabara, Andrew B. Schwartz, Daniel W. Moran, Douglas J. Weber, Brian Wodlinger, Ramana K. Vinjamuri, Robin C. Ashmore, John W. Kelly, and Michael L. Boninger. "An Electrocorticographic Brain Interface in an Individual With Tetraplegia". In: *PLoS ONE* 8.2 (2013), e55344. DOI: 10.1371/journal.pone.0055344. URL: https://doi.org/10.1371/journal.pone.0055344.

[38] Mariska J. Vansteensel, Elmar G.M. Pels, Martin G. Bleichner, Mariana P. Branco, Timothy Denison, Zachary V. Freudenburg, Peter Gosselaar, Sacha Leinders, Thomas H. Ottens, Max A. Van Den Boom, Peter C. Van Rijen, Erik J. Aarnoutse, and Nick F. Ramsey. "Fully Implanted Brain-Computer Interface in a Locked-In Patient With Als". In: *New England Journal of Medicine* 375.21 (2016), pp. 2060–2066. DOI: 10.1056/nejmoa1608085. URL: https://doi.org/10.1056/nejmoa1608085.

[39] Chethan Pandarinath, Paul Nuyujukian, Christine H Blabe, Brittany L Sorice, Jad Saab, Francis R Willett, Leigh R Hochberg, Krishna V Shenoy, and Jaimie M Henderson. "High Performance Communication By People With Paralysis Using an Intracortical Brain-Computer Interface". In: *eLife* 6 (2017). DOI: 10.7554/elife.18554. URL: https://doi.org/10.7554/elife.18554.

[40] Xiaomei Pei, Dennis L Barbour, Eric C Leuthardt, and Gerwin Schalk. "Decoding Vowels and Consonants in Spoken and Imagined Words Using Electrocorticographic Signals in Humans". In: *Journal of Neural Engineering* 8.4 (2011), p. 046028. DOI: 10.1088/1741-2560/8/4/046028. URL: https://doi.org/10.1088/1741-2560/8/4/046028.

[41] Gopala K. Anumanchipalli, Josh Chartier, and Edward F. Chang. "Speech Synthesis From Neural Decoding of Spoken Sentences". In: *Nature* 568.7753 (2019), pp. 493–498. DOI: 10.1038/s41586-019-1119-1. URL: https://doi.org/10.1038/s41586-019-1119-1.

[42] Jennifer L Collinger, Brian Wodlinger, John E Downey, Wei Wang, Elizabeth C Tyler-Kabara, Douglas J Weber, Angus JC McMorland, Meel Velliste, Michael L Boninger, and Andrew B Schwartz. "High-Performance Neuroprosthetic Control By an Individual With Tetraplegia". In: *The Lancet* 381.9866 (2013), pp. 557–564. DOI: 10.1016/s0140-6736(12)61816-9. URL: https://doi.org/10.1016/s0140-6736(12)61816-9.

[43] Alim Louis Benabid, Thomas Costecalde, Andrey Eliseyev, Guillaume Charvet, Alexandre Verney, Serpil Karakas, Michael Foerster, Aurélien Lambert, Boris Morinière, Neil Abroug, Marie-Caroline Schaeffer, Alexandre Moly, Fabien Sauter-Starace, David Ratel, Cecile Moro, Napoleon Torres-Martinez, Lilia Langar, Manuela Oddoux, Mircea Polosan, Stephane Pezzani, Vincent Auboiroux, Tetiana Aksenova, Corinne Mestais, and Stephan Chabardes. "An Exoskeleton Controlled By an Epidural Wireless Brain-Machine Interface in a Tetraplegic Patient: a Proof-Of-Concept Demonstration". In: *The Lancet Neurology* 18.12 (2019), pp. 1112–1122. DOI: 10.1016/s1474-4422(19)30321-7. URL: https://doi.org/10.1016/s1474-4422(19)30321-7.

[44] P. Hunter Peckham. "The History of Neuromuscular Electrical Stimulation-The Evolution of Functional Neuromuscular Stimulation and Future Directions". In: *Neuromodulation*. Neuromodulation. Elsevier, 2018, pp. 1131–1135. DOI: 10.1016/b978-0-12-805353-9.00093-0. URL: https://doi.org/10.1016/b978-0-12-805353-9.00093-0.

[45] Chad E. Bouton, Ammar Shaikhouni, Nicholas V. Annetta, Marcia A. Bockbrader, David A. Friedenberg, Dylan M. Nielson, Gaurav Sharma, Per B. Sederberg, Bradley C. Glenn, W. Jerry Mysiw, Austin G. Morgan, Milind Deogaonkar, and Ali R. Rezai. "Restoring Cortical Control of Functional Movement in a Human With Quadriplegia". In: *Nature* 533.7602 (2016), pp. 247–250. DOI: 10.1038/nature17435. URL: https://doi.org/10.1038/nature17435.

[46] A Bolu Ajiboye, Francis R Willett, Daniel R Young, William D Memberg, Brian A Murphy, Jonathan P Miller, Benjamin L Walter, Jennifer A Sweet, Harry A Hoyen, Michael W Keith, P Hunter Peckham, John D Simeral, John P Donoghue, Leigh R Hochberg, and Robert F Kirsch. "Restoration of Reaching and Grasping Movements Through Brain-Controlled Muscle Stimulation in a Person With Tetraplegia: a Proof-Of-Concept Demonstration". In: *The Lancet* 2018-April.10081 (2018), pp. 901–905. ISSN: 15206149. DOI: 10/gf6jdn. URL: https://doi.org/10/gf6jdn.

[47] L F Haas. "Hans Berger (1873-1941), Richard Caton (1842-1926), and Electroencephalography". In: *Journal of Neurology, Neurosurgery & Psychiatry* 74.1 (2003), pp. 9–9. DOI: 10.1136/jnnp.74.1.9. URL: https://doi.org/10.1136/jnnp.74.1.9.

[48] J J Vidal. "Toward Direct Brain-Computer Communication". In: *Annual Review of Biophysics and Bioengineering* 2.1 (1973), pp. 157–180. DOI: 10.1146/annurev.bb.02.060173.001105. URL: https://doi.org/10.1146/annurev.bb.02.060173.001105.

[49] J.J. Vidal. "Real-Time Detection of Brain Events in Eeg". In: *Proceedings of the IEEE* 65.5 (1977), pp. 633–641. DOI: 10.1109/proc.1977.10542. URL: https://doi.org/10.1109/proc.1977.10542.

[50] S. Bozinovski, M. Sestakov, and L. Bozinovska. "Using EEG alpha rhythm to control a mobile robot". In: *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. 1988. DOI: 10.1109/iembs.1988.95357. URL: https://doi.org/10.1109/iembs.1988.95357.

[51] S. Bozinovski. "Mobile Robot Trajectory Control: From Fixed Rails to Direct Bioelectric Control". In: *Proceedings of the IEEE International Workshop on Intelligent Motion Control*. 1990. DOI: 10.1109/imc.1990.687362. URL: https://doi.org/10.1109/imc.1990.687362.

[52] Erich E. Sutter. "The Brain Response Interface: Communication Through Visually-Induced Electrical Brain Responses". In: *Journal of Microcomputer Applications* 15.1 (1992), pp. 31–45. DOI: 10.1016/0745-7138(92)90045-7. URL: https://doi.org/10.1016/0745-7138(92)90045-7.

[53] M. Middendorf, G. McMillan, G. Calhoun, and K.S. Jones. "Brain-Computer Interfaces Based on the Steady-State Visual-Evoked Response". In: *IEEE Transactions on Rehabilitation Engineering* 8.2 (2000), pp. 211–214. DOI: 10.1109/86.847819. URL: https://doi.org/10.1109/86.847819.

[54] Jonathan R. Wolpaw. "Brain-computer interfaces (BCIs) for communication and control". In: *Proceedings of the 9th international ACM SIGACCESS conference on Computers and accessibility - Assets '07*. 2007. DOI: 10.1145/1296843.1296845. URL: https://doi.org/10.1145/1296843.1296845.

[55] NeuroSky. *NeuroSky: Body and Mind. Quantified.* 2020. URL: http://neurosky.com/ (visited on 06/28/2020).

[56] InteraXon Inc. *Muse: Meditation Made Easy with the Muse Headband.* 2020. URL: https://choosemuse.com/ (visited on 06/26/2020).

[57] Emotiv Inc. *Emotiv: Neurotech for the Global Community.* 2020. URL: https://www.emotiv.com/ (visited on 05/12/2020).

[58] OpenBCI. *OpenBCI: Open Source Brain-Computer Interfaces*. 2020. URL: https://openbci.com/ (visited on 06/23/2020).

[59] Costantino Iadecola. "Neurovascular Regulation in the Normal Brain and in Alzheimer's Disease". In: *Nature Reviews Neuroscience* 5.5 (2004), pp. 347–360. DOI: 10.1038/nrn1387. URL: https://doi.org/10.1038/nrn1387.

[60] F. Jobsis. "Noninvasive, Infrared Monitoring of Cerebral and Myocardial Oxygen Sufficiency and Circulatory Parameters". In: *Science* 198.4323 (1977), pp. 1264–1267. DOI: 10.1126/science.929199. URL: https://doi.org/10.1126/science.929199.

[61] Shirley M Coyle, Tomás E Ward, and Charles M Markham. "Brain-Computer Interface Using a Simplified Functional Near-Infrared Spectroscopy System". In: *Journal of Neural Engineering* 4.3 (2007), pp. 219–226. DOI: 10.1088/1741-2560/4/3/007. URL: https://doi.org/10.1088/1741-2560/4/3/007.

[62] Shirley Coyle, Tomás Ward, Charles Markham, and Gary McDarby. "On the Suitability of Near-Infrared (NIR) Systems for Next-Generation Brain-Computer Interfaces". In: *Physiological Measurement* 25.4 (2004), pp. 815–822. DOI: 10.1088/0967-3334/25/4/003. URL: https://doi.org/10.1088/0967-3334/25/4/003.

[63] Thorsten O Zander and Christian Kothe. "Towards Passive Brain-Computer Interfaces: Applying Brain-Computer Interface Technology To Human-Machine Systems in General". In: *Journal of Neural Engineering* 8.2 (2011), p. 025005. DOI: 10.1088/1741-2560/8/2/025005. URL: https://doi.org/10.1088/1741-2560/8/2/025005.

[64] Bosworth, Russell, and Jacob. "Update of Fnirs As an Input To Brain-Computer Interfaces: a Review of Research From the Tufts Human-Computer Interaction Laboratory". In: *Photonics* 6.3 (2019), p. 90. DOI: 10.3390/photonics6030090. URL: https://doi.org/10.3390/photonics6030090.

[65] Daniel Afergan, Evan M. Peck, Erin T. Solovey, Andrew Jenkins, Samuel W. Hincks, Eli T. Brown, Remco Chang, and Robert J.K. Jacob. "Dynamic difficulty using brain metrics of workload". In: (2014). DOI: 10.1145/2556288.2557230. URL: https://doi.org/10.1145/2556288.2557230.

[66] Matti Hämäläinen, Riitta Hari, Risto J. Ilmoniemi, Jukka Knuutila, and Olli V. Lounasmaa. "Magnetoencephalography-Theory, Instrumentation, and Applications To Noninvasive Studies of the Working Human Brain". In: *Reviews of Modern Physics* 65.2 (1993), pp. 413–497. DOI: 10.1103/revmodphys.65.413. URL: https://doi.org/10.1103/revmodphys.65.413.

[67] Rabie A. Ramadan and Athanasios V. Vasilakos. "Brain Computer Interface: Control Signals Review". In: *Neurocomputing* 223 (2017), pp. 26–44. DOI: 10.1016/j.neucom.2016.10.024. URL: https://doi.org/10.1016/j.neucom.2016.10.024.

[68] Elena Boto, Niall Holmes, James Leggett, Gillian Roberts, Vishal Shah, Sofie S. Meyer, Leonardo Duque Muñoz, Karen J. Mullinger, Tim M. Tierney, Sven Bestmann, Gareth R. Barnes, Richard Bowtell, and Matthew J. Brookes. "Moving Magnetoencephalography Towards Real-World Applications With a Wearable System". In: *Nature* 555.7698 (2018), pp. 657–661. DOI: 10.1038/nature26147. URL: https://doi.org/10.1038/nature26147.

[69] Apostolos P. Georgopoulos, Frederick J. P. Langheim, Arthur C. Leuthold, and Alexander N. Merkle. "Magnetoencephalographic Signals Predict Movement Trajectory in Space". In: *Experimental Brain Research* 167.1 (2005), pp. 132–135. DOI: 10.1007/s00221-005-0028-8. URL: https://doi.org/10.1007/s00221-005-0028-8.

[70] Thomas Navin Lal, Niels Birbaumer, Bernhard Schölkopf, Michael Schröder, N. Jeremy Hill, Hubert Preissl, Thilo Hinterberger, Jürgen Mellinger, Martin Bogdan, Wolfgang Rosenstiel, and Thomas Hofmann. "A brain computer interface with online feedback based on magnetoencephalography". In: *Proceedings of the 22nd international conference on Machine learning - ICML '05*. 2005. DOI: 10.1145/1102351.1102410. URL: https://doi.org/10.1145/1102351.1102410.

[71] Jürgen Mellinger, Gerwin Schalk, Christoph Braun, Hubert Preissl, Wolfgang Rosenstiel, Niels Birbaumer, and Andrea Kübler. "An Meg-Based Brain-Computer Interface (BCI)". In: *NeuroImage* 36.3 (2007), pp. 581–593. DOI: 10.1016/j.neuroimage.2007.03.019. URL: https://doi.org/10.1016/j.neuroimage.2007.03.019.

[72] Noha I. Sabra and Manal Abdel Wahed. "The use of MEG-based brain computer interface for classification of wrist movements in four different directions". In: *2011 28th National Radio Science Conference (NRSC)*. Apr. 2011. DOI: 10.1109/nrsc.2011.5873644. URL: https://doi.org/10.1109/nrsc.2011.5873644.

[73] Wilbert McClay, Nancy Yadav, Yusuf Ozbek, Andy Haas, Hagaii Attias, and Srikantan Nagarajan. "A Real-Time Magnetoencephalography Brain-Computer Interface Using Interactive 3d Visualization and the Hadoop Ecosystem". In: *Brain Sciences* 5.4 (2015), pp. 419–440. DOI: 10.3390/brainsci5040419. URL: https://doi.org/10.3390/brainsci5040419.

[74] National Institute of Biomedical Imaging and Bioengineering. *Magnetic Resonance Imaging (MRI)*. 2020. URL: https://www.nibib.nih.gov/science-education/science-topics/magnetic-resonance-imaging-mri (visited on 07/07/2020).

[75] D.D. Langleben, L. Schroeder, J.A. Maldjian, R.C. Gur, S. McDonald, J.D. Ragland, C.P. O'Brien, and A.R. Childress. "Brain Activity During Simulated Deception: an Event-Related Functional Magnetic Resonance Study". In: *NeuroImage* 15.3 (2002), pp. 727–732. DOI: 10.1006/nimg.2001.1003. URL: https://doi.org/10.1006/nimg.2001.1003.

[76] Nikolaus Weiskopf, Frank Scharnowski, Ralf Veit, Rainer Goebel, Niels Birbaumer, and Klaus Mathiak. "Self-Regulation of Local Brain Activity Using Real-Time Functional Magnetic Resonance Imaging (fMRI)". In: *Journal of Physiology-Paris* 98.4-6 (2004), pp. 357–373. DOI: 10.1016/j.jphysparis.2005.09.019. URL: https://doi.org/10.1016/j.jphysparis.2005.09.019.

[77] R. C. deCharms, F. Maeda, G. H. Glover, D. Ludlow, J. M. Pauly, D. Soneji, J. D. E. Gabrieli, and S. C. Mackey. "Control Over Brain Activation and Pain Learned By Using Real-Time Functional Mri". In: *Proceedings of the National Academy of Sciences* 102.51 (2005), pp. 18626–18631. DOI: 10.1073/pnas.0505210102. URL: https://doi.org/10.1073/pnas.0505210102.

[78] Stephen Johnston, D. E. J. Linden, D. Healy, R. Goebel, I. Habes, and S. G. Boehm. "Upregulation of Emotion Areas Through Neurofeedback With a Focus on Positive Mood". In: *Cognitive, Affective, & Behavioral Neuroscience* 11.1 (2010), pp. 44–51. DOI: 10.3758/s13415-010-0010-1. URL: https://doi.org/10.3758/s13415-010-0010-1.

[79] L. Subramanian, J. V. Hindle, S. Johnston, M. V. Roberts, M. Husain, R. Goebel, and D. Linden. "Real-Time Functional Magnetic Resonance Imaging Neurofeedback for Treatment of Parkinson's Disease". In: *Journal of Neuroscience* 31.45 (2011), pp. 16309–16317. DOI: 10.1523/jneurosci.3498-11.2011. URL: https://doi.org/10.1523/jneurosci.3498-11.2011.

[80] F. Scharnowski, C. Hutton, O. Josephs, N. Weiskopf, and G. Rees. "Improving Visual Perception Through Neurofeedback". In: *Journal of Neuroscience* 32.49 (2012), pp. 17830–17841. DOI: 10.1523/jneurosci.6334-11.2012. URL: https://doi.org/10.1523/jneurosci.6334-11.2012.

[81] James Sulzer, Ranganatha Sitaram, Maria Laura Blefari, Spyros Kollias, Niels Birbaumer, Klaas Enno Stephan, Andreas Luft, and Roger Gassert. "Neurofeedback-Mediated Self-Regulation of the Dopaminergic Midbrain". In: *NeuroImage* 83 (2013), pp. 817–825. DOI: 10.1016/j.neuroimage.2013.05.115. URL: https://doi.org/10.1016/j.neuroimage.2013.05.115.

[82] Seung-Schik Yoo, Ty Fairneny, Nan-Kuei Chen, Seh-Eun Choo, Lawrence P. Panych, HyunWook Park, Soo-Young Lee, and Ferenc A. Jolesz. "Brain-Computer Interface Using Fmri: Spatial Navigation By Thoughts". In: *NeuroReport* 15.10 (2004), pp. 1591–1595. DOI: 10.1097/01.wnr.0000133296.

39160.fe. URL: https://doi.org/10.1097/01.wnr.0000133296.39160.fe.

[83] John-Dylan Haynes and Geraint Rees. "Decoding Mental States From Brain Activity in Humans". In: *Nature Reviews Neuroscience* 7.7 (2006), pp. 523–534. DOI: 10.1038/nrn1931. URL: https://doi.org/10.1038/nrn1931.

[84] Stephen M. LaConte, Scott J. Peltier, and Xiaoping P. Hu. "Real-Time Fmri Using Brain-State Classification". In: *Human Brain Mapping* 28.10 (2007), pp. 1033–1044. DOI: 10.1002/hbm.20326. URL: https://doi.org/10.1002/hbm.20326.

[85] Jong-Hwan Lee, Jeongwon Ryu, Ferenc A. Jolesz, Zang-Hee Cho, and Seung-Schik Yoo. "Brain-Machine Interface Via Real-Time Fmri: Preliminary Study on Thought-Controlled Robotic Arm". In: *Neuroscience Letters* 450.1 (2009), pp. 1–6. DOI: 10.1016/j.neulet.2008.11.024. URL: https://doi.org/10.1016/j.neulet.2008.11.024.

[86] Maurice Hollmann, Jochem W. Rieger, Sebastian Baecke, Ralf Lützkendorf, Charles Müller, Daniela Adolf, and Johannes Bernarding. "Predicting Decisions in Human Social Interactions Using Real-Time Fmri and Pattern Classification". In: *PLoS ONE* 6.10 (2011), e25304. DOI: 10.1371/journal.pone.0025304. URL: https://doi.org/10.1371/journal.pone.0025304.

[87] M. Boly, M.R. Coleman, M.H. Davis, A. Hampshire, D. Bor, G. Moonen, P.A. Maquet, J.D. Pickard, S. Laureys, and A.M. Owen. "When Thoughts Become Action: an Fmri Paradigm To Study Volitional Brain Activity in Non-Communicative Brain Injured Patients". In: *NeuroImage* 36.3 (2007), pp. 979–992. DOI: 10.1016/j.neuroimage.2007.02.047. URL: https://doi.org/10.1016/j.neuroimage.2007.02.047.

[88] Bettina Sorger, Brigitte Dahmen, Joel Reithler, Olivia Gosseries, Audrey Maudoux, Steven Laureys, and Rainer Goebel. "Another kind of 'BOLD Response': answering multiple-choice questions via online decoded single-trial brain signals". In: *Progress in Brain Research*. Progress in Brain Research. Elsevier, 2009, pp. 275–292. DOI: 10.1016/s0079-6123(09)17719-1. URL: https://doi.org/10.1016/s0079-6123(09)17719-1.

[89] Bettina Sorger, Joel Reithler, Brigitte Dahmen, and Rainer Goebel. "A Real-Time Fmri-Based Spelling Device Immediately Enabling Robust Motor-Independent Communication". In: *Current Biology* 22.14 (2012), pp. 1333–1338. DOI: 10.1016/j.cub.2012.05.022. URL: https://doi.org/10.1016/j.cub.2012.05.022.

[90] L. Naci, R. Cusack, V. Z. Jia, and A. M. Owen. "The Brain's Silent Messenger: Using Selective Attention To Decode Human Thought for Brain-Based Communication". In: *Journal of Neuroscience* 33.22 (2013), pp. 9385–9393. DOI: 10.1523/jneurosci.5577-12.2013. URL: https://doi.org/10.1523/jneurosci.5577-12.2013.

[91] Amanda Kaas, Rainer Goebel, Giancarlo Valente, and Bettina Sorger. "Topographic Somatosensory Imagery for Real-Time Fmri Brain-Computer Interfacing". In: *Frontiers in Human Neuroscience* 13 (2019). DOI: 10.3389/fnhum.2019.00427. URL: https://doi.org/10.3389/fnhum.2019.00427.

[92] Keum-Shik Hong and Muhammad Jawad Khan. "Hybrid Brain-Computer Interface Techniques for Improved Classification Accuracy and Increased Number of Commands: a Review". In: *Frontiers in Neurorobotics* 11 (2017). DOI: 10.3389/fnbot.2017.00035. URL: https://doi.org/10.3389/fnbot.2017.00035.

[93] Bojan Kerous and Fotis Liarokapis. "BrainChat - A Collaborative Augmented Reality Brain Interface for Message Communication". In: *Adjunct Proceedings of the 2017 IEEE International Symposium on Mixed and Augmented Reality, ISMAR-Adjunct 2017* (2017), pp. 279–283. DOI: 10.1109/ISMAR-Adjunct.2017.91.

[94] Audrey Girouard, Erin Treacy Solovey, Leanne M. Hirshfield, Krysta Chauncey, Angelo Sassaroli, Sergio Fantini, and Robert J. K. Jacob. "Distinguishing Difficulty Levels with Non-invasive Brain Activity Measurements". In: *Human-Computer Interaction - INTERACT 2009*. Human-Computer Interaction - INTERACT 2009. Springer Berlin Heidelberg, 2009, pp. 440–452. DOI: 10.1007/978-3-642-03655-2_50. URL: https://doi.org/10.1007/978-3-642-03655-2_50.

[95] Adi Stein, Yair Yotam, Rami Puzis, Guy Shani, and Meirav Taieb-Maimon. "EEG-triggered dynamic difficulty adjustment for multiplayer games". In: *Entertainment Computing* 25.December 2017 (2018), pp. 14–25. DOI: 10.1016/j.entcom.2017.11.003. URL: https://doi.org/10.1016/j.entcom.2017.11.003.

[96] Gabriel Alves Mendes Vasiljevic and Leonardo Cunha de Miranda. "Brain-Computer Interface Games Based on Consumer-Grade Eeg Devices: a Systematic Literature Review". In: *International Journal of Human-Computer Interaction* (2019), pp. 1–38. DOI: 10.1080/10447318.2019.1612213. URL: https://doi.org/10.1080/10447318.2019.1612213.

[97] Christopher G. Coogan and Bin He. "Brain-Computer Interface Control in a Virtual Reality Environment and Applications for the Internet of Things". In: *IEEE Access* 6 (2018), pp. 10840–10849. DOI: 10.1109/ACCESS.2018.2809453.

[98] Beste F. Yuksel, Kurt B. Oleson, Lane Harrison, Evan M. Peck, Daniel Afergan, Remco Chang, and Robert JK Jacob. "Learn Piano with BACh". In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. May 2016. DOI: 10.1145/2858036.2858388. URL: https://doi.org/10.1145/2858036.2858388.

[99] Erin Treacy Solovey, Audrey Girouard, Robert J.K. Jacob, Francine Lalooses, Krysta Chauncey, Douglas Weaver, Margarita Parasi, Matthias Scheutz, Angelo Sassaroli, Sergio Fantini, and Paul Schermerhorn. "Sensing cognitive multitasking for a brain-based adaptive user interface". In: *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*. 2011. DOI: 10.1145/1978942.1978997. URL: https://doi.org/10.1145/1978942.1978997.

[100] Erin Solovey, Paul Schermerhorn, Matthias Scheutz, Angelo Sassaroli, Sergio Fantini, and Robert Jacob. "Brainput". In: *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems - CHI '12*. 2012. DOI: 10.1145/2207676.2208372. URL: https://doi.org/10.1145/2207676.2208372.

[101] Cuntai Guan, M. Thulasidas, and Jiankang Wu. "High performance p300 speller for brain-computer interface". In: *IEEE International Workshop on Biomedical Circuits and Systems, 2004*. DOI: 10.1109/biocas.2004.1454155. URL: https://doi.org/10.1109/biocas.2004.1454155.

[102] Friedrich Vogel. "The genetic basis of the normal human electroencephalogram (EEG)". In: *Humangenetik* 10.2 (1970), pp. 91–114. DOI: 10.1007/bf00295509. URL: https://doi.org/10.1007%2Fbf00295509.

[103] M. Poulos, M. Rangoussi, and N. Alexandris. "Neural network based person identification using EEG features". In: *1999 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings. ICASSP99 (Cat. No.99CH36258)*. Vol. 2. 1999, 1117–1120 vol.2.

[104] R.B. Paranjape, J. Mahovsky, L. Benedicenti, and Z. Koles'. "The electroencephalogram as a biometric". In: *Canadian Conference on Electrical and Computer Engineering 2001. Conference Proceedings (Cat. No.01TH8555)*. 2001, pp. 1363–1366. DOI: 10.1109/ccece.2001.933649. URL: https://doi.org/10.1109/ccece.2001.933649.

[105] Kavitha P Thomas and A. P. Vinod. "Eeg-Based Biometric Authentication Using Gamma Band Power During Rest State". In: *Circuits, Systems, and Signal Processing* 37.1 (2017), pp. 277–289. DOI: 10.1007/s00034-017-0551-4. URL: https://doi.org/10.1007/s00034-017-0551-4.

[106] Ga-Young Choi, Soo-In Choi, and Han-Jeong Hwang. "Individual identification based on resting-state EEG". In: *2018 6th International Conference on Brain-Computer Interface (BCI)*. Jan. 2018. DOI: 10.1109/iww-bci.2018.8311515. URL: https://doi.org/10.1109/iww-bci.2018.8311515.

[107] Ga-Young Choi, Soo-In Choi, Rahmawati Rahmawati, Hyung-Tak Lee, Yun-Sung Lee, Seong-Uk Kim, and Han-Jeong Hwang. "Biometrics Based on Single-Trial EEG". In: *2019 7th International Winter Conference on Brain-Computer Interface (BCI)*. Feb. 2019. DOI: 10.1109/iww-bci.2019.8737254. URL: https://doi.org/10.1109/iww-bci.2019.8737254.

[108] Ayman Khalafallah, Aly Ibrahim, Bahieeldeen Shehab, Hisham Raslan, Omar Eltobgy, and Shady Elbaroudy. "A Pragmatic Authentication System Using Electroencephalography Signals". In: Apr. 2018, pp. 901–905. DOI: 10.1109/ICASSP.2018.8461659.

[109] Takashi Nakamura, Valentin Goverdovsky, and Danilo P. Mandic. "In-Ear Eeg Biometrics for Feasible and Readily Collectable Real-World Person Authentication". In: *IEEE Transactions on Information Forensics and Security* 13.3 (2018), pp. 648–661. DOI: 10.1109/tifs.2017.2763124. URL: https://doi.org/10.1109/tifs.2017.2763124.

[110] Sherif Nagib Abbas Seha and Dimitrios Hatzinakos. "A New Approach for EEG-Based Biometric Authentication Using Auditory Stimulation". In: *2019 International Conference on Biometrics (ICB)*. June 2019. DOI: 10.1109/icb45273.2019.8987271. URL: https://doi.org/10.1109/icb45273.2019.8987271.

[111] Chandragupta Borkotoky, Swapil Galgate, and S. B. Nimbekar. "Human computer interaction". In: *Proceedings of the 1st Bangalore annual Compute conference on - Compute '08*. 2008. DOI: 10.1145/1341771.1341797. URL: https://doi.org/10.1145/1341771.1341797.

[112] Seul-Ki Yeom, Heung-Il Suk, and Seong-Whan Lee. "Person Authentication From Neural Activity of Face-Specific Visual Self-Representation". In: *Pattern Recognition* 46.4 (2013), pp. 1159–1169. DOI: 10.1016/j.patcog.2012.10.023. URL: https://doi.org/10.1016/j.patcog.2012.10.023.

[113] Moonwon Yu, Netiwit Kaongoen, and Sungho Jo. "P300-BCI-based authentication system". In: *2016 4th International Winter Conference on Brain-Computer Interface (BCI)*. Feb. 2016. DOI: 10.1109/iww-bci.2016.7457443. URL: https://doi.org/10.1109/iww-bci.2016.7457443.

[114] Min Wang, Hussein A. Abbass, and Jiankun Hu. "Continuous authentication using EEG and face images for trusted autonomous systems". In: *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. Dec. 2016. DOI: 10.1109/pst.2016.7906958. URL: https://doi.org/10.1109/pst.2016.7906958.

[115] Ericsen, Kavitha P. Thomas, and A. P. Vinod. "Eeg-based biometrie authentication using self-referential visual stimuli". In: *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. Oct. 2017. DOI: 10.1109/smc.2017.8123093. URL: https://doi.org/10.1109/smc.2017.8123093.

[116] Violeta Tulceanu. "Brainwave Authentication Using Emotional Patterns". In: *International Journal of Advanced Intelligence Paradigms* 9.1 (2017), p. 1. DOI: 10.1504/ijaip.2017.10002023. URL: https://doi.org/10.1504/ijaip.2017.10002023.

[117] Denise Kerbaj, Walid Hassan, and Amine Nait-Ali. "Verifying a personas identity using brain responses to visual stimuli". In: *2017 2nd International Conference on Bio-engineering for Smart Technologies (BioSMART)*. Aug. 2017. DOI: 10.1109/biosmart.2017.8095344. URL: https://doi.org/10.1109/biosmart.2017.8095344.

[118] Feng Lin, Kun Woo Cho, Chen Song, Wenyao Xu, and Zhanpeng Jin. "Brain Password: a Secure and Truly Cancelable Brain Biometrics for Smart Headwear". In: *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services - MobiSys '18* (2018), pp. 296–309. DOI: 10/gf6jdm. URL: https://doi.org/10/gf6jdm.

[119] Nick Merrill, Max T. Curran, and John Chuang. "Is the Future of Authenticity All in Our Heads?" In: *Proceedings of the 2017 New Security Paradigms Workshop on ZZZ - NSPW 2017* (2017), pp. 70–79. DOI: 10/gf6jgd. URL: https://doi.org/10/gf6jgd.

[120] Ramaswamy Palaniappan. "Two-Stage Biometric Authentication Method Using Thought Activity Brain Waves". In: *International journal of neural systems* 18 1 (2008), pp. 59–66.

[121] Ramaswamy Palaniappan. "Multiple Mental Thought Parametric Classification: A New Approach for Individual Identification". In: *World Academy of Science, Engineering and Technology, International Journal of Medical, Health, Biomedical, Bioengineering and Pharmaceutical Engineering* 2 (2008), pp. 303–306.

[122] A Riera, A Soria-Frisch, M Caparrini, C Grau, and G Ruffini. "Multiple Mental Thought Parametric Classification: A New Approach for Individual Identification". In: *EURASIP Journal on Advances in Signal Processing volume* 143728 (2008).

[123] Shiliang Sun. "Multitask learning for EEG-based biometrics". In: *2008 19th International Conference on Pattern Recognition*. 2008, pp. 1–4.

[124] I. Nakanishi, S. Baba, and C. Miyamoto. "EEG based biometric authentication using new spectral features". In: *2009 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*. 2009, pp. 651–654.

[125] Corey Ashby, Amit Bhatia, Francesco Tenore, and Jacob Vogelstein. "Low-cost electroencephalogram (EEG) based authentication". In: *2011 5th International IEEE/EMBS Conference on Neural Engineering*. Apr. 2011. DOI: 10.1109/ner.2011.5910581. URL: https://doi.org/10.1109/ner.2011.5910581.

[126] Qiong Gui, Zhanpeng Jin, and Wenyao Xu. "Exploring EEG-based biometrics for user identification and authentication". In: *2014 IEEE Signal Processing in Medicine and Biology Symposium (SPMB)*. Dec. 2014. DOI: 10.1109/spmb.2014.7002950. URL: https://doi.org/10.1109/spmb.2014.7002950.

[127] Tien Pham, Wanli Ma, Dat Tran, Phuoc Nguyen, and Dinh Phung. "Multi-factor EEG-based user authentication". In: *2014 International Joint Conference on Neural Networks (IJCNN)*. July 2014. DOI: 10.1109/ijcnn.2014.6889569. URL: https://doi.org/10.1109/ijcnn.2014.6889569.

[128] Tien Pham, Wanli Ma, Dat Tran, Duc Su Tran, and Dinh Phung. "A study on the stability of EEG signals for user authentication". In: *2015 7th International IEEE/EMBS Conference on Neural Engineering (NER)*. Apr. 2015. DOI: 10.1109/ner.2015.7146575. URL: https://doi.org/10.1109/ner.2015.7146575.

[129] Montri Phothisonothai. "An investigation of using SSVEP for EEG-based user authentication system". In: *2015 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*. Dec. 2015. DOI: 10.1109/apsipa.2015.7415406. URL: https://doi.org/10.1109/apsipa.2015.7415406.

[130] Alireza Jolfaei, Xin-Wen Wu, and Vallipuram Muthukkumarasamy. "On the Feasibility and Performance of Pass-Thought Authentication Systems". In: *2013 Fourth International Conference on Emerging Security Technologies*. Sept. 2013. DOI: 10.1109/est.2013.12. URL: https://doi.org/10.1109/est.2013.12.

[131] Abdul Serwadda, Vir V. Phoha, Sujit Poudel, Leanne M. Hirshfield, Danushka Bandara, Sarah E. Bratt, and Mark R. Costa. "fNIRS: A new modality for brain activity-based biometric authentication". In: *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. Sept. 2015. DOI: 10.1109/btas.2015.7358763. URL: https://doi.org/10.1109/btas.2015.7358763.

[132] Yashraj S. Soni, S. B. Somani, and V. V. Shete. "Biometric user authentication using brain waves". In: *2016 International Conference on Inventive Computation Technologies (ICICT)*. Aug. 2016. DOI: 10.1109/inventive.2016.7824888. URL: https://doi.org/10.1109/inventive.2016.7824888.

[133] Maria V. Ruiz-Blondet, Zhanpeng Jin, and Sarah Laszlo. "Cerebre: a Novel Method for Very High Accuracy Event-Related Potential Biometric Identification". In: *IEEE Transactions on Information Forensics and Security* 11.7 (2016), pp. 1618–1629. DOI: 10.1109/tifs.2016.2543524. URL: https://doi.org/10.1109/tifs.2016.2543524.

[134] Yiyu Chen, Ayalneh Dessalegn Atnafu, Isabella Schlattner, Wendimagegn Tariku Weldtsadik, Myung-Cheol Roh, Hyoung Joong Kim, Seong-Whan Lee, Benjamin Blankertz, and Siamac Fazli. "A High-Security Eeg-Based Login System With Rsvp Stimuli and Dry Electrodes". In: *IEEE Transactions on Information Forensics and Security* 11.12 (2016), pp. 2635–2647. DOI: 10.1109/tifs.2016.2577551. URL: https://doi.org/10.1109/tifs.2016.2577551.

[135] Qiong Gui, Maria V. Ruiz-Blondet, Sarah Laszlo, and Zhanpeng Jin. "A Survey on Brain Biometrics". In: *ACM Computing Surveys* 51.6 (2019), pp. 1–38. DOI: 10.1145/3230632. URL: https://doi.org/10.1145/3230632.

[136] I. Jayarathne, M. Cohen, and S. Amarakeerthi. "Survey of EEG-based biometric authentication". In: *2017 IEEE 8th International Conference on Awareness Science and Technology (iCAST)*. 2017, pp. 324–329.

[137] Blair C. Armstrong, Maria V. Ruiz-Blondet, Negin Khalifian, Kenneth J. Kurtz, Zhanpeng Jin, and Sarah Laszlo. "Brainprint: Assessing the Uniqueness, Collectability, and Permanence of a Novel Method for Erp Biometrics". In: *Neurocomputing* 166 (2015), pp. 59–67. DOI: 10.1016/j.neucom.2015.04.025. URL: https://doi.org/10.1016/j.neucom.2015.04.025.

[138] Maria V. Ruiz Blondet, Sarah Laszlo, and Zhanpeng Jin. "Assessment of permanence of non-volitional EEG brainwaves as a biometric". In: *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015)*. Mar. 2015. DOI: 10.1109/isba.2015.7126359. URL: https://doi.org/10.1109/isba.2015.7126359.

[139] Koosha Sadeghi, Junghyo Lee, Ayan Banerjee, Javad Sohankar, and Sandeep K. S. Gupta. "Permanency analysis on human electroencephalogram signals for pervasive Brain-Computer Interface systems". In: *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. July 2017. DOI: 10.1109/embc.2017.8036937. URL: https://doi.org/10.1109/embc.2017.8036937.

[140] Emanuele Maiorana, Daria La Rocca, and Patrizio Campisi. "On the Permanence of Eeg Signals for Biometric Recognition". In: *IEEE Transactions on Information Forensics and Security* 11.1 (2016), pp. 163–175. DOI: 10.1109/tifs.2015.2481870. URL: https://doi.org/10.1109/tifs.2015.2481870.

[141] Jane E. Huggins, Patricia A. Wren, and Kirsten L. Gruis. "What Would Brain-Computer Interface Users Want? Opinions and Priorities of Potential Users With Amyotrophic Lateral Sclerosis". In: *Amyotrophic Lateral Sclerosis* 12.5 (2011), pp. 318–324. DOI: 10.3109/17482968.2011.572978. URL: https://doi.org/10.3109/17482968.2011.572978.

[142] Jane E. Huggins, Aisha A. Moinuddin, Anthony E. Chiodo, and Patricia A. Wren. "What Would Brain-Computer Interface Users Want: Opinions and Priorities of Potential Users With Spinal Cord Injury". In: *Archives of Physical Medicine and Rehabilitation* 96.3 (2015), S38–S45.e5. DOI: 10.1016/j.apmr.2014.05.028. URL: https://doi.org/10.1016/j.apmr.2014.05.028.

[143] Stefanie Blain-Moraes, Riley Schaff, Kirsten L. Gruis, Jane E. Huggins, and Patricia A. Wren. "Barriers to and mediators of brain–computer interface user acceptance: focus group findings". In: *Ergonomics* 55.5 (2012). PMID: 22455595, pp. 516–525. DOI: 10.1080/00140139.2012.661082. eprint: https://doi.org/10.1080/00140139.2012.661082. URL: https://doi.org/10.1080/00140139.2012.661082.

[144] Andrew Geronimo, Helen E. Stephens, Steven J. Schiff, and Zachary Simmons. "Acceptance of Brain-Computer Interfaces in Amyotrophic Lateral Sclerosis". In: *Amyotrophic Lateral Sclerosis and Frontotemporal Degeneration* 16.3-4 (2014), pp. 258–264. DOI: 10.3109/21678421.2014.969275. URL: https://doi.org/10.3109/21678421.2014.969275.

[145] Lucy Diep and Gregor Wolbring. "Perceptions of Brain-Machine Interface Technology Among Mothers of Disabled Children". In: *Disability Studies Quarterly* 35.4 (2015). DOI: 10.18061/.v35i4.3856. URL: https://doi.org/10.18061/.v35i4.3856.

[146] G. Lightbody, L. Galway, and P. McCullagh. "The Brain Computer Interface: Barriers to Becoming Pervasive". In: *Pervasive Health*. Pervasive Health. Springer London, 2014, pp. 101–129. DOI: 10.1007/978-1-4471-6413-5_5. URL: https://doi.org/10.1007/978-1-4471-6413-5_5.

[147] Tamara Denning, Yoky Matsuoka, and Tadayoshi Kohno. "Neurosecurity: Security and Privacy for Neural Devices". In: *Neurosurgical Focus* 27.1 (2009), E7. DOI: 10.3171/2009.4.focus0985. URL: https://doi.org/10.3171/2009.4.focus0985.

[148] Carmen Camara, Pedro Peris-Lopez, and Juan E. Tapiador. "Security and Privacy Issues in Implantable Medical Devices: a Comprehensive Survey". In: *Journal of Biomedical Informatics* 55 (2015), pp. 272–289. DOI: 10.1016/j.jbi.2015.04.007. URL: https://doi.org/10.1016/j.jbi.2015.04.007.

[149] Marcello Ienca and Pim Haselager. "Hacking the Brain: Brain-Computer Interfacing Technology and the Ethics of Neurosecurity". In: *Ethics and Information Technology* 18.2 (2016), pp. 117–129. DOI: 10.1007/s10676-016-9398-9. URL: https://doi.org/10.1007/s10676-016-9398-9.

[150] Marcello Ienca and Roberto Andorno. "Towards New Human Rights in the Age of Neuroscience and Neurotechnology". In: *Life Sciences, Society and Policy* 13.1 (2017), p. 5. DOI: 10.1186/s40504-017-0050-1. URL: https://doi.org/10.1186/s40504-017-0050-1.

[151] Marcello Ienca, Pim Haselager, and Ezekiel J Emanuel. "Brain Leaks and Consumer Neurotechnology". In: *Nature Biotechnology* 36.9 (2018), pp. 805–810. DOI: 10.1038/nbt.4240. URL: https://doi.org/10.1038/nbt.4240.

[152] Tamara Bonaci and Howard Chizeck. "Privacy by Design in Brain-Computer Interfaces". In: Jan. 2013.

[153] Tamara Bonaci, Ryan Calo, and Howard Jay Chizeck. "App Stores for the Brain : Privacy and Security in Brain-Computer Interfaces". In: *IEEE Technology and Society Magazine* 34.2 (2015), pp. 32–39. DOI: 10.1109/mts.2015.2425551. URL: https://doi.org/10.1109/mts.2015.2425551.

[154] Laurie Pycroft and Tipu Z. Aziz. "Security of Implantable Medical Devices With Wireless Connections: the Dangers of Cyber-Attacks". In: *Expert Review of Medical Devices* 15.6 (2018), pp. 403–406. DOI: 10.1080/17434440.2018.1483235. URL: https://doi.org/10.1080/17434440.2018.1483235.

[155] Jonathan Pugh, Laurie Pycroft, Anders Sandberg, Tipu Aziz, and Julian Savulescu. "Brainjacking in Deep Brain Stimulation and Autonomy". In: *Ethics and Information Technology* 20.3 (2018), pp. 219–232. ISSN: 15728439. DOI: 10/gf6jdc. URL: https://doi.org/10/gf6jdc.

[156] Laurie Pycroft, Sandra G. Boccard, Sarah L.F. Owen, John F. Stein, James J. Fitzgerald, Alexander L. Green, and Tipu Z. Aziz. "Brainjacking: Implant Security Issues in Invasive Neuromodulation". In: *World Neurosurgery* 92 (2016), pp. 454–462. DOI: 10.1016/j.wneu.2016.05.010. URL: https://doi.org/10.1016/j.wneu.2016.05.010.

[157] Nick Merrill, John Chuang, and Coye Cheshire. "Sensing is Believing". In: *Proceedings of the 2019 on Designing Interactive Systems Conference - DIS '19*. 2019. DOI: 10.1145/3322276.3322286. URL: https://doi.org/10.1145/3322276.3322286.

[158] Ivan Martinovic, Doug Davies, Mario Frank, Daniele Perito, Tomas Ros, and Dawn Song. "On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces". In: *USENIX Security Symposium*. Bellevue, WA, 2012.

[159] Mario Frank, Tiffany Hwu, Sakshi Jain, Robert T. Knight, Ivan Martinovic, Prateek Mittal, Daniele Perito, Ivo Sluganovic, and Dawn Song. "Using EEG-Based BCI Devices to Subliminally Probe for Private Information". In: *Proceedings of the 2017 on Workshop on Privacy in the Electronic Society - WPES '17*. 2017. DOI: 10.1145/3139550.3139559. URL: https://doi.org/10.1145/3139550.3139559.

[160] Richard Matovu and Abdul Serwadda. "Your substance abuse disorder is an open secret! Gleaning sensitive personal information from templates in an EEG-based authentication system". In: *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. Sept. 2016. DOI: 10.1109/btas.2016.7791210. URL: https://doi.org/10.1109/btas.2016.7791210.

[161] Ofir Landau, Aviad Cohen, Shirley Gordon, and Nir Nissim. "Mind Your Privacy: Privacy Leakage Through Bci Applications Using Machine Learning Methods". In: *Knowledge-Based Systems* 198 (2020), p. 105932. DOI: 10.1016/j.knosys.2020.105932. URL: https://doi.org/10.1016/j.knosys.2020.105932.

[162] Guohua Shen, Kshitij Dwivedi, Kei Majima, Tomoyasu Horikawa, and Yukiyasu Kamitani. "End-To-End Deep Image Reconstruction From Human Brain Activity". In: *Frontiers in Computational Neuroscience* 13 (2019). DOI: 10.3389/fncom.2019.00021. URL: https://doi.org/10.3389/fncom.2019.00021.

[163] Thomas Naselaris, Ryan J. Prenger, Kendrick N. Kay, Michael Oliver, and Jack L. Gallant. "Bayesian Reconstruction of Natural Images From Human Brain Activity". In: *Neuron* 63.6 (2009), pp. 902–915. DOI: 10.1016/j.neuron.2009.09.006. URL: https://doi.org/10.1016/j.neuron.2009.09.006.

[164] Shinji Nishimoto, An T. Vu, Thomas Naselaris, Yuval Benjamini, Bin Yu, and Jack L. Gallant. "Reconstructing Visual Experiences From Brain Activity Evoked By Natural Movies". In: *Current Biology* 21.19 (2011), pp. 1641–1646. DOI: 10.1016/j.cub.2011.08.031. URL: https://doi.org/10.1016/j.cub.2011.08.031.

[165] Changde Du, Changying Du, and Huiguang He. "Sharing deep generative representation for perceived image reconstruction from human brain activity". In: *2017 International Joint Conference on Neural Networks (IJCNN)*. May 2017. DOI: 10.1109/ijcnn.2017.7965968. URL: https://doi.org/10.1109/ijcnn.2017.7965968.

[166] Guohua Shen, Tomoyasu Horikawa, Kei Majima, and Yukiyasu Kamitani. *Deep image reconstruction from human brain activity*. 2017. DOI: 10.1101/240317. URL: https://doi.org/10.1101/240317.

[167] K. Seeliger, U. Güçlü, L. Ambrogioni, Y. Güçlütürk, and M.A.J. van Gerven. "Generative Adversarial Networks for Reconstructing Natural Images From Brain Activity". In: *NeuroImage* 181 (2018), pp. 775–785. DOI: 10.1016/j.neuroimage.2018.07.043. URL: https://doi.org/10.1016/j.neuroimage.2018.07.043.

[168] Christina Braz and Jean-Marc Robert. "Security and usability". In: *Proceedings of the 18th international conference on Association Francophone d'Interaction Homme-Machine - IHM '06*. 2006. DOI: 10.1145/1132736.1132768. URL: https://doi.org/10.1145/1132736.1132768.

[169] Ashley Colley, Tobias Seitz, Tuomas Lappalainen, Matthias Kranz, and Jonna Häkkilä. "Extending the Touchscreen Pattern Lock Mechanism With Duplicated and Temporal Codes". In: *Advances in Human-Computer Interaction* 2016 (2016), pp. 1–11. DOI: 10.1155/2016/8762892. URL: https://doi.org/10.1155/2016/8762892.

[170] Grant S. Taylor and Christina Schmidt. "Empirical Evaluation of the Emotiv Epoc Bci Headset for the Detection of Mental Actions". In: *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 56.1 (2012), pp. 193–197. DOI: 10.1177/1071181312561017. URL: https://doi.org/10.1177/1071181312561017.

[171] Emotiv Inc. *Cortex V2 Documentation*. 2020. URL: https://emotiv.gitbook.io/cortex-api/.

[172] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. "A Comparative Usability Study of Two-Factor Authentication". In: *Proceedings 2014 Workshop on Usable Security*. 2014. DOI: 10.14722/usec.2014.23025. URL: https://doi.org/10.14722/usec.2014.23025.

[173] Anders Bruun, Kenneth Jensen, and Dianna Kristensen. "Usability of Single- and Multi-factor Authentication Methods on Tabletops: A Comparative Study". In: *Human-Centered Software Engineering*. Human-Centered Software Engineering. Springer Berlin Heidelberg, 2014, pp. 299–306. DOI: 10.1007/978-3-662-44811-3_22. URL: https://doi.org/10.1007/978-3-662-44811-3_22.

[174] B.S. Archana, Ashika Chandrashekar, Anusha Govind Bangi, B.M. Sanjana, and Syed Akram. "Survey on usable and secure two-factor authentication". In: *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. May 2017. DOI: 10.1109/rteict.2017.8256716. URL: https://doi.org/10.1109/rteict.2017.8256716.

[175] Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. "Multi-Factor Authentication: a Survey". In: *Cryptography* 2.1 (2018), p. 1. DOI: 10.3390/cryptography2010001. URL: https://doi.org/10.3390/cryptography2010001.

[176] expressjs. *express: Fast, unopinionated, minimalist web framework for node.* 2020. URL: https://github.com/expressjs/express.

[177] MongoDB Inc. *MongoDB: The most popular database for modern apps.* 2020. URL: https://mongodb.com5.

[178] Mozilla Development Network. *Promise*. 2020. URL: https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/Promise.

[179] Snap.svg. *Snap.svg: The JavaScript SVG library for the modern web*. 2020. URL: http://snapsvg.io/.

[180] R. N. Shepard and J. Metzler. "Mental Rotation of Three-Dimensional Objects". In: *Science* 171.3972 (1971), pp. 701–703. DOI: 10.1126/science.171.3972.701. URL: https://doi.org/10.1126/science.171.3972.701.

[181] Gijsbert Stoet. *PsyToolkit: Mental Rotation Task*. URL: https://www.psytoolkit.org/experiment-library/mentalrotation.html.

[182] Takayuki Nakachi, Hiroyuki Ishihara, and Hitoshi Kiya. "Privacy-Preserving Network BMI Decoding of Covert Spatial Attention". In: *2018 12th International Conference on Signal Processing and Communication Systems (ICSPCS)*. Dec. 2018. DOI: 10.1109/icspcs.2018.8631768. URL: https://doi.org/10.1109/icspcs.2018.8631768.

[183] Dennis Frank, Jasmine Mabrey, and Kenji Yoshigoe. "Personalizable neurological user authentication framework". In: *2017 International Conference on Computing, Networking and Communications (ICNC)*. Jan. 2017. DOI: 10.1109/iccnc.2017.7876258. URL: https://doi.org/10.1109/iccnc.2017.7876258.

[184] Virginia Braun and Victoria Clarke. "Using Thematic Analysis in Psychology". In: *Qualitative Research in Psychology* 3.2 (2006), pp. 77–101. DOI: 10.1191/1478088706qp063oa. URL: https://doi.org/10.1191/1478088706qp063oa.

[185] Virginia Braun, Victoria Clarke, Nikki Hayfield, and Gareth Terry. "Thematic Analysis". In: *Handbook of Research Methods in Health Social Sciences*. Handbook of Research Methods in Health Social Sciences. Springer Singapore, 2019, pp. 843–860. DOI: 10.1007/978-981-10-5251-4_103. URL: https://doi.org/10.1007/978-981-10-5251-4_103.

[186] Su Yang and Farzin Deravi. "On the Usability of Electroencephalographic Signals for Biometric Recognition: a Survey". In: *IEEE Transactions on Human-Machine Systems* 47.6 (2017), pp. 958–969. DOI: 10.1109/thms.2017.2682115. URL: https://doi.org/10.1109/thms.2017.2682115.

[187] The Autodidacts. *NeuroBB: The EEG, BCI, and neurofeedback discussion forum*. 2020. URL: https://neurobb.com/.

[188] Inc. Reddit. *Brain-Computer Interfaces, Thought-controlled computing*. 2020. URL: https://www.reddit.com/r/BCI/.

[189] Johannes Kögel, Jennifer R. Schmid, Ralf J. Jox, and Orsolya Friedrich. "Using Brain-Computer Interfaces: a Scoping Review of Studies Employing Social Research Methods". In: *BMC Medical Ethics* 20.1 (2019), p. 18. DOI: 10.1186/s12910-019-0354-1. URL: https://doi.org/10.1186/s12910-019-0354-1.

[190] Joshua I. Ekandem, Timothy A. Davis, Ignacio Alvarez, Melva T. James, and Juan E. Gilbert. "Evaluating the Ergonomics of Bci Devices for Research and Experimentation". In: *Ergonomics* 55.5 (2012), pp. 592–598. DOI: 10.1080/00140139.2012.662527. URL: https://doi.org/10.1080/00140139.2012.662527.

[191] W David Hairston, Keith W Whitaker, Anthony J Ries, Jean M Vettel, J Cortney Bradford, Scott E Kerick, and Kaleb McDowell. "Usability of Four Commercially-Oriented EEG Systems". In: *Journal of Neural Engineering* 11.4 (July 2014), p. 046018. DOI: 10.1088/1741-2560/11/4/046018. URL: https://doi.org/10.1088/1741-2560/11/4/046018.

[192] I. Mustafa, H. Farooq, and T.K. Khatri. "EEG based user authentication using visual stimuli of geometric shapes". In: cited By 0. 2019, pp. 247–251. DOI: 10.1109/C-CODE.2019.8680987. URL: https://doi.org/10.1109/C-CODE.2019.8680987.

[193] Serge Egelman and Eyal Peer. "Scaling the Security Wall". In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*. ACM Press, 2015. DOI: 10.1145/2702123.2702249. URL: https://doi.org/10.1145%2F2702123.2702249.

[194] Marc Anderson. "Big Five Personality Dimensions". In: *Encyclopedia of Management Theory*. Encyclopedia of Management Theory. SAGE Publications, Inc., 2013. DOI: 10.4135/9781452276090.n24. URL: https://doi.org/10.4135/9781452276090.n24.

[195] Samuel D Gosling, Peter J Rentfrow, and William B Swann. "A very brief measure of the Big-Five personality domains". In: *Journal of Research in Personality* 37.6 (Dec. 2003), pp. 504–528. DOI: 10.1016/s0092-6566(03)00046-1. URL: https://doi.org/10.1016%2Fs0092-6566%2803%2900046-1.

[196] Arun Vishwanath. "Impact of personality on technology adoption: An empirical model". In: *Journal of the American Society for Information Science and Technology* 56.8 (2005), pp. 803–811. DOI: 10.1002/asi.20169. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/asi.20169. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/asi.20169.

[197] Gunnvald B. Svendsen, Jan-Are K. Johnsen, Live Almås-Sørensen, and Joar Vittersø. "Personality and technology acceptance: the influence of personality factors on the core constructs of the Technology Acceptance Model". In: *Behaviour & Information Technology* 32.4 (2013), pp. 323–334. DOI: 10.1080/0144929X.2011.553740. eprint: https://doi.org/10.1080/0144929X.2011.553740. URL: https://doi.org/10.1080/0144929X.2011.553740.

[198] Philipp Rauschnabel, Alexander Brem, and Bjørn S. Ivens. "Who will buy smart glasses?: Empirical results of two pre-market-entry studies on the role of personality in individual awareness and intended adaption of Google Glass Wearables". English. In: *Computers in Human Behavior* 49 (2015), pp. 635–647. ISSN: 0747-5632. DOI: 10.1016/j.chb.2015.03.003.

[199] Philipp A. Rauschnabel and Young K. Ro. "Augmented reality smart glasses: an investigation of technology acceptance drivers". In: *International Journal of Technology Marketing* 11.2 (2016), pp. 123–148. DOI: 10.1504/IJTMKT.2016.075690. eprint: https://www.inderscienceonline.com/doi/pdf/10.1504/IJTMKT.2016.075690. URL: https://www.inderscienceonline.com/doi/abs/10.1504/IJTMKT.2016.075690.

[200] Michael A. Rupp, Jessica R. Michaelis, Daniel S. McConnell, and Janan A. Smither. "The role of individual differences on perceptions of wearable fitness device trust, usability, and motivational impact". In: *Applied Ergonomics* 70 (2018), pp. 77–87. ISSN: 0003-6870. DOI: https://doi.org/10.1016/j.apergo.2018.02.005. URL: http://www.sciencedirect.com/science/article/pii/S0003687018300292.

[201] Yang Lu, Savvas Papagiannidis, and Eleftherios Alamanos. "Exploring the emotional antecedents and outcomes of technology acceptance". In: *Computers in Human Behavior* 90 (2019), pp. 153–169. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2018.08.056. URL: http://www.sciencedirect.com/science/article/pii/S074756321830431X.

[202] James F. Knight and Chris Baber. "A Tool To Assess the Comfort of Wearable Computers". In: *Human Factors: The Journal of the Human Factors and Ergonomics Society* 47.1 (2005), pp. 77–91. DOI: 10.1518/0018720053653875. URL: https://doi.org/10.1518/0018720053653875.

[203] LimeSurvey Project Team / Carsten Schmitz. *LimeSurvey: An Open Source survey tool*. LimeSurvey Project. Hamburg, Germany, 2012. URL: http://www.limesurvey.org.

[204] Leib Litman, Jonathan Robinson, and Tzvi Abberbock. "Turkprime.com: a Versatile Crowdsourcing Data Acquisition Platform for the Behavioral Sciences". In: *Behavior Research Methods* 49.2 (2016), pp. 433–442. DOI: 10.3758/s13428-016-0727-z. URL: https://doi.org/10.3758/s13428-016-0727-z.

[205] R Core Team. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing. Vienna, Austria, 2020. URL: https://www.R-project.org/.

[206] Djellel Difallah, Elena Filatova, and Panos Ipeirotis. "Demographics and Dynamics of Mechanical Turk Workers". In: *Proceedings of the Eleventh ACM International Conference on Web Search and Data Mining - WSDM '18*. 2018. DOI: 10.1145/3159652.3159661. URL: https://doi.org/10.1145/3159652.3159661.

[207] Joel Ross, Lilly Irani, M. Six Silberman, Andrew Zaldivar, and Bill Tomlinson. "Who are the crowdworkers?" In: *Proceedings of the 28th of the international conference extended abstracts on Human factors in computing systems - CHI EA '10*. 2010. DOI: 10.1145/1753846.1753873. URL: https://doi.org/10.1145/1753846.1753873.

[208] S.D. Gosling, P.J. Rentfrow, and J. Potter. "Norms for the Ten Item Personality Test". 2014. URL: https://gosling.psy.utexas.edu/scales-weve-developed/ten-item-personality-measure-tipi/.

Appendices

Appendix A

Research Ethics Approval

The studies described in this thesis were reviewed and approved by the Carleton University Research Ethics Board (CUREB) prior to any participant interaction (CUREB File No. **111922**). The following pages contain the materials that were submitted to CUREB including consent forms, recruitment posts/posters, and study instruments for the three studies.

A.1 Authentication System Usability Study

Carleton UNIVERSITY
Canada's Capital University

Consent Form

Title of research project: Exploring Thought-Based Passwords
Funding Source: NSERC
Date of ethics clearance: To be determined by CUREB (on clearance form)
Ethics Clearance for the Collection of Data Expires: To be determined by CUREB
CUREB-B Clearance # 111922

I, _____, volunteer to participate in a study on thought-based passwords. This study aims to develop a usable password system using thought-based interaction. **The researchers for this study are Prof. Robert Biddle and Josh Carr.**

The present study is meant to test the usability and feasibility of a thought-based password system using a commercial device that measures mental states called the Emotiv Insight. This device allows you to give directional commands (such as 'up', 'down', 'left', 'right') by engaging in a specific mental activity that you have associated with that command. The Insight device uses small sensors that sit on the surface of your scalp and measure your mental activity. The technology behind the Insight has been around for nearly 100 years and has not been associated with any negative side-effects. The Insight is only capable of reading mental activity; it cannot affect your brain in any way.

To participate in this study, you must meet the be at least 18 years old, comfortable communicating in English, and have normal or corrected-to-normal vision (glasses or contacts are okay). You also must not suffer from any major neurological conditions such as epilepsy or traumatic brain injury, and be comfortable wearing a 1.2kg headband for approximately 1 hour (with breaks).

During the study, you will be asked to wear a light headband-like device around your head while sitting at a computer, and to use the device to draw a pattern on a screen by engaging in specific mental tasks. The study will last approximately 1 hour.

For our study, we will not record or keep any of the sensor data. The Insight uses its measurements to generate output commands and then the data is discarded automatically and immediately. All data that we do collect from the study will be stored on a secure server and will not be associated with your name or any identifying information. We will keep your anonymized data and potentially conduct additional analysis at a later time.

Our study is related to passwords, but you will not be asked anything about the real passwords that you use in everyday life. The passwords for our study will be generated by the

authentication application. Your participation in this study is completely voluntary and you may withdraw at any point without consequence. If at any point you do not wish to continue, simply tell the researcher and they will end the study. If you withdraw before the end of the study, all information you have provided will be immediately destroyed. After the study is completed, you will not be able to withdraw your data because it will be anonymized and we will have no way of linking it back to you.

Researcher contact information:
Josh Carr
Computer Science/ Cognitive Science
josh.carr@carleton.ca

Supervisor contact
Robert Biddle
Computer Science/ Cognitive Science
robert.biddle@carleton.ca

By signing below, you agree to participate in the study as described above

_____	_____
Signature of participant	Date
_____	_____
Signature of researcher	Date

Should you have any ethical concerns with the study, please contact the REB Chair, Carleton University Research Ethics Board-B (by phone: 613-520-2600 ext. 4085 or by email: ethics@carleton.ca). For all other questions about the study, please contact the researcher.

_____

Carleton UNIVERSITY

Participate in a study on thought-based passwords!

To participate in this study, you must be:

✓ At least 18 years old
✓ Comfortable in the English language
✓ Have 20/20 or corrected to 20/20 vision
✓ Without any major neurological conditions
✓ Comfortable wearing a 1.2kg (2.5lb) headband for approximately 1 hour (with breaks)

My name is Josh Carr and I am a Master's student in the Human-Computer Interaction program. I am working with Professor Biddle on a project called "Exploring Thought-Based Passwords",about a password system that uses mental commands as input.

This is a 60-minute study. You will be asked to wear a lightweight (1.2kg) headband-like device that measures mental activity and to use the device to enter a password by drawing a pattern on the screen. As a token of our appreciation for your time, you will receive compensation of $15.

The ethics protocol for this project has been reviewed and cleared by the Carleton University Research Ethics. [CUREB-B Clearance # 111922]

Demographics Questionnaire

Thank you for volunteering for this study! The purpose of this short questionnaire is to acquire some general background information about you that will help in interpreting the results. The answers to these questions are strictly confidential. You can skip any question that you do not want to answer. *Please circle the answer(s) that best applies to you.*

1) Age:

18-19 20-29
30-39 40-49
50-60 >60

2) What is your highest/current academic level?

Trade school
Diploma
Professional School (Medical, Dental, Legal, etc.)
Undergraduate
Master's
PhD
Other:_____

3) What is your field of study/work? If more than one, please state them all.

_____

4) How often do you use a laptop/desktop computer?

everyday once a week once a month once a year never

5) Have you ever used a brain-sensing device to control a computer?

Yes No

6) Have you ever been advised of any unusual or significant neurological conditions?

Yes No

DEBRIEFING

TITLE: USABILITY STUDY ON BROWSER SECURITY CERTIFICATES

What are we trying to learn in this research?

This research is aimed at testing the usability and practical feasibility of an alternative password system. Our overall goal is to overcome the security and usability problems that are inherent in text-based passwords. We are interested in assessing whether our system is easy to use, the amount of time that it takes, and whether it is prone to errors.

Why is this important to scientists or the general public?

Text-based passwords are the primary method of digital authentication used around the world. However, the security of passwords is reduced because of their poor usability. Remembering a unique password for every online account is very difficult, so most people resort to reusing their passwords or writing them down. Both of these strategies present significant security problems. A great deal of work has been done in designing and testing various alternative password systems, but so far none have emerged as a clear candidate to replace text-passwords in everyday use. Thought-based passwords are interesting to study because the uniqueness of how each individual person's brain expresses thoughts provides a biometric authentication factor (like a fingerprint or your voice). Authentication systems, however, are only as secure as they are usable, so the results of this study will indicate whether or not thought-based passwords could be pursued as a viable alternative to text-based ones.

Where can I learn more?

To learn more about the Emotiv Insight device, check out their website: Emotiv.com

Below are a few published papers on password security, brain-computer interfaces, and thought-based passwords that inspired this project:

What if I have questions later?

You are welcome to email the researcher at any time if you have any questions, concerns, or comments about the experiment. Josh (Lead Researcher) can be reached at josh.carr@carleton.ca, and Professor Biddle at robert.biddle@carleton.ca.

Thank you! Your time is valuable and we appreciate you using some of it to help us!

User-testing Procedure

Summary

- We will use randomly generated passwords for this study; we will not ask or learn anything about the participant's real passwords.
- The participant will be asked to engage in mental motor-intention tasks such as '*imagine moving your left arm in a circular motion*' without actually moving.
- A head-worn device that detects mental states (Emotiv Insight) will be used to translate mental motor-intention tasks into discrete commands that can be used to interact with a computer system.
- The commands for our study correspond to four movement directions: up, down, left, and right. The type of motor-intent is spatially related to the command: the 'left' command is initiated by a mental motor-intention task focused on the left arm/hand; the 'up' command is associated with the head, and so on.
- The participant will be asked to use these commands to draw a path through a 2-dimensional grid, which constitutes a password.
- The participant will be asked to learn three randomly-generated passwords of this sort. They will then engage in a distractor task for some time, followed by attempting to enter each of the passwords that were created earlier.

Procedure

- The participant will be invited into a room in our lab designated for user-testing.
- A consent form (attached) will be provided and the researcher will explain the objective of the study
- The researcher will explain that that the participant may choose to withdraw from the study at any time and will still receive full compensation.
- The participant will have an opportunity to ask the researcher any questions that they may have about the study, and informed that they may also ask questions at any point during the study.
- The researcher will remain in the room with the participant for the duration of the study.
- The participant will be asked to complete a brief demographic questionnaire which will ask their age, field of work/study, frequency of desktop/laptop computer use, and whether they have ever used a brain-sensing device or similar.

- Training Phase

    - The participant will be asked to place the mental-activity sensing device onto their head and shown a diagram indicating the correct position.
    - The device may require some adjustment. The researcher will ask the participant whether they are comfortable with the researcher adjusting the device on their head; if they are not, the researcher will provide verbal instructions and guidance to assist the participant in fitting the device.
    - Using Emotiv BCI software, the participant will train four mental commands corresponding to 'up', 'down', 'left', and 'right'. This process involves the user selecting a command to train, and then performing a specific mental activity during an 8-second window. This is done repeatedly for four commands until the device can reliably discriminate between the commands.
- Password Creation
    - The participant will be assigned a randomly generated password consisting of a starting point on 2-dimensional grid and a series of directional steps that represent a path through the grid (similar to a *pattern unlock* paradigm that is common on mobile phones).
    - The participant will practice entering their password by entering the correct series of mental commands to draw their assigned pattern on the grid. Initially, there will be a guide showing the correct pattern overlaid on the grid.
    - The password entry process is as follows: the participant will press the 'Spacebar' key on the computer keyboard to initiate a command. A visual indicator will appear on screen indicating that the system is listening for commands. The system will listen until a threshold value for a specific command is reached, at which point the chosen command will be executed.
        - e.g., the participant wants to enter the command 'left'; they press the spacebar and begin performing the mental activity that they have associated with that command; after a few seconds, the 'strength' of the 'left' command will surpass the threshold value and the 'left' command will be executed; the circular position indicator on the grid will move one point to the left.
        - the participant has the ability to 'undo' their last steps or to undo all steps and reset the grid to its initial state using keyboard commands.
    - After successfully entering their password twice with the guide, the guide will be hidden and they will be asked to enter their passwtord again twice without the additional visual aid. Once they have

succeeded twice without a guide, their password will have been successfully created.
    - The participant will repeat this process to create a total of three passwords, which will be referred to with different names (i.e., "Facebook Password", "Banking Password", etc.).
- Distractor Task
    - The participant will be asked to do a mental rotation task (https://www.psytoolkit.org/experiment-library/mentalrotation.html). A complex 3-dimensional geometric shape is presented as the target, along with three other similar shapes. One of the shapes is a rotated version of the target, and the participant is asked to find that shape.
    - We are interested in collecting any data from this task; the purpose is to occupy the participant and prevent mental rehearsal of the passwords learned in the first phase in order to have a more robust test of password recall in the following phase.

- Password Entry
    - The participant will be asked to enter each of the three passwords that they practised during the password creation stage. The order in which they are asked to enter the passwords will be pseudorandomized and different from the order in which they were created.
    - The guide is hidden during password entry attempts.
    - The participant will have limited time during each password entry (2 minutes), and the trial will continue until the participant (a) successfully enters their password, (b) does not successfully enter their password within the time limit, or (c), gives up and ends the trial.
    - After attempting to enter all three passwords, the study will be concluded. The participant will be given a debriefing document containing more information and background about the study, as well as contact information of the researcher and PI if they wish to followup with additional questions. The participant will have an opportunity before leaving to ask questions. The participant will be paid and they will sign a receipt verifying that they have received compensation.

A.2 Interview Study

Semi-Structured Interview Procedure

We will conduct semi-structured qualitative interviews with BCI users and researchers recruited from online forums (reddit.com/r/bci and neurobb.com). There are five topics that we intend to explore during the interviews which are: basic information about the participant and their experience with BCI devices; usability and user experience of BCI devices; physical and psychological comfort with BCI use; opinions about data privacy relating to BCI devices; and the use of BCIs for authentication. If the participant is a researcher, the interviewer will ask about the participant's personal experiences as a BCI user as well as their experiences conducting research with other users.

Prior to each interview, the potential participant will receive a consent form through email. They may indicate their consent to participate by replying to the email with a message explicitly indicating their consent. Participants will be verbally reminded at the beginning of the interview that they may choose to not answer any question that they do not wish to answer and are free to withdraw end the interview at any time.

For each topic, the interviewer will ask a series of pre-determined open-ended questions (see attached Interview Guide) that are intended to start a conversation about the topic. Based on the participants' answers, the interviewer will ask follow-up questions in order to draw out additional information or to clarify parts of the answers. These followup questions are not predetermined and will be informed by the participants' previous answers.

The interviews will be conducted remotely via Skype voice calls. The interviews will be audio-recorded and the interviewer will also record notes on a laptop. Audio recordings will be kept until the conclusion of the study, at which time they will be deleted. We aim to have the interviews last approximately one hour, but due to the semi-structured approach they may take more or less time depending on the participant and the length of their answers.

After the interview, the interviewer will verbally debrief the participant, explaining the rationale and value of the study as well as where they could find more information. A debriefing email will be sent to the participant containing the same information.

Recruitment Post
The following will be posted to www.reddit.com/r/bci and www.neurobb.com.

[Post title: Participate in a study about BCI authentication!]

Hello,

My name is Josh Carr and I'm a researcher at Carleton University in Ottawa, Canada studying BCIs. For my Master's thesis I'm conducting a study about BCI authentication. As part of this, I'm hoping to conduct interviews with some users and/or researchers about their thoughts and opinions about privacy, cybersecurity, and authentication with regard to BCIs. In particular I'm interested in discussing non-invasive commercial BCI devices (i.e., Emotiv, OpenBCI, Neurosky, Muse) that are used in a non-medical context.

The interview would be done over the phone or via Skype and would last approximately 1 hour. All data collected from the interview will be anonymized and stripped of any information that could potentially be used to identify you. You must be over the age of 18 to participate.

If you are interested in participating, please contact me by email at josh.carr@carleton.ca or send me a private message through [reddit/neurobb].

The ethics protocol for this study has been reviewed and cleared by the Carleton University Research Ethics Board [CUREB-B Clearance # 111922.

Interview Guide

The following questions will be asked of interviewees. Top level bullets are primary questions which will definitely be asked for each participant, and sub-bullets are potential followup questions which may or may not be asked depending on the participants' answers to the primary questions. Other followup questions may be asked depending on participants' answers in order to draw out information. Not all followup questions can be known in advance.

Basic Information

- In what capacity do you have experience with BCIs? As a researcher, a casual user, or something else?
- What types/brands of commercial BCIs do you have experience with? (e.g., Emotiv, Muse, OpenBCI, Neurosky)

Usability

- Generally speaking, how do you feel about the performance of BCIs? Do they live up to your expectations?
  - Are there times when [you/users] have greater/lesser difficulty using BCIs?
  - Do [you/users] ever become frustrated when using BCIs? Why?

Comfort

- What do you think about the physical comfort of wearing BCI devices?
- Does the comfort of wearing a BCI change over the course of a session?
- What about the appearance of the device?
  - Would you feel comfortable using a BCI in public or in the presence of strangers?

Privacy

- What do you think about the privacy implications of using BCIs?
  - Concerning the BCI devices that you have used, are you familiar with the manufacturers' privacy policies?
  - Would you be willing to allow the BCI manufacturer or a third-party company to collect data from your BCI device in exchange for additional features or services?
- What do you think about /neuromarketing/, or the idea that companies could use data from BCIs to learn a user's likes/dislikes and use that information to target specific advertisements toward them?

Authentication

- Have you ever tried to use any type of authentication (e.g., entering a password) using a BCI?
  - Describe your experience; was it easy or difficult? how long did it take?
- What do you think about BCI biometric authentication, similar to using your fingerprint or iris?
  - Would you feel comfortable with the level of security offered by such a system? Why/why not?
  - What about the idea of a /passthought/ system where you authenticate by thinking a particular thought (such as a strong memory or part of a song)?
- Do you think this would be more or less secure than simple biometric authentication?

Interview Consent
[The following will be sent to interested potential participants via email]

You are invited to participate in a study on brain-computer interfaces (BCIs) and BCI-based authentication. This study aims to understand the psychological and social factors underlying brain-computer interface (BCI) adoption, particularly with respect to privacy and cybersecurity. The researchers for this study are Professor Robert Biddle and Josh Carr.

The present study is meant to learn about factors related to BCI use and adoption as well as attitudes toward privacy and cybersecurity with respect to BCIs. The study will be in the form of a ~60 minute semi-structured interview. The interviewer will ask you a series of open-ended questions about your experience with BCIs, your opinions about the physical and psychological comfort of using BCIs, your opinions about privacy with respect to data collected from BCIs, and your experience and opinions regarding digital authentication using BCIs. You may respond to these questions in any way that you prefer; there are no bad answers. Based on your answers, the interviewer will ask follow-up questions in order to clarify or get more information. You may choose not to answer any of the questions. If at any point you do not wish to continue, simply tell the interviewer and they will end the interview. The interviewer will ask you if you wish to withdraw your data, in which case all records of your interview will be immediately destroyed.

The interview will be audio recorded and the recording will be kept for a period of 3 months for analysis, after which they will be deleted. Notes from the interview will be anonymized: any data that could potentially be used to identify you will not be included the interview notes and the interview data will not be associated with your name or identity in any way. After the recordings have been deleted, you will no longer be able to withdraw your data from the study as we will have no way of linking the data back to you.

To be eligible to participate, you must be at least 18 years of age and have experience with non-invasive commercial BCI devices (e.g., Emotiv, OpenBCI, Muse) either as a casual user or as a researcher.

Once you have read this document, if you still wish to participate in the study, please reply to this email with the text "I [your name] have read the Consent Form and volunteer to participate in the study entitled 'Exploring Thought-Based Passwords'".

The ethics protocol for this study has been reviewed and cleared by the Carleton University Research Ethics Board [CUREB-B Clearance # 111922].

Researcher contact information:
Josh Carr
Computer Science/Cognitive Science
josh.carr@carleton.ca

Supervisor contact information:
Dr. Robert Biddle
Computer Science/Cognitive Science
robert.biddle@carleton.ca

Should you have any ethical concerns with the study, please contact the REB Chair, Carleton University Research Ethics Board-B (by phone: 613-520-2600 ext. 4085, or by email: ethics@carleton.ca). For all other questions about the study, please contact the researcher.

Interview Debriefing
[The following will be sent to interview participants via email at the end of the study]

What are we trying to learn in this research?
This interview study is part of a larger effort to develop and test feasibility of a BCI-based authentication system. Through these interviews we hope to get a better understanding of BCI-users' perspectives on authentication and related topics, such as data privacy, which will help us in contextualizing the rest of our findings.

Why is this research important?
Most research into BCI-based authentication has focused on technical elements, such as system performance and error-rates, while relatively little work has been done to examine the personal and psychological factors related the adoption of BCI-based authentication. The goal of this study is to address that gap by conducting interviews with experienced BCI users and researchers. In doing this we hope to gain valuable insights which will help us in designing a suitable authentication system.

BCI-based authentication is interesting as a potential alternative to traditional password authentication. Passwords are the most common method of authentication but suffer from poor usability, which in turn negatively impacts their security. Remembering unique passwords for every account is difficult, which frequently results in users re-using the same password multiple times or writing their passwords down, both of which present significant security vulnerabilities. BCI-based authentication offers unique possibilities due to the unique way in which each individual's brain expresses thoughts. This allows us to combine multiple authentication factors into a single step, potentially offering better security and usability than other methods.

Where can I learn more?
Below are a few published papers on the topic of password security and BCI-based authentication that inspired this project:

Thorpe, J., van Oorschot, P.C., and Somayaji, A. 2005. Passthoughts: Authenticating with our Minds. Proceedings of the 2005 Workshop on New Security Paradigms. DOI: https://doi.org/10/dt5ht4

Lin, F., Cho, K.W., Song, C., Xu, W., Jin, Z. 2018. Brain Password: A secure and Truly Cancelable Brain Biometrics for Smart Headware. MobiSys '18. DOI: https://doi.org/10/gf6jdm

Paranjape, R.B., Mahovsky, J., Benedicenti, L., and Koles, Z. 2001. The electroencephalogram as a biometric. Canadian Conference on Electrical and Computer Engineering 2001. DOI: 10.1109/ccece.2001.933649

Jayarathne, I., Cohen, M., and Amarakeerthi, S. 2017. Survey of EEG-based biometric authentication. IEEE iCAST 8. DOI: 10.1109/icawst.2017.8256471},

What if I have questions later?
You are welcome to email the researcher at any time if you have any questions, concerns, or comments about the experiment. Josh (Lead Researcher) can be reached at josh.carr@carleton.ca, and Professor Biddle at robert.biddle@carleton.ca.

A.3 MTurk Questionnaire Study

A2. **Title of research project: Exploring Thought-Based Passwords**
Funding Source: NSERC
Date of ethics clearance: April 2, 2020
Ethics Clearance for the Collection of Data Expires: November 30, 2020
CUREB-B Clearance # 111922

You are invited to complete a questionnaire about the possibilities for brain-computer interfaces (BCIs). This study aims to understand the psychological and social factors underlying brain-computer interface (BCI) adoption, particularly with respect to privacy and cybersecurity. The researchers for this study are Professor Robert Biddle and Josh Carr.

This study will involve a series of questions and statements that you will be asked to respond to. The questions are meant to assess general personality traits, cybersecurity behaviours, and perceptions and attitudes toward brain-computer interfaces. You will not be asked to disclose any private or sensitive information. Your responses will help us to understand how that privacy and security concerns influence acceptance of new technologies.
You must be fluent in English to participate. All responses are completely anonymous. The questionnaire will take approximately 15 minutes and you will be compensated $2. There are no risks associated with this study, as it will take place entirely in your web browser.

Data from this questionnaire will be retained indefinitely on our on-site server. Because responses are anonymous, it will not be possible to withdraw or have your data deleted at a later time as there will be no way of linking the data back to you.

Researcher contact information:
Josh Carr
Carleton University
Computer Science/Cognitive Science
josh.carr@carleton.ca
Supervisor contact information:
Dr. Robert Biddle
Carleton University
Computer Science/Cognitive Science robert.biddle@carleton.ca

Should you have any ethical concerns with the study, please contact the REB Chair, Carleton University Research Ethics Board-B (by phone: 613-520-2600 ext. 4085, or by email: ethics@carleton.ca). For all other questions about the study, please contact the researcher.

I have read the Consent Form and agree to participate in the study (Continue to Survey) ☐

I do not wish to participate in the study (Exit Survey) ☐

Section B: Demographics

B1. Please enter your age in years

B2. What is your level of education?

- [ ] Primary/Elementary School
- [ ] High-School
- [ ] Vocational/Trade School
- [ ] Bachelor's Degree
- [ ] Graduate/Professional School
- [ ] Other

Other

B3. Please indicate your gender identity:

- [ ] Female
- [ ] Male
- [ ] Prefer not to answer
- [ ] Self-describe:

Self-describe:

Section C: Ten Item Personality Inventory

Here are a number of personality traits that may or may not apply to you. For each pair of traits, please indicate the extent to which you agree or disagree that those traits apply to you. You should rate the extent to which the pair of traits applies to you, even if one applies more strongly than the other.

C1. I see myself as...

	Strongly disagree	Disagree	Disagree somewhat	Neutral	Agree somewhat	Agree	Strongly agree
Extraverted, enthusiastic	☐	☐	☐	☐	☐	☐	☐
Critical, quarrelsome	☐	☐	☐	☐	☐	☐	☐
Dependable, self-disciplined	☐	☐	☐	☐	☐	☐	☐
Anxious, easily upset	☐	☐	☐	☐	☐	☐	☐
Open to new experiences, complex	☐	☐	☐	☐	☐	☐	☐
Reserved, quiet	☐	☐	☐	☐	☐	☐	☐
Sympathetic, warm	☐	☐	☐	☐	☐	☐	☐
Disorganized, careless	☐	☐	☐	☐	☐	☐	☐
Calm, emotionally stable	☐	☐	☐	☐	☐	☐	☐
Conventional, uncreative	☐	☐	☐	☐	☐	☐	☐

Section D: Security Behaviour Intentions Scale

D1. Please rate the following statements according to how often they apply to you:

	Never	Rarely	Sometimes	Often	Always
When I'm prompted about a software update, I install it right away.	☐	☐	☐	☐	☐
I try to make sure that the programs I use are up-to-date.	☐	☐	☐	☐	☐
I manually lock my computer screen when I step away from it.	☐	☐	☐	☐	☐
I set my computer screen to automatically lock if I don't use it for a prolonged period of time.	☐	☐	☐	☐	☐
I use a PIN or passcode to unlock my mobile phone.	☐	☐	☐	☐	☐

	Never	Rarely	Sometimes	Often	Always
I use a password/passcode to unlock my laptop or tablet.	☐	☐	☐	☐	☐
If I discover a security problem, I continue what I was doing because I assume someone else will fix it.	☐	☐	☐	☐	☐
When someone sends me a link, I open it without first verifying where it goes.	☐	☐	☐	☐	☐
I verify that my anti-virus software has been regularly updating itself.	☐	☐	☐	☐	☐
When browsing websites, I mouseover links to see where they go before clicking them.	☐	☐	☐	☐	☐
I know what websites I'm visiting based on its look and feel, rather than by looking on the URL bar.	☐	☐	☐	☐	☐
I do no change passwords unless I have to.	☐	☐	☐	☐	☐
I use different passwords for different accounts that I have.	☐	☐	☐	☐	☐
I do no include special characters in my password if it's not required.	☐	☐	☐	☐	☐
When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.	☐	☐	☐	☐	☐
I submit information to websites without first verifying that it will be sent securely (e.g., SSL, HTTPS, a lock icon).	☐	☐	☐	☐	☐

Section E: BCI Description

A brain-computer interface, or BCI, is a system that allows a user to control a computer system with their mind. At it's simplest, a BCI reads signals coming from the brain and then does something based on the signals it receives, such as moving a mouse cursor on a screen or controlling a robotic arm. There are several BCI devices on the market which measure the electrical activity of parts of the brain using sensors placed on the scalp.

Below are a few images of a wearable BCI device called the Emotiv Insight (www.emotiv.com). Please look at them and try to imagine what it would be like to wear the device. In the next section you will be asked about your thoughts about the device.

Section F: Comfort of Wearable Devices Scale

Images from the previous page:

F1. Concerning the device in the photos above, please rate the following statements based on how much you agree with them:

	Strongly disagree	Disagree	Disagree somewhat	Neutral	Agree somewhat	Agree	Strongly agree
I would be worried about how I looked wearing the device and what others would think .	☐	☐	☐	☐	☐	☐	☐
I would be constantly aware of the device's presence on my head.	☐	☐	☐	☐	☐	☐	☐
After some time I would get used to the presence of the device on my head.	☐	☐	☐	☐	☐	☐	☐
The device would be safe, and unable to cause me any physical harm.	☐	☐	☐	☐	☐	☐	☐
The device would make me feel physically different. I would feel strange wearing it.	☐	☐	☐	☐	☐	☐	☐
The device would affect the way that I move. It would inhibit or restrict my movement.	☐	☐	☐	☐	☐	☐	☐
My movement would be unaffected by wearing the device.	☐	☐	☐	☐	☐	☐	☐
I would feel at-risk while wearing the device. Wearing the device would make me anxious.	☐	☐	☐	☐	☐	☐	☐
I would feel normal wearing the device. It wouldn't make me feel physically different.	☐	☐	☐	☐	☐	☐	☐

Section G: BCI Questions

G1. Please rate your level of knowledge/experience of BCI devices.

	No knowledge/experience whatsoever	Aware of BCIs but don't know much about them	A bit knowledgeable about BCIs	Moderately knowledgeable about BCIs	Very knowledgeable about BCIs
BCI Knowledge	☐	☐	☐	☐	☐

G2. BCIs in the future

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
In the future, wearable BCI devices will become mainstream and most people will use them.	☐	☐	☐	☐	☐
BCI devices will probably never become popular.	☐	☐	☐	☐	☐
Wearable BCI devices will be vulnerable to previously-unknown types of security challenges.	☐	☐	☐	☐	☐
In the future, companies like Google and Facebook will use data from BCI devices to learn about users for the purpose of advertisement targeting.	☐	☐	☐	☐	☐

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
In the future, governments will use wearable BCI devices for surveillance.	☐	☐	☐	☐	☐

G3. Consumer protections for BCI users

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
There should be special protections or regulations about the collection and use of data from wearable BCI	☐	☐	☐	☐	☐
Current privacy regulations are sufficient to protect BCI users.	☐	☐	☐	☐	☐
Companies that collect data from these BCI devices should be required to disclose how the data will be used.	☐	☐	☐	☐	☐
Please select "Agree" as your answer for this question.	☐	☐	☐	☐	☐
Companies that collect data from these BCI devices should be required to ask for consent before collecting any data.	☐	☐	☐	☐	☐
BCI manufacturers should be able to collect and use data from BCI devices without explicit permission.	☐	☐	☐	☐	☐
Users should have no rights to force companies to delete data collected from them.	☐	☐	☐	☐	☐

G4. Security of BCIs

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Data from BCI devices is more sensitive than that of other wearable devices (e.g., smartwatch).	☐	☐	☐	☐	☐
Current security practices like encryption are insufficient to protect data generated by BCI devices.	☐	☐	☐	☐	☐
It would be impossible for a hacker to cause physical harm or damage by taking control of the device.	☐	☐	☐	☐	☐
A hacker could use data intercepted from a BCI device to infer private information about the user.	☐	☐	☐	☐	☐

G5. What sort of information might they be able to learn (select all that apply):

- Gender ☐
- Sexual Orientation ☐
- Ethnicity ☐
- Political/religious beliefs ☐
- Emotional State ☐
- Passwords for online accounts ☐
- Medical or health-related information (including mental health) ☐
- Whether the user is telling the truth or lying ☐

You have reached the end of the survey. Thank you for your participation! The completion code for this study is: BC99

Appendix B

R Code

B.1 Data Validation and Pre-Processing Script

```
library(tidyverse)

process_data  <- function(df) {
  # remove empty columns
  df <- df[,colSums(is.na(df))<nrow(df)]

  df  <- df %>%
    rename(
      bciKnowledge       = `bciKnowledge[01]`,
      bciDataGender      = `bciData[gender]`,
      bciDataOrientation = `bciData[orientation]`,
      bciDataEthnicity   = `bciData[ethnicity]`,
      bciDataReligpolit  = `bciData[religpolit]`,
      bciDataEmotion     = `bciData[emotion]`,
      bciDataPassword    = `bciData[password]`,
      bciDataHealth      = `bciData[health]`,
      bciDataTruth       = `bciData[truth]`,

      # the timings dont have the group titles by default
      consentTime = groupTime392,
      demogTime   = groupTime386,
      tipiTime    = groupTime387,
      sebisTime   = groupTime388,
      bciDescTime = groupTime389,
      comfortTime = groupTime391,
      bciTime     = groupTime390,

      # rename and fix some unfortunate typos in the survey question codes
      COMFappearance     = `comfort[COMFemotion]`,
      COMFattachment1 = `comfort[COMFattachment]`,
      COMFattachment2 = `comfort[COMattachment2]`,
      COMFharm        = `comfort[COMFharm]`,
      COMFchange1     = `comfort[COMFchange]`,
      COMFchange2     = `comfort[COMchange2]`,
      COMFmovement1   = `comfort[COMFmovement]`,
      COMFmovement2   = `comfort[COMmovement2]`,
      COMFanxiety     = `comfort[COMFanxiety]`,

      # this validation question should be 4 if the respondent is paying
      # attention
      flagQuestion = `bciConsumer[07]`
    )

  # remove all remaining brackets from column titles
  names(df) <- str_replace(names(df), "\\[", "")
  names(df) <- str_replace(names(df), "\\]", "")

  df <- df %>%
    filter(
      # remove cases that didn't accept consent
      consent == "yes",
    ) %>%
    mutate(
      # calculate difference between reversed items for validation
```

```r
        validation1 = abs(COMFattachment1 - reverse_7_item(COMFattachment2)),
        validation2 = abs(COMFmovement1 - reverse_7_item(COMFmovement2)),
        validation3 = abs(COMFchange1 - reverse_7_item(COMFchange2)),
        validation4 = abs(bciFuture01 - reverse_5_item(bciFuture02)),
        validation5 = abs(bciConsumer04 - reverse_5_item(bciConsumer05)),

        inconsistent_answers = (
            # set difference thresholds here
            # 1-3 are from 7-choice responses, 4 and 5 are 5-choice
            validation1 > 4 |
            validation2 > 4 |
            validation3 > 4 |
            validation4 > 3 |
            validation5 > 3
          ),

        # recode answers to education question
        edu = recode_factor(factor(edu, ordered = T,
                                   levels = c("A1", "A2", "A3", "A4", "A5")),
                            A1 = "Primary", A2 = "High-school",
                            A3 = "Trade/Vocational", A4 = "Bachelor's",
                            A5 = "Graduate/Professional"),
        edu = fct_explicit_na(edu),

        # calculate subscale scores
        TIPIextraversion        = (tipi01 + reverse_7_item(tipi06)) / 2,
        TIPIagreeableness       = (reverse_7_item(tipi02) +tipi07) / 2,
        TIPIconscientiousness   = (tipi03 + reverse_7_item(tipi08)) / 2,
        TIPIemotional_stability = (reverse_7_item(tipi04) + tipi09) / 2,
        TIPIopenness_to_exp     = (tipi05 + reverse_7_item(tipi10)) / 2,

        SEBISsecurement         = (sebis04 + sebis06 + sebis03 + sebis05 ) / 4,
        SEBISpasswordgen        = (reverse_5_item(sebis12) + sebis13 +
                                   sebis15 + reverse_5_item(sebis14) ) / 4,
        SEBISproactiveawareness = (reverse_5_item(sebis08) + reverse_5_item(sebis11) +
                                   reverse_5_item(sebis16) + sebis10 +
                                   reverse_5_item(sebis07) ) / 5,
        SEBISupdating           = (sebis01 + sebis02 + sebis09 ) / 3,

        COMFappearance    = reverse_7_item(COMFappearance),
        COMFattachment = (COMFattachment1 + reverse_7_item(COMFattachment2)) / 2,
        COMFharm       = reverse_7_item(COMFharm),
        COMFchange     = (COMFchange1 + reverse_7_item(COMFchange2)) / 2,
        COMFmovement   = (COMFmovement1 + reverse_7_item(COMFmovement2)) / 2,
        COMFanxiety    = COMFanxiety,

        bciFuture   = (bciFuture01 + reverse_5_item(bciFuture02) +
                       bciFuture03 + bciFuture04 + bciFuture05) / 5,
        bciConsumer = (bciConsumer01 + reverse_5_item(bciConsumer02) +
                       bciConsumer03 + bciConsumer04 +
                       reverse_5_item(bciConsumer05) +
                       reverse_5_item(bciConsumer06)) / 6,
        bciSecurity = (bciSec01 + bciSec02 + reverse_5_item(bciSec03) +
                       bciSec04) / 4,
        )

    # summary
    pre_n_male   <- sum(df$gender == "m")
    pre_n_female <- sum(df$gender == "f")
    pre_mean_age <- mean(df$age)
    pre_sd_age   <- sd(df$age)
    n_failed_flag <- sum(df$flagQuestion != 4, na.rm = T)
    inconsistent_answers <- sum(df$inconsistent_answers, na.rm = T)
    pre_fast_completion  <- sum(df$interviewtime < 240)

    print("Summary (before filtering):")
    print("~~~~~~~~~")
```

```
  print(sprintf("n: %s", nrow(df)))
  print(sprintf("n male: %s   female: %s", pre_n_male, pre_n_female))
  print(sprintf("mean age: %s   sd: %s", round(pre_mean_age, digits = 2),
                round(pre_sd_age, digits = 2)))
  print(sprintf("n failed flag question: %s", n_failed_flag))
  print(sprintf("n inconsistent answers: %s", inconsistent_answers))
  print(sprintf("n < 4 min: %s", pre_fast_completion))
  print("~~~~~~~~~")
  writeLines("")

  df  <- filter(df, flagQuestion == 4, !inconsistent_answers)

  post_n_male   <- sum(df$gender == "m")
  post_n_female <- sum(df$gender == "f")
  post_mean_age <- mean(df$age)
  post_sd_age   <- sd(df$age)
  post_fast_completion  <- sum(df$interviewtime < 240)

  print("Summary (after filtering):")
  print("~~~~~~~~~")
  print(sprintf("n: %s", nrow(df)))
  print(sprintf("n male: %s   female: %s", post_n_male, post_n_female))
  print(sprintf("mean age: %s   sd: %s", round(post_mean_age, digits = 2),
                round(post_sd_age, digits = 2)))
  print(sprintf("n < 4 min: %s", post_fast_completion))
  print("~~~~~~~~~")

  return(df)
}

# functions to reverse-score columns
reverse_7_item  <- function(col) {
  for (i in (1:length(col))) {
    if (is.na(col[i])) { }
    else if (col[i] == 7) { col[i]  <- 1 }
    else if (col[i] == 6) { col[i]  <- 2 }
    else if (col[i] == 5) { col[i]  <- 3 }
    else if (col[i] == 3) { col[i]  <- 5 }
    else if (col[i] == 2) { col[i]  <- 6 }
    else if (col[i] == 1) { col[i]  <- 7 }
  }
  return(col)
}

reverse_5_item  <- function(col) {
  for (i in (1:length(col))) {
    if (is.na(col[i])) { }
    else if (col[i] == 5) { col[i]  <- 1 }
    else if (col[i] == 4) { col[i]  <- 2 }
    else if (col[i] == 2) { col[i]  <- 4 }
    else if (col[i] == 1) { col[i]  <- 5 }
  }
  return(col)
}

# import
data  <- read_csv("bci_survey_results.csv")
df_processed  <- process_data(data)
```

B.2 Data Analysis and Hypothesis Testing Script

```
# SETUP
library(tidyverse)
```

```r
library(ggExtra)
library(gridExtra)
library(ggpubr)
library(xtable)
library(extrafont) # for embedding fonts

source("validation.r")

loadfonts()

theme_set(
  theme_classic()
)

theme_update(
  strip.background = element_rect(color = NA),
)

update_geom_defaults("col",   list(colour = "black", fill = "grey"))
update_geom_defaults("bar",   list(colour = "black", fill = "grey"))


# DATA IMPORT
df  <- read_csv("bci_survey_results.csv")
df  <- process_data(df)


# DESCRIPTIVE STATS
# Gender
n_male  <- sum(df$gender == "m")
n_female  <- sum(df$gender == "f")


# Age
median_age  <- round(median(df$age, na.rm = TRUE), digits = 2)
mean_age  <- round(mean(df$age, na.rm = TRUE), digits = 2)
sd_age  <- round(sd(df$age, na.rm = TRUE), digits = 2)

age_hist  <- ggplot(df, aes(age)) +
  geom_histogram(binwidth = 2) +
  geom_vline(xintercept = median_age, alpha = 2/3, linetype = "dashed") +
  labs(x = "Age (years)",
       y = "n",
       title = "a)"
       # caption = "* dashed line is the median"
       )
ggsave(filename = "figures/hist_age.png", height = 8, width = 8, units = "cm")
# embed_fonts("figures/hist_age.pdf")


# Education
by_edu <- df %>%
  group_by(edu) %>%
  summarize(n = n()) %>%
  rename(Education = edu)
print(xtable(by_edu, sanitize.text.function = identity,
             label = "desc_edu",
             caption = "Frequency table of levels of education for the sample."
            ), file = "tables/edu_desc.tex", include.rownames = FALSE)
# print(by_edu)

edu_hist <- ggplot(by_edu, aes(Education, n)) +
  geom_col() +
  labs(x = "Education Level",
       y = "n"
       # title = "c)"
       )
```

```r
ggsave(filename = "figures/hist_edu.png", width = 14, height = 8, units = "cm")
# embed_fonts("figures/hist_edu.pdf")


# Time
mean_time  <- round(mean(df$interviewtime, na.rm = TRUE), digits = 2)
median_time  <- median(df$interviewtime, na.rm = TRUE)
sd_time  <- round(sd(df$interviewtime, na.rm = TRUE), digits = 2)
n_under_4 <- round(sum(df$interviewtime < 240), digits = 2)

time_hist  <- ggplot(df, aes(interviewtime)) +
  geom_histogram() +
  geom_vline(xintercept = median_time, alpha = 2/3, linetype = "dashed") +
  labs(x = "Survey Duration (seconds)",
       y = "n",
       title = "b)"
       # caption = "* dashed line is the median"
       )
ggsave(filename = "figures/hist_time.png")
# embed_fonts("figures/hist_time.pdf")

hist_demogs_merged <- grid.arrange(age_hist, time_hist, nrow = 1)
ggsave(hist_demogs_merged, filename = "figures/hist_demogs_merged.png",
      width = 20, height = 8, units = "cm"
       )
# embed_fonts("figures/hist_demogs_merged.pdf")

# function to plot subscales for sebis, tipi, etc
subscale_plot <- function(df, subscales, bw = 0.5, labx = "", laby = "n") {
  plot  <- ggplot(df, aes(value)) +
    geom_histogram(binwidth = bw) +
    facet_wrap(~ Scale, ncol = 2) +
    labs(x = labx,
         y = laby)

  for (scale in subscales) {
    plot  <- plot +
      geom_vline(
        data = filter(df, scale == Scale),
        aes(xintercept = median(value)),
        linetype = "dashed")
  }
}


# TIPI Big5
tipi_by_scale  <- df %>%
  select(id, TIPIextraversion:TIPIopenness_to_exp) %>%
  rename(
    "Agreeableness" = TIPIagreeableness,
    "Conscientiousness" = TIPIconscientiousness,
    "Extraversion" = TIPIextraversion,
    "Emotional Stability" = TIPIemotional_stability,
    "Openness to Experience" = TIPIopenness_to_exp,
    ) %>%
  pivot_longer(cols = "Extraversion":"Openness to Experience", names_to = "Scale")

popnorms <- c(4.91, 4.94, 4.56, 3.98, 5.46)

tipi_desc_table <- tipi_by_scale %>%
  group_by(Scale) %>%
  summarize(Median = median(value),
            Mean = mean(value),
            SD = sd(value))

tipi_desc_table["Population Mean"]  <- popnorms

```

```r
print(xtable(tipi_desc_table,
             label = "tipi_desc",
             caption = c("Descriptive statistics for the subscales of the TIPI.
             Scores on each subscale are calculated by taking the average of the
             subscale items after reverse-scoring as appropriate. Population
             mean values are from \\authorcite{gosling14}. Scores on each
             subscale can range from 0 to 7.",
             "Descriptive statistics for the subscales of the TIPI.")),
      file = "tables/tipi_desc.tex",
      include.rownames = FALSE)
# print(tipi_desc_table)

tipi_subscale_hist  <- subscale_plot(tipi_by_scale,
                                     c("Agreeableness", "Conscientiousness",
                                       "Extraversion", "Emotional Stability",
                                       "Openness to Experience"))
print(tipi_subscale_hist)
ggsave(filename = "figures/hist_tipi.png",
       height = 18, width = 18, units = "cm"
       )
# embed_fonts("figures/hist_tipi.pdf")


# SeBIS
sebis_by_scale  <- df %>%
  select(id, SEBISsecurement:SEBISupdating) %>%
  rename(
    "Securement" = SEBISsecurement,
    "Password Generation" = SEBISpasswordgen,
    "Proactive Awareness" = SEBISproactiveawareness,
    "Updating" = SEBISupdating
  ) %>%
  pivot_longer(cols = Securement:Updating, names_to = "Scale")

sebis_desc_table <- sebis_by_scale %>%
  group_by(Scale) %>%
  summarize(Median = median(value),
            Mean = mean(value),
            SD = sd(value))
print(xtable(sebis_desc_table,
             label = "sebis_desc",
             caption = c("Descriptive statistics of the subscales of the SeBIS.
             Scores on each subscale are calculated by taking the average of
             the subscale items after reverse-scoring as appropriate. Scores
             on each subscale can range from 0 to 5.",
             "Descriptive statistics of the subscales of the SeBIS.")),
             file = "tables/sebis_desc.tex", include.rownames = FALSE)
# print(sebis_desc_table)

sebis_subscale_hist  <- subscale_plot(sebis_by_scale,
                                      c("Securement", "Password Generation",
                                        "Proactive Awareness", "Updating"))
print(sebis_subscale_hist)
ggsave(filename = "figures/hist_sebis_subscales.png",
       height = 18, width = 18, units = "cm"
       )
# embed_fonts("figures/hist_sebis_subscales.pdf")


# Comfort
comfort_by_scale  <- df %>%
  select(id, COMFappearance, COMFharm, COMFanxiety, COMFattachment:COMFmovement) %>%
  rename(
    "Appearance" = COMFappearance,
    "Harm" = COMFharm,
    "Anxiety" = COMFanxiety,
    "Attachment" = COMFattachment,
```

```
    "Change" = COMFchange,
    "Movement" = COMFmovement
  ) %>%
  pivot_longer(cols = Appearance:Movement, names_to = "Scale")

comfort_desc_table <- comfort_by_scale %>%
  group_by(Scale) %>%
  summarize(Median = median(value),
            Mean = mean(value),
            SD = sd(value))
print(xtable(comfort_desc_table,
         label = "comfort_desc",
         caption = c("Descriptive statistics of the six dimensions measured by
         the CRS. Scores on each subscale are calculated by taking the average
         of the subscale items after reverse-scoring as appropriate. Scores on
         each subscale can range from 0 to 7.",
         "Descriptive statistics of the six dimensions measured by the CRS.")),
       file = "tables/comfort_desc.tex", include.rownames = FALSE)

comfort_subscale_hist  <- subscale_plot(comfort_by_scale,
                                        c("Appearance", "Harm", "Anxiety",
                                          "Attachment", "Change", "Movement"),
                                        bw = 1)
print(comfort_subscale_hist)
ggsave(filename = "figures/hist_comfort_subscale.png",
       width = 18, height = 18, units = "cm")
# embed_fonts("figures/hist_comfort_subscale.pdf")


# BCI Scales
bci_by_scale  <- df %>%
  select(id, bciKnowledge, bciFuture:bciSecurity) %>%
  rename(
    "BCI Knowledge" = bciKnowledge,
    "Future of BCIs" = bciFuture,
    "Consumer Protection" = bciConsumer,
    "BCI Security" = bciSecurity,
    ) %>%
  pivot_longer(cols = "BCI Knowledge":"BCI Security", names_to = "Scale")

bci_desc_table <- bci_by_scale %>%
  group_by(Scale) %>%
  summarize(Median = median(value),
            Mean = mean(value),
            SD = sd(value))
print(xtable(bci_desc_table,
             label = "bci_desc",
             caption = c("Descriptive statistics for the four subscales of the
             BIS. Scores on each subscale are calculated by taking the average
             of the subscale items after reverse-scoring as appropriate. Scores on
             each subscale can range from 0 to 5.",
             "Descriptive statistics for the four subscales of the BIS.")),
       file = "tables/bci_desc.tex", include.rownames = FALSE)
# print(bci_desc_table)

bci_subscale_hist  <- subscale_plot(bci_by_scale,
                                    c("BCI Knowledge", "Future of BCIs",
                                      "Consumer Protection", "BCI Security"),
                                    bw = 1)
print(bci_subscale_hist)
ggsave(filename = "figures/hist_bci_subscale.png", width = 18,
       height = 18, units = "cm")
# embed_fonts("figures/hist_bci_subscale.pdf")

bci_private_info <- df %>%
  select(id, bciSec04) %>%
  mutate(bciSec04 = factor(bciSec04, ordered = TRUE),
```

```
271           bciSec04 = fct_recode(bciSec04,
272                                 "Strongly disagree" = "1",
273                                 "Disagree" = "2",
274                                 "Neutral" = "3",
275                                 "Agree" = "4",
276                                 "Strongly agree" = "5",
277                                 )) %>%
278     rename(Answer = bciSec04) %>%
279     group_by(Answer) %>%
280     summarize(n = n())
281
282   print(xtable(bci_private_info,
283                label = "bci_private_info",
284                caption = "Frequency table of the responses to the BIS:Security
285                item ``A hacker could use data intercepted from a BCI device to
286                infer private information about the user.''",
287                digits = c(0, 0, 0)),
288         file = "tables/bci_private_info_desc.tex", include.rownames = FALSE)
289   # print(bci_private_info)
290
291
292   bci_private_info_hist  <- ggplot(bci_private_info, aes(Answer, n)) +
293     geom_col() +
294     labs(
295       x = "Response",
296       y = "n"
297     )
298   ggsave(filename = "figures/hist_bci_private_info.png", width = 5, height = 5)
299   # embed_fonts("figures/hist_bci_private_info.pdf")
300
301
302   bci_info_types  <- df %>%
303     select(id, bciSec04, bciDataGender:bciDataTruth) %>%
304     rename(
305       Gender = bciDataGender,
306       `Emotional State` = bciDataEmotion,
307       Ethnicity = bciDataEthnicity,
308       `Medical/Health` = bciDataHealth,
309       `Sexual Orientation` = bciDataOrientation,
310       Passwords = bciDataPassword,
311       `Religious/Political Beliefs` = bciDataReligpolit,
312       Truthfulness = bciDataTruth,
313       ) %>%
314     filter(bciSec04 %in% c(4, 5)) %>%
315     pivot_longer(cols = Gender:Truthfulness, names_to = "Info type") %>%
316     group_by(`Info type`) %>%
317     summarize(n = sum(value)) %>%
318     arrange(desc(n))
319
320   print(xtable(bci_info_types,
321                label = "bci_info_types",
322                caption = c("Frequency table of the responses to the followup question
323                ``What sort of information might they be able to learn (select all
324                that apply)?'', shown to respondents who selected \\emph{Agree} or
325                \\emph{Strongly agree} as their answer to the question in
326                \\ref{bci_private_info}.",
327                "Frequency table of the responses to the followup question
328                ``What sort of information might they be able to learn (select all
329                that apply)?''")),
330                file = "tables/bci_info_types_desc.tex", include.rownames = FALSE)
331
332   bci_info_types_hist  <- ggplot(bci_info_types, aes(reorder(`Info type`, n) , n)) +
333     geom_col() +
334     labs(
335       x = "Response",
336       y = "n"
337     ) +
```

```
  coord_flip()
ggsave(filename = "figures/hist_bci_info_types.png", width = 5, height = 5)
# embed_fonts("figures/hist_bci_info_types.pdf")


# HYPOTHESIS TESTS
median_split_test  <- function(x, y) {
  wilcox.test(y ~ x <= median(x))
}

# custom scatterplot function w/ marginal histograms
plot_width = 10
plot_height = 10

scatterplot  <- function(df, x, y, plot_title = element_blank(),
                         plot_caption = element_blank(), xlab = element_blank(),
                         ylab = element_blank(), xlim = 7, ylim = 7, model,
                         sides = "both") {
    plot  <- ggplot(df, aes(x, y)) +
    geom_smooth(colour = "grey", method = lm, se = FALSE, formula = y ~ x) +
    geom_jitter(alpha = 2/3) +
    labs(title = plot_title, caption = plot_caption, x = xlab, y = ylab) +
    stat_cor(method = "spearman", cor.coef.name = "rho") +
    scale_x_continuous(breaks = 1:xlim, limits = c(1, xlim)) +
    scale_y_continuous(breaks = 1:ylim, limits = c(1, ylim)) +
    coord_fixed()

  plot <- ggMarginal(plot, type = "histogram", fill = "grey", margins = "both")
  return(plot)
}

# SeBIS
# calculate test statistics
hs_1_grp <- median_split_test(df$SEBISsecurement, df$bciSecurity)
hs_1_cor <- cor.test(df$SEBISsecurement, df$bciSecurity, method = "spearman")

hs_2_grp <- median_split_test(df$SEBISsecurement, df$bciFuture)
hs_2_cor <- cor.test(df$SEBISsecurement, df$bciFuture, method = "spearman")

hs_3_grp <- median_split_test(df$SEBISproactiveawareness, df$bciSecurity)
hs_3_cor <- cor.test(df$SEBISproactiveawareness, df$bciSecurity, method = "spearman")

hs_4_grp <- median_split_test(df$SEBISproactiveawareness, df$bciFuture)
hs_4_cor <- cor.test(df$SEBISproactiveawareness, df$bciFuture, method = "spearman")

# create a table
hs_names  <- c("$HS_1$", "$HS_2$", "$HS_3$", "$HS_4$")
hs_rho_vals  <- c()
hs_cor_p_vals  <- c()
hs_grp_stats <- c()
hs_grp_p_vals <- c()

for (test in list(hs_1_cor, hs_2_cor, hs_3_cor, hs_4_cor)) {
  hs_rho_vals  <- c(hs_rho_vals, round(test$estimate, digits = 3))
  hs_cor_p_vals  <- c(hs_cor_p_vals, round(test$p.value, digits = 3))
}

for (test in list(hs_1_grp, hs_2_grp, hs_3_grp, hs_4_grp)) {
  hs_grp_stats <- c(hs_grp_stats, round(test$statistic, digits = 3))
  hs_grp_p_vals <- c(hs_grp_p_vals, round(test$p.value, digits = 3))
}


sebis_hypoth_tests <- tibble(hs_names, hs_rho_vals, hs_cor_p_vals, hs_grp_stats,
                             hs_grp_p_vals) %>%
  rename(Test = hs_names,
         `Spearman $\\rho$` = hs_rho_vals,
```

```
405           `Spearman $p$-value` = hs_cor_p_vals,
406           `Wilcoxon $W$` = hs_grp_stats,
407           `Wilcoxon $p$-value` = hs_grp_p_vals)
408
409   print(xtable(sebis_hypoth_tests,
410                label = "sebis_hypoth_tests",
411                caption = c("Results and $p$-values of Spearman correlation tests
412                and Wilcoxon rank sum test for the SeBIS hypotheses. Wilcoxon
413                tests were conducting by performing a median split on the data
414                based on the relevant SeBIS dimension and testing for a difference
415                between the two groups on the other variable.",
416                "Results and $p$-values of Spearman correlation tests
417                and Wilcoxon rank sum test for the SeBIS hypotheses.")),
418         file = "tables/sebis_hypoth_tests.tex",
419         sanitize.colnames.function = identity,
420         sanitize.text.function = identity,
421         include.rownames = FALSE,
422
423         )
424
425   print(sebis_hypoth_tests)
426
427   # create some scatterplots
428   securement_bcisec_scatter <- scatterplot(df, df$SEBISsecurement, df$bciSecurity,
429                                            plot_title = expression(paste("HS"[1])),
430                                            # plot_title = "(a)",
431                                            xlab = "SeBIS: Securement",
432                                            ylab = "BIS: Security",
433                                            xlim = 5, ylim = 5,
434                                            sides = "both",
435                                            model = hs_1_cor)
436   ggsave(plot = securement_bcisec_scatter,
437          filename = "figures/hs1_scatter_securement_bcisec.pdf",
438          width = plot_width, height = plot_height, units = "cm")
439   embed_fonts("figures/hs1_scatter_securement_bcisec.pdf")
440
441   securement_bcifuture_scatter  <- scatterplot(df, df$SEBISsecurement, df$bciFuture,
442                                               plot_title = expression(paste("HS"[2])),
443                                               # plot_title = "(c)",
444                                               xlab = "SeBIS: Securement",
445                                               ylab = "BIS: Future",
446                                               xlim = 5, ylim = 5,
447                                               # sides = "none",
448                                               model = hs_2_cor)
449   ggsave(plot = securement_bcifuture_scatter,
450          filename = "figures/hs2_scatter_securement_bcifuture.pdf",
451          width = plot_width, height = plot_height, units = "cm")
452   embed_fonts("figures/hs2_scatter_securement_bcifuture.pdf")
453
454   proaware_bcisec_scatter  <- scatterplot(df, df$SEBISproactiveawareness, df$bciSecurity,
455                                           plot_title = expression(paste("HS"[3])),
456                                           # plot_title = "(b)",
457                                           xlab = "SeBIS: Proactive Awareness",
458                                           ylab = "BIS: Security",
459                                           xlim = 5, ylim = 5,
460                                           sides = "both",
461                                           model = hs_3_cor)
462   ggsave(plot = proaware_bcisec_scatter,
463          filename = "figures/hs3_scatter_proaware_bcisec.pdf",
464          width = plot_width, height = plot_height, units = "cm")
465   embed_fonts("figures/hs3_scatter_proaware_bcisec.pdf")
466
467   proaware_bcifuture_scatter  <- scatterplot(df,
468                                             df$SEBISproactiveawareness,
469                                             df$bciFuture,
470                                             plot_title = expression(paste("HS"[4])),
471                                             # plot_title = "(d)",
```

```
                                        xlab = "SeBIS: Proactive Awareness",
                                        ylab = "BIS: Future",
                                        xlim = 5, ylim = 5,
                                        sides = "both",
                                        model = hs_4_cor)
ggsave(plot = proaware_bcifuture_scatter,
       filename = "figures/hs4_scatter_proaware_bcifuture.pdf",
       width = plot_width, height = plot_height, units = "cm")
embed_fonts("figures/hs4_scatter_proaware_bcifuture.pdf")

hs_scatterplots <- grid.arrange(securement_bcisec_scatter,
                                securement_bcifuture_scatter,
                                proaware_bcisec_scatter,
                                proaware_bcifuture_scatter,
                                nrow = 2)
ggsave(hs_scatterplots, file = "figures/hs_scatter_merged.png",
       width = 18, height = 18, units = "cm")
# embed_fonts("figures/hs_scatter_merged.pdf")

# Big 5 Personality
# calculate test statistics
hp_1_grp <- median_split_test(df$TIPIagreeableness, df$COMFanxiety)
hp_1_cor  <- cor.test(df$TIPIagreeableness, df$COMFanxiety, method = "spearman")

hp_2_grp <- median_split_test(df$TIPIemotional_stability, df$COMFappearance)
hp_2_cor  <- cor.test(df$TIPIemotional_stability,
                      df$COMFappearance, method = "spearman")

hp_3_grp <- median_split_test(df$TIPIemotional_stability, df$COMFharm)
hp_3_cor  <- cor.test(df$TIPIemotional_stability,
                      df$COMFharm, method = "spearman")

hp_4_grp <- median_split_test(df$TIPIemotional_stability, df$COMFanxiety)
hp_4_cor  <- cor.test(df$TIPIemotional_stability,
                      df$COMFanxiety, method = "spearman")

hp_5_grp <- median_split_test(df$TIPIopenness_to_exp, df$bciFuture)
hp_5_cor  <- cor.test(df$TIPIopenness_to_exp,
                      df$bciFuture, method = "spearman")

hp_6_grp <- median_split_test(df$TIPIopenness_to_exp, df$COMFappearance)
hp_6_cor  <- cor.test(df$TIPIopenness_to_exp,
                      df$COMFappearance, method = "spearman")

hp_7_grp <- median_split_test(df$TIPIopenness_to_exp, df$COMFanxiety)
hp_7_cor  <- cor.test(df$TIPIopenness_to_exp,
                      df$COMFanxiety, method = "spearman")

hp_8_grp  <- median_split_test(df$TIPIextraversion, df$COMFappearance)
hp_8_cor  <- cor.test(df$TIPIextraversion,
                      df$COMFappearance, method = "spearman")

# create a table
hp_names  <- c("$HP_1$", "$HP_2$", "$HP_3$", "$HP_4$",
               "$HP_5$", "$HP_6$", "$HP_7$", "$HP_8$")
hp_rho_vals  <- c()
hp_cor_p_vals  <- c()
hp_grp_stats <- c()
hp_grp_p_vals <- c()

for (test in list(hp_1_cor, hp_2_cor, hp_3_cor, hp_4_cor,
                  hp_5_cor, hp_6_cor, hp_7_cor, hp_8_cor)) {
  hp_rho_vals  <- c(hp_rho_vals, round(test$estimate, digits = 3))
  hp_cor_p_vals  <- c(hp_cor_p_vals, round(test$p.value, digits = 3))
}

for (test in list(hp_1_grp, hp_2_grp, hp_3_grp, hp_4_grp,
```

```
                  hp_5_grp, hp_6_grp, hp_7_grp, hp_8_grp)) {
  hp_grp_stats  <- c(hp_grp_stats, round(test$statistic, digits = 3))
  hp_grp_p_vals  <- c(hp_grp_p_vals, round(test$p.value, digits = 3))
}

tipi_hypoth_tests <- tibble(hp_names, hp_rho_vals, hp_cor_p_vals,
                            hp_grp_stats, hp_grp_p_vals) %>%
  rename(Test = hp_names,
         `Spearman $\\rho$` = hp_rho_vals,
         `Spearman $p$-value` = hp_cor_p_vals,
         `Wilcoxon $W$` = hp_grp_stats,
         `Wilcoxon $p$-value` = hp_grp_p_vals)
print(xtable(tipi_hypoth_tests,
             label = "tipi_hypoth_tests",
             caption = c("Results and $p$-values of Spearman correlation tests
             and Wilcoxon rank sum test for the TIPI hypotheses. Wilcoxon tests
             were conducting by performing a median split on the data based on
             the relevant SeBIS dimension and testing for a difference between
             the two groups on the other variable.",
             "Results and $p$-values of Spearman correlation tests
             and Wilcoxon rank sum test for the TIPI hypotheses.")),
      sanitize.colnames.function = identity,
      sanitize.text.function = identity,
      file = "tables/tipi_hypoth_tests.tex",
      include.rownames = FALSE)
print(tipi_hypoth_tests)


# scatterplots
agreeableness_anxiety_scatter <- scatterplot(df, df$TIPIagreeableness, df$COMFanxiety,
                                             plot_title = expression(paste("HP"[1])),
                                             xlab = "TIPI: Agreeableness",
                                             ylab = "Comfort: Anxiety",
                                             model = hp_1)
ggsave(plot = agreeableness_anxiety_scatter,
       filename = "figures/hp1_scatter_agreeableness_anxiety.pdf",
       width = plot_width, height = plot_height, units = "cm")

emotstabil_appearance_scatter <- scatterplot(df,
                                             df$TIPIemotional_stability,
                                             df$COMFappearance,
                                             plot_title = expression(paste("HP"[2])),
                                             xlab = "TIPI: Emotional Stability",
                                             ylab = "Comfort: Appearance",
                                           model = hp_2)
ggsave(plot = emotstabil_appearance_scatter,
       filename = "figures/hp2_scatter_emotstabil_appearance.pdf",
       width = plot_width, height = plot_height, units = "cm")

emotstabil_harm_scatter <- scatterplot(df, df$TIPIemotional_stability, df$COMFharm,
                                       plot_title = expression(paste("HP"[3])),
                                       xlab = "TIPI: Emotional Stability",
                                       ylab = "Comfort: Harm",
                                       model = hp_3)
ggsave(plot = emotstabil_harm_scatter,
       filename = "figures/hp3_scatter_emotstabil_harm.pdf",
       width = plot_width, height = plot_height, units = "cm")

emotstabil_anxiety_scatter  <- scatterplot(df,
                                           df$TIPIemotional_stability,
                                           df$COMFanxiety,
                                           plot_title = expression(paste("HP"[4])),
                                           xlab = "TIPI: Emotional Stability",
                                           ylab = "Comfort: Anxiety",
                                           model = hp_4)
ggsave(plot = emotstabil_anxiety_scatter,
       filename = "figures/hp4_scatter_emotstabil_anxiety.pdf",
```

```
606         width = plot_width, height = plot_height, units = "cm")
607
608   openness_bcifuture_scatter <- scatterplot(df, df$TIPIopenness_to_exp, df$bciFuture,
609                                             plot_title = expression(paste("HP"[5])),
610                                             xlab = "TIPI: Openness to Experience",
611                                             ylab = "BIS: Future",
612                                             ylim = 5,
613                                             model = hp_5)
614   ggsave(plot = openness_bcifuture_scatter,
615         filename = "figures/hp5_scatter_openness_bcifuture.pdf",
616         width = plot_width, height = plot_height, units = "cm")
617
618   openness_appearance_scatter <- scatterplot(df,
619                                              df$TIPIopenness_to_exp,
620                                              df$COMFappearance,
621                                              plot_title = expression(paste("HP"[6])),
622                                              xlab = "TIPI: Openness to Experience",
623                                              ylab = "Comfort: Appearance",
624                                              model = hp_6)
625   ggsave(plot = openness_appearance_scatter,
626         filename = "figures/hp6_scatter_openness_appearance.pdf",
627         width = plot_width, height = plot_height, units = "cm")
628
629   openness_anxiety_scatter <- scatterplot(df, df$TIPIopenness_to_exp, df$COMFanxiety,
630                                           plot_title = expression(paste("HP"[7])),
631                                           xlab = "TIPI: Openness to Experience",
632                                           ylab = "Comfort: Anxiety",
633                                           model = hp_7)
634   ggsave(plot = openness_anxiety_scatter,
635         filename = "figures/hp7_scatter_openness_anxiety.pdf",
636         width = plot_width, height = plot_height, units = "cm")
637
638   extraversion_appearance_scatter <- scatterplot(df, df$TIPIextraversion,
639                                                  df$COMFappearance,
640                                                  plot_title = expression(paste("HP"[8])),
641                                                  xlab = "TIPI: Extraversion",
642                                                  ylab = "Comfort: Appearance",
643                                                  model = hs_8)
644   ggsave(plot = extraversion_appearance_scatter,
645         filename = "figures/hp8_scatter_extraversion_appearance.pdf",
646         width = plot_width, height = plot_height, units = "cm")
647
648   hp_scatterplots1 <- grid.arrange(agreeableness_anxiety_scatter,
649                                    emotstabil_appearance_scatter,
650                                    emotstabil_harm_scatter,
651                                    emotstabil_anxiety_scatter,
652                                    ncol = 2)
653
654   hp_scatterplots2 <- grid.arrange(openness_bcifuture_scatter,
655                                    openness_appearance_scatter,
656                                    openness_anxiety_scatter,
657                                    extraversion_appearance_scatter,
658                                    ncol = 2)
659
660   ggsave(hp_scatterplots1, file = "figures/hp_scatter_merged1.png",
661         width = 18, height = 18, units = "cm")
662   # embed_fonts("figures/hp_scatter_merged1.pdf")
663   ggsave(hp_scatterplots2, file = "figures/hp_scatter_merged2.png",
664         width = 18, height = 18, units = "cm")
665
666   # embed_fonts("figures/hp_scatter_merged2.pdf")
```