Privacy and security issues in Brain Computer Interface

Kaushik Sundararajan

A thesis submitted to the graduate faculty of Design and Creative Technologies
Auckland University of Technology
in partial fulfilment of the
requirements for the degree of
Master of Information Security and Digital Forensics

School of Engineering, Computer and Mathematical Sciences

Auckland, New Zealand
2017

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

Kaushik S

Kaushik Sundararajan

Acknowledgements

I would like to thank Auckland University of Technology for the opportunity to utilize my knowledge and hone my skills. I am in debt to my parents for giving me the chance to study in this esteemed university. They have been through many struggles to get me to this university and I will always be thankful for that.

A special thanks to my supervisor Dr. Brain Cusack who has been the best supervisor I could have ever asked for. His guidance has been invaluable to get my thesis completed successfully. I am grateful to him for sharing his experiences. I am very fortunate to have had the opportunity to learn a great deal.

I would like to thank Mr. Bryce Coad, my second mentor for the thesis. His support for my studies and the advice on the choices for the hardware and software is greatly appreciated.

I also want to thank Dr. Alastair Nisbet to have accepted me in to this exciting course of MISDF.

Finally, I would like to thank my friends Suraj and Shardul for having motivated me whenever I hit a dead end.

Abstract

Technologies that utilize the human brain energies for control have expanded in number and ease of use. A greater number of Brain-Computer Interfaces (BCIs) are being used in restorative and nonmedical fields, including advertising, gaming and media outlets. BCI-empowered innovation has an incredible potential to enhance and improve the quality of human lives. The BCI examined for this thesis is the Emotiv Insight, a 5 channel EEG headset used for monitoring brain activity and to control external devices such as, electronic wheelchairs and robotic arms. The functionality of BCIs is increasing in terms of treating motor disabilities, and enhancing abilities of users by extending their range of communication.

The current problem is the consideration of security and privacy of the information being transmitted by the BCI technologies. The checks for the security and privacy in the use of the headsets and the devices, and the pairing connection, are not a high priority when utility is the design objective. This research study analyzed the various possibilities to capture information transmitted from the BCI and tested the feasibility for attacks, and vulnerability identification. The threats described in the study create an awareness of the implications for improved BCI security designs and for greater care in the production of the headsets so that privacy issues may be addressed. Systematic testing of the BCI technologies for security and privacy vulnerability is required before use. The research question pursued in this research is "**What are the security and privacy vulnerabilities for information in the use of Brain Computer Interface devices**?".

The developers of the hardware and the applications need to shift their focus from creating device longevity and portability, and consider the broader risks that include malicious intervention and service disruption. The successful attacks described in this research can be mitigated if manufacturers accept the performance costs associated with implementing the BLE 4.2 security standard in preference for the cheaper and more efficient BLE 4.0 standard that is generally used in the headsets. A comprehensive framework is required for developers to follow for better risk management and end-user protection.

The research findings showed that with readily available basic hardware tools, information can be captured, read and manipulated. In addition, various types of attacks can be performed on the identified vulnerabilities and the intended purpose of the technology disrupted, changed, and corrupted. The implications of these findings are important for the users and their safety. The different types of attacks achieved in the laboratory included the following:

- Passive eavesdropping: Listening to information transferred to the smartphone application from Emotiv Insight without the user's knowledge.
- Active interception: Interception of active information sent from the application to the headset. The intercepted data could be dropped or chosen to forward to the headset.
- Denial of service: The connection of the Emotiv Insight to the smartphone application could be jammed by advertising bogus data packets.
- Data modification attack: The intercepted data could be modified to a different data and forwarded to the Emotiv Insight to perform a different task.

The importance of this thesis is to highlight the impact of the attacks and the level of damage that can be caused. It also points towards harm that may be caused to users dependent upon this technology for their daily life functionality. EEG headsets such as the Emotiv Insight are becoming increasing popular in terms of usability and functionality, and are easy to purchase. The EEG headsets have been used for medical applications, gameplay, learning, and in a wide variety of control situations. This research emphasizes the vulnerabilities in the devices that may be exploited and cause potential harm to users. The designers, developers, and manufacturers of these devices need to pay greater attention to protecting the confidentiality and integrity of information critical to the intended functionality.

Table of Contents

Table of Figures

List of Tables

Chapter 1
INTRODUCTION

1.0 INTRODUCTION

The purpose of the experimental work in this thesis is to perform security testing for vulnerabilities and the potential identification of exploitations. The focus is on security issues for information exchanged between a consumer grade Brain Computer Interface (BCI) and the application installed on a smartphone. The experiment work is designed to capture all data transmitted by the BCI using two Bluetooth sniffers namely the Adafruit BLE sniffer and the Ubertooth-one. Furthermore, a Man In The Middle (MITM) framework will be used to test the feasibility of different types of attacks such as eavesdropping, Denial of Service (DoS) and a data modification attack. The importance of the research is disclosure of possible security flaws in the use of a BCI.

This introduction chapter aims to introduce the research and to summarize the findings and their implications. Section 1.1 provides a description of the motivation behind the research. Section 1.2 describes the research approach and findings generated from the experiments. Finally, section 1.3 outlines the structure for the thesis.

1.1 MOTIVATION FOR RESEARCH

The field of medical technology has benefited from technologies to overcome human disabilities. Human communication to machines has proven to be valuable and beneficial for many of people suffering from neurological disorders. These disorders include severe motor disabilities such as Amyotrophic Lateral Sclerosis (ALS), spinal cord strokes, locked-in syndrome wherein an individual is cognitively alive but does not possess any muscular function. The BCI technology enables an individual to control external devices through brain signals instead of a muscular action. BCIs enable the communication of brain signals or neural signals to be translated to digital signals directed towards the external device. In my critical reflection, I asked: How secure are these devices and what protection of information is there for a user?

Initially, BCIs were only invasive which meant that the individual had to undergo a surgery to connect the electrodes to the scalp. But modern technology has given rise to non-invasive BCIs which resemble a headphone. These types of BCIs do not require surgery and contain dry electrodes that capture the electrophysiological activity when placed on the head of an individual. The BCI used for this research is the Emotiv Insight designed by Emotiv. This BCI is a 5 channel brainware which measures critical regions of the brain, and primarily the frontal lobe and the parietal lobe. These lobes or divisions contribute to important functions in the brain. The frontal lobe is responsible for thought generation and intellectual capabilities whereas the parietal lobe deals with the emotions and decision-making capabilities. These signals captured by the BCI are sent to an application installed on a smartphone. There are also applications designed for desktop and laptop computers with extended functionality.

The BCI technology has resulted in a better quality of life for individuals with neuromuscular disabilities. Individuals can communicate and control external appliances such as a wheelchair or a robotic arm by just thinking. In addition, this technology has also aided people with speaking disabilities to directly control spelling software installed on a computer to translate their thoughts into words. The future of BCI technology will assist these individuals and others with challenges for more satisfying communication and movement. However, today these BCI applications are still in developmental stages and the focus is still on information access, rather than secure communications. They have limited security associated with the data sent to the application on the smartphone. Also these applications are at risk as there are no set standards or guarantees for security and privacy for information being sent and received. This research investigates the security and privacy vulnerabilities in the use of BCIs.

A falsifiability statement is proposed as an assertion for testing. The research question is selected to guide the research and to obtain the answers. Furthermore, one hypothesis and four sub questions have been defined in order to answer the research question and provide a greater resolution of issues in the context of this research.

Falsifiability statement: *That the data transmitted from a consumer grade Brain Computer Interface to the end user cannot be captured, and the transfer of data is secure and encrypted.*

Thus, the research question proposed is:

Research Question: *What are the security and privacy vulnerabilities for information in the use of Brain Computer Interface devices?*

The research goal of this thesis is to determine the security and privacy vulnerabilities for information transfer between the BCI and the application. To answer the research question, four sub questions have been defined.

Sub Question 1: *What data can be captured from a communication session between the BCI and the user interface?*
Sub Question 2: *How can the pairing authentication information be interpreted?*
Sub Question 3: *How can the pairing between the BCI and the smartphone application be jammed?*
Sub Question 4: *How can captured information be substituted for a manipulated information exchange?*

This research aims to provide a practical demonstration of the possibilities for capturing encrypted information transmitted from the Emotiv Insight.

1.2 RESEARCH APPROACH AND FINDINGS

The research approach for this thesis was decided through a search of peer reviewed literature and publications thereby compiling a review of information with relevance to the research topic. The literature analysis identified the clinical and social applications of Brain Computer Interface (BCIs). Furthermore, the security and privacy issues in the use of BCIs were identified. The issues highlighted in the literature review lead to the designing of the research methodology and the research question. The research methodology was formed by analyzing similar research studies pertaining to BCIs. Five studies were identified similar to this research, analyzed for how the researchers went about doing the research, and then a research methodology was proposed based on guidance from the similar studies.

The methodology proceeds in phases. The Emotiv Insight must be prepared which starts with the recording of a baseline. The primary setup included the account of the cerebrum signals with no thoughts. After the benchmarking of the standard, the push charge was prepared. This included intuition to push a cube in a recreated domain introduced by the application installed on the cell phone. The principal cycles contained an arrangement of ten tests, and recorded by utilizing the Adafruit BLE sniffer. In this way, another arrangement of ten test records were determined utilizing the Ubertooth-one sniffer. Each document was captured in a .pcap file and later examined in Wireshark. These test records were additionally analyzed utilizing CrackLE, an application intended to unscramble any protected data contained inside the caught documents. Of the twenty test documents, sixteen records were decoded and disclosed the Long Term Key retrieved by CrackLE. The Long Term Key is an encryption key traded by both the gadgets, the cell phone and the Emotiv Insight. This security key secures the communication including a wide range of information exchanged between the Emotiv Insight and the application.

The results obtained were analyzed to answer the research question and test the hypotheses. The hypothesis:

That the data transmitted from a consumer grade Brain Computer Interface to the end user cannot be captured; failed because the information could be captured and modified as well.

Research Question: *What are the security and privacy vulnerabilities for information in the use of Brain Computer Interface devices;* was answered by demonstrating the following vulnerabilities:

- Passive Eavesdropping – The information was captured passively and recorded to a .pcap file. The information included advertising data, mac addresses of the Emotiv Insight and the smartphone, the encryption key, the data exchanged between the two devices and the connection request.
- Active Interception – The data transmitted from the smartphone was actively intercepted. All data intended to be forwarded to the Emotiv Insight could be intercepted and could also be dropped causing the Emotiv Insight to malfunction.
- Denial of Service: The Ubertooth-one sniffer was used to cause a Radiofrequency jamming by broadcasting dummy data and prevented the Emotiv Insight to connect to the smartphone.
- Replay attack: The data which was actively intercepted could replayed back to the Emotiv Insight and could also be looped to perform the same action repeatedly.
- Data Modification: The intercepted could also be modified to a different information requirement, and then be forwarded to the Emotiv Insight. A specific command such as a push command could be changed to a completely different command causing the Emotiv Insight to perform a different function than what it is expected to do.

The Sub Question 1: *What data can be captured from a communication session between the BCI and the user interface?; was answered by:*

> The advertising data broadcasted by the Emotiv Insight, the connection request initiated by the smartphone, the encryption key, the data beginning from the physical layer to the L2CAP layer, the Attribute layer and finally the application layer data.

The Sub Question 2: *How can the pairing authentication information be interpreted?;* was answered by:

> The pairing information could be captured using the Ubertooth-one. The pairing information contains several parameters which could be decrypted using the CrackLE software. The Short-term key and the Long Term Key could be derived using the CrackLE interface.

The Sub Question 3: *How can the pairing between the BCI and the smartphone application be jammed?;* was answered by:

> The pairing between the BCI and the smartphone could be jammed using the Ubertooth-one. The Ubertooth-one acts as a dummy device and broadcasts several packets with a different mac address and interferes in the pairing between the BCI and smartphone application.

The Sub Question 4: *How can captured information be substituted for a manipulated information exchange?;* was answered by:

> The captured information could be substituted by manipulated information using the Btlejuice Man In The Middle (MITM) framework. The framework can capture the application layer data and additionally facilitated the modification of the captured information, and then forward the modified information to the Emotiv Insight.

The findings of the data captured using the Bluetooth sniffers demonstrates the simplicity of the attack. Furthermore, it provides a gateway to much more sophisticated attacks. The security flaws in a consumer grade BCI such as Emotiv Insight opens opportunities to expose the potential security and privacy issues. The application layer data could be captured in a raw format using the Btlejuice framework. There is a need to evaluate these security flaws so that they can be mitigated to ensure a safe and secure environment for the individuals using this technology. The research has provided an overall analysis of the potential vulnerabilities in the use of BCI technology. Furthermore, as the underlying issues with the use of the technology is Bluetooth Low Energy in wireless then not only Emotiv Insight is valuable but also insulin pumps, smart locks, motor vehicle apps, and so on. All these technologies lead to the Internet of Things (IoT) which will form the epicenter of human requirements in the near future. Thus, it is a recommendation for future research that all these devices need to be upgraded to Bluetooth 4.2 and tested. It has advanced technology using the Diffie Hellman Elliptical Cryptography (ECDH) algorithm. The cryptographic technology makes the device more secure and less prone to attack. Eventually, individuals depending on such technologies could have less risks and get better protection from the attacks demonstrated in this thesis. However, the issue of computational costs will also have to be overcome.

1.3 THESIS STRUCTURE

The thesis starts with the literature review in Chapter 2. Chapter 2 introduces the structure of the human brain and the functional areas of the brain. In addition, Section 2.1 gives the mapping of the essential areas of the brain that have relevance in terms of the BCI. Section 2.2 describes the Brain Computer Interface (BCI) technology developments, the hardware and software components associated with a BCI. Sections 2.3 discusses the social and clinical applications of BCIs and also summarize the challenges and disadvantages connected to the use of a BCI. Section 2.4 highlights the potential security and privacy issues in the use of BCIs and Section 2.5 summarizing the issues and the problems in the use of BCIs. Section 2.6 concludes the literature review.

After reviewing various journals and peer reviewed literature, five papers with a similar interest were chosen to guide the construction of the research methodology for this thesis. Section 3.1 presents the review of the five similar studies. Section 3.2 describes the research design and section 3.3 presents the data requirements including data generation, data collection, data processing and analysis. Section 3.4 discusses the limitations in terms of reliability and validity and finally Section 3.5 concludes Chapter 3. After specifying the methodology, the experiments were carried out as per the research design and the results were obtained. Section 4.2 describes the hardware set up for the experiment and Section 4.3 defines an experimental design to be followed in order to obtain the results. Section 4.4 presents the results and the analysis is discussed in Section 4.5. Section 4.6 concludes the research findings.

The results obtained in Chapter 4 were then analyzed to test the hypothesis and answer the research question and sub questions. Section 5.1 tests the hypothesis for falsifiability with Sections 5.2 and 5.3 answering the research question and sub questions. Section 5.4 presents the discussion for this thesis and Section 5.5 concludes the chapter. The thesis is concluded in Chapter 6 by discussing the limitations and directions for further research. The final reflection in the thesis is my personal journey and critical reflection on the learning gained in this thesis.

Chapter 2
LITERATURE REVIEW

2.0 INTRODUCTION

The literature was selected through keyword searches from the Auckland University of Technology, elibrary portal. In addition, google scholar was used in finding other information pertaining to the brain-computer interface. The initial search phrases were to understand the topic from a broader perspective and the set of keyword searches included Brain-computer interface, BCI's implementation, and BCI application. The search terms were then narrowed to specific phrases such as 'Privacy issues in Brain-computer interfaces', 'neural signals 'and 'translation algorithm in BCI's'.

The brain has always been an organ of interest for research. The brain is an unfolding mystery and the understanding of brain activity useful for utilization in applications. The advancement of technology and brain-computer interfaces have aided people with motor disabilities (Schalk, McFarland, Hinterberger, Birbaumer, & Wolpaw, 2004) . The activity of the brain can be recorded non-invasively, as shown by the pioneering efforts of Hans Berger. He established that there was a specific rhythm at 10Hz noticeable on the posterior scalp. This specific rhythm came to be known as alpha rhythm. These observations lead to the evolution of Electroencephalography (EEG) which could use these rhythms and access the gross state of the brain (Wolpaw, Birbaumer, McFarland, Pfurtscheller, & Vaughan, 2002). The concept of brain-computer interface technology became a reality in the 1950's. The exploration of brain-computer interface began in the Defense Advanced Research Projects Agency (DARPA) in during the 1970s (Miranda et al. 2015). After this period, many innovations have been made for brain-computer interface technology. The recent brainwear designs have replaced the use of electrodes with sensor technology.

Chapter 2 is structured to review the relevant literature on brainware. Section 2.1 reviews the human brain, different lobes of the brain, neural activity and the electroencephalogram reading interpretations. The sub sections for this section includes the overview of the human brain, the significance of EEG to understand the brain activity and interpret the results from the EEG. Section 2.2 analyses the brainwear device 'Emotiv Insight' used for this study. The sub sections describe the working of the device and the reports that can be extracted from the application interface. Various aspects from a consumer and prosumer perspective has been investigated for the Emotiv. The advantages and the disadvantages of the device are also discussed. Section 2.2 concludes with the explanation and analysis of the brainware BCI2000 environment and Emotiv Insight. Section 2.3 describes the social applications of brainwear, the Emotiv Insight application, and its application for gaming purposes. Various parameters such as the stress level, the excitement level, the interest level and three others are also described in this section. The use of Emotiv Insight in the medical industry is also outlined. The final section sums up with potential issues for using the device. Finally, section 2.4 evaluates potential security and privacy issues followed by section 2.5 summarizing the issues of the Emotiv Insight and 2.6 concludes the review.

2.1 HUMAN BRAIN

Section 2.1 provides an overview of the brain anatomy with the critical areas and the functions associated. After reviewing the brain, the next sections will define the Electroencephalogram and the relation with the human brain. Section 2.1.1 analyses the various anatomical features of the human brain. It also includes the various lobes of the human brain and the sections of the human brain. Section 2.1.2 explores the concepts of electroencephalography, the various activities that the electroencephalogram measures, and section 2.1.3 concludes with the relationship between the human brain mapping activity and the electroencephalography.

2.1.1 Human Brain – The Anatomy

The most complex part of the human body is the brain. There are various sections or anatomical classes for the human brain, and the sectional anatomy for the brain. The sectioning anatomy of the brain is into three orthogonal planes for structuring investigation into the internal structures of the brain (Forstmann & Wagenmakers, 2015). Figure 2.1 is a representation of the structure of the human brain. The human brain majorly comprises of the ventricular system with the cerebrospinal fluid (CSF) flowing throughout the different regions of the ventricular system (Forstmann & Wagenmakers, 2015). The brain can be divided into three major sections chiefly: the forebrain, the mid brain and the hind brain (Rains, 2001).

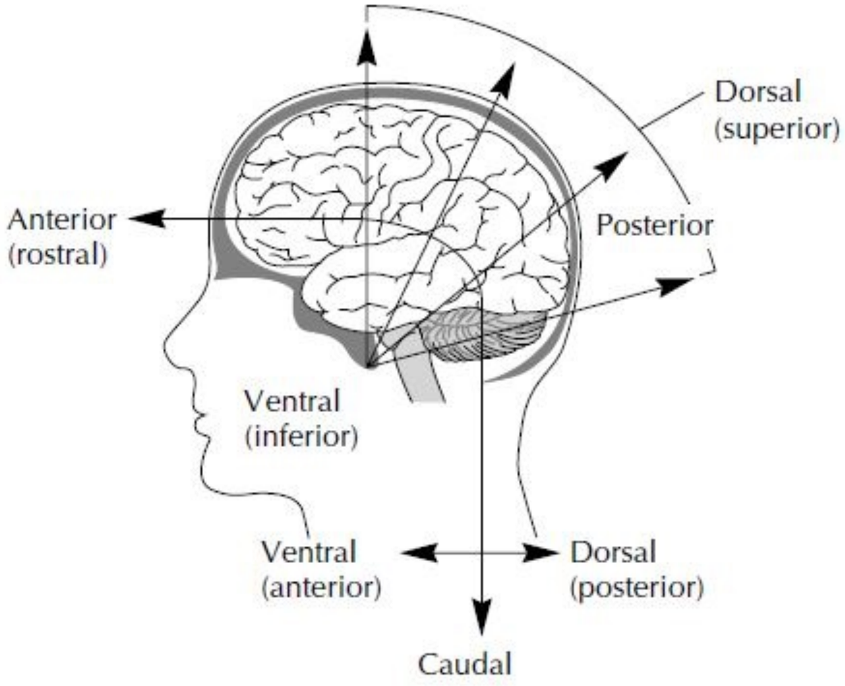


Figure 2.1. Structure of the human brain (Rains, 2001, p. 46)

From figure 2.1, the brain structure can be divided into distinct locations namely:

- Anterior or rostral
- Dorsal or superior
- Ventral or inferior
- Caudal
- Posterior

The central nervous system comprises of the brain and the spinal cord. The different divisions of the brain structure have been presented in Table 2.1. The table is divided into three divisions:

- Primitive brain divisions
- Mammalian brain divisions
- Regions of the human brain

The primitive brain divisions are divided into the forebrain, midbrain and the Hindbrain. The corresponding mammalian brain division to the forebrain include Telencephalon and Diencephalon. The division corresponding to hind brain is Mesencephalon. Finally, the mammalian division with respect to the hind brain comprise of Metencephalon and

Myelencephalon (Rains, 2001). The last column explains various regions of the human brain in terms of the forebrain, midbrain and hindbrain.

Table 2.1: Summary of the different sections of the brain from (Rains, 2001, p. 49)

Primitive Brain Divisions	Mammalian Brain division	Regions of the Human brain
Forebrain	Telencephalon Diencephalon	Neocortex, Basal Ganglia, Lateral ventricles, Limbic system Thalamus, Hypothalamus, Pineal Gland, Third ventricle
Midbrain	Mesencephalon	Tectum, Tegmentum, Aqueduct of Sylvius
Hindbrain	Metencephalon Myencephalon	Pons, Cerebellum and fourth ventricle Medulla Oblongata, fourth ventricle

In this case, the different regions in the forebrain include neocortex, basal ganglia, lateral ventricles, limbic system, thalamus, hypothalamus, pineal gland and the third ventricle. The regions of the midbrain include the tectum, tegmentum and aqueduct of Sylvius. The hindbrain has regions such as Pons, cerebellum, fourth ventricle, medulla oblongata and the fourth ventricle.

The forebrain contributes the higher cognitive functions, out of which the most significant one is the cerebral cortex. The cerebral cortex forms the outer covering of the cerebral hemispheres. More than 70% of the neurons of the central nervous system is known to be present in the cerebral cortex. In addition to the above divisions, the brain encompasses four different lobes chiefly:

- Frontal Lobe
- Parietal Lobe
- Temporal Lobe
- Occipital Lobe

Figure 2.2 shows the position of the various lobes in the human brain. The frontal lobe is mainly responsible for intelligence being a part of the cerebral cortex. Just behind the frontal lobe, the parietal lobe and temporal lobe are located on either side of the hemispheres. The parietal lobe is responsible for emotions, thoughts and feelings, whereas the temporal lobe is majorly responsible for auditory functions. Finally, the occipital lobe is responsible for vision. In this manner, all these lobes are responsible for critical functioning of the entire human body.

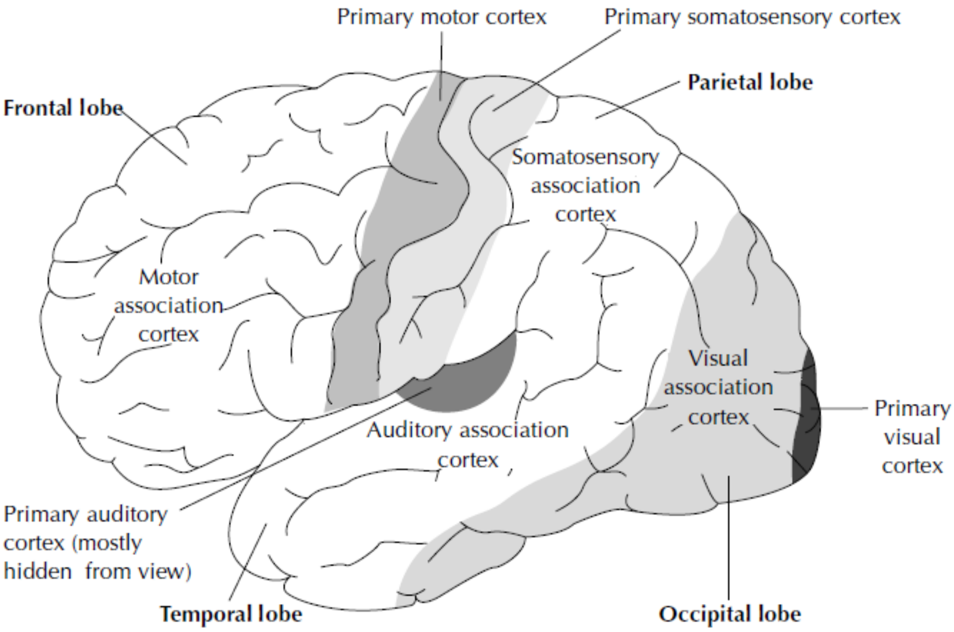

Primary motor cortex
Primary somatosensory cortex
Parietal lobe
Frontal lobe
Somatosensory association cortex
Motor association cortex
Visual association cortex
Primary visual cortex
Auditory association cortex
Primary auditory cortex (mostly hidden from view)
Temporal lobe
Occipital lobe

Figure 2.2. Different lobes of the brain (Rains, 2001, p. 57)

In addition to these lobes, the forebrain comprises other important components, the thalamus, hypothalamus, hippocampus. The midbrain comprises of two major components the tectum acting such as a roof and the tegmentum acting such as a sheath covering (Rains, 2001). Finally, the hindbrain includes pons, medulla oblongata and the cerebellum. The pons is composed of pontine tegmental regions forming the base of the fourth ventricle. The medulla oblongata is one of the important components in the hind brain and is continued as the spinal cord. Finally, the cerebellum is responsible for body movements and balance of the entire body. In conclusion, the entire nervous system is divided into the central and the peripheral nervous system. The central nervous system comprises of the brain and the spinal cord, whereas the peripheral nervous system is the motor and the sensory neurons (Rains, 2001). These definitions of human brain elements are relevant to understanding the functionality of BCI devices in relation to the human.

2.1.2 Electroencephalography [EEG]

Caton (1899) is considered to have pioneered electroencephalographic research (Blinowska & Durka, 2006). His experiments displayed a low amount of varying energy passing through the multiplier with respect to electrode placements. Later, pioneers such as Adolf Beck, and Napoleon Cybulski extended Caton's research. But it was not until 1929, Hans Berger presented the first official electroencephalogram from the surface of the human scalp (Nunez, 1981). Once the different components of the human brain were analyzed, research was undertaken to understand the working of each component. To understand the working of these underlying brain activities in relation to higher cognitive functions, there arose a need for a non-invasive recording method. This gave rise to a new science that came to be known as electroencephalography.

The branch of science that studies the recordings and the interpretation an electroencephalogram is known as electroencephalography (Blinowska & Durka, 2006). The human brain has a constant neuronal communication resulting in a synapse. This synaptic activity creates an electrified field in the brain. The activity of the electrified field can be recorded and analyzed. This recording of the brain activity in real time is known as electroencephalogram. Electroencephalogram generally makes use of electrodes on different functional areas on the human brain. The position of the electrodes on the scalp of the brain classifies EEG into distinct types. Some of the types are listed below:

- ElectroCorticoGram or ECoG is the measurement when the electrodes are placed directly on the scalp.
- Local Fields Potentials or LFP is the measurement of electric fields when the electrodes are placed in an intracortical position.
- When the EEG is generated because of a response to an external or internal stimulus is known as Event Related Potential whereas EEG recorded in the absence of a stimulus it is known as spontaneous EEG (Blinowska & Durka, 2006).

There are different types of brain rhythms distinguished based on frequency. Figure 2.3 presents an illustration of different types of rhythms from an EEG reading.

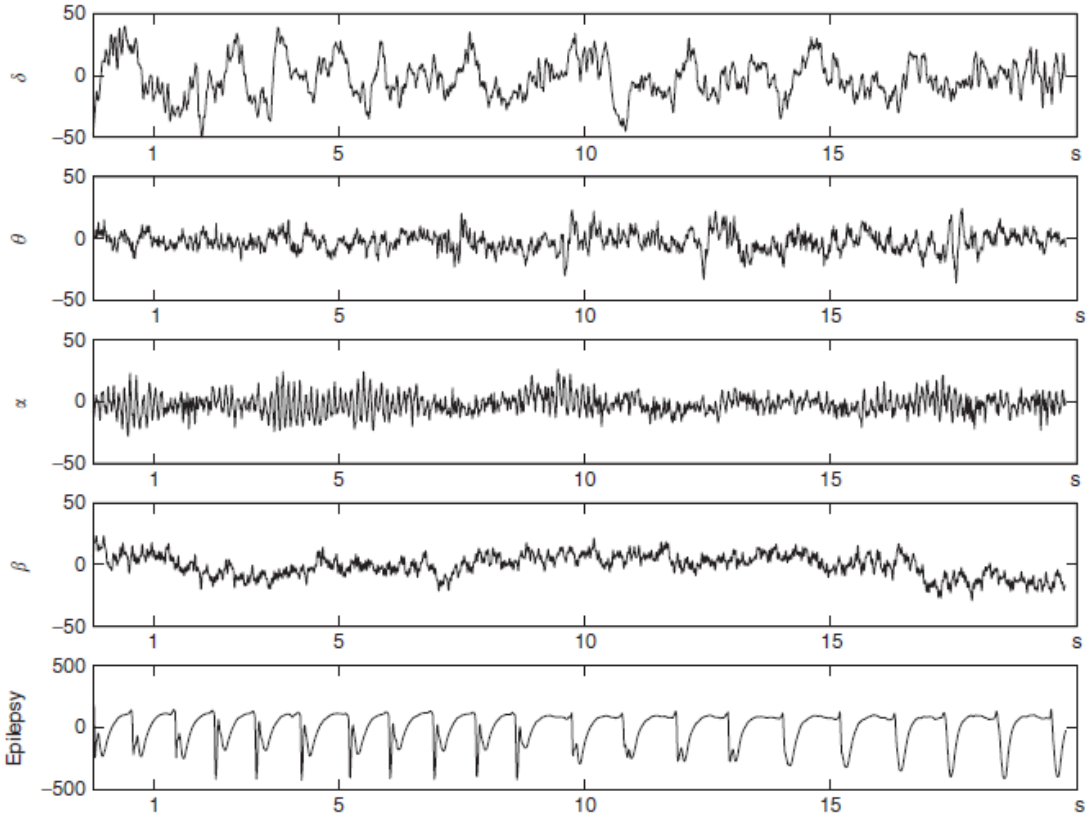


Figure 2.3. EEG rhythms: delta, theta, alpha, beta and gamma rhythms (Blinowska & Durka, 2006)

The four types of rhythms presented in figure 2.3 are:

- Delta rhythm: The frequency usually in delta rhythms ranges from 0.5-4Hz. It is a predominant feature of an EEG during a deep sleep (Blinowska & Durka, 2006).
- Theta rhythm: The frequency is a bit higher starting from 4-12Hz in the theta rhythm. The transfer of information in rodents has been observed in this specific frequency whereas in human beings found only during an emotional or some cognitive state (Da Silva, 1996).
- Alpha rhythm: The most important rhythm pattern observed during an awaken stage of human beings, usually observed at the posterior regions of the head. They are best found when the mental state is relaxed with eyes closed.
- Beta rhythm: This rhythm usually denotes the state of increased alertness. In addition, it also presents a state of concentration and attention.
- Gamma rhythm: This rhythm is associated with the processing of information. It usually involves the recognition of an external stimulus, and it also includes the movement of voluntary muscles.

EEG data presentation has become significant when monitoring the brain activity. With an increase in age, an increase in rhythm frequency is very common in EEG (Blinowska & Durka, 2006). EEG is usually affected by the central nervous system disorders including metabolic and neurodegenerative diseases. EEG plays a significant role in detection of psychiatric diseases and in sleep related disorders. Furthermore, EEG has also been widely employed to pharmacological substances as well. The effect of psychoactive drugs can assist in the assessment of actions in the central nervous system. The simple method of analysing EEG has the signals plotted on a piece of a paper. But with modern advancements in computer technology raw data can be imported into a smartphone for visual presentation (Moore, 2003).

Even though there are modern tests such as Positron Emission Topography (PET) and Magnetic Resonance Imaging (MRI), EEG is still important for the measurement of brain activity. The former tests provide the absorption level of certain substances with respect to the brain structure, and has a time advantage in comparison to EEG (Blinowska & Durka, 2006). EEG has also been used to help patients with neurorehabilitation. The technology is based on brain computer interface (BCI) with robotic feedback (Ang et al. 2010). The next section will discuss the relationship between the human brain and EEG.

2.1.3 Human Brain Mapping and EEG

Through research much knowledge has been gained about the human brain. EEG has played a pivotal role throughout the understanding of various brain functions (Darvas, Pantazis, Kucukaltun-Yildirim, & Leahy, 2004). EEG offers a different perspective when it comes to the human brain. The synaptic communication creates an electrified field arising as a result of communication or exchange of messages between millions of neurons (Salhi, MacLaurin, & Toumi, 2016). EEG reads the electromagnetic signals produced by the human brain. The measurement of EEG signals can be performed from the scalp itself. The usual set up includes the use of electrodes or sensors placed on the scalp of the head. The electrodes or sensors picks up the activity produced by the neurons. The measurement is achieved in combination of high impedance amplifiers and digital data gathering system. This digital system is responsible for acquiring data from the brain activity and translating it into digital data which can be recorded and used for analysis (Darvas et al. 2004). The use of electrodes requires hydration in the form of saline or conductive gel for the electrodes to conduct the activity. The recent ones involve the use of dry electrodes thereby avoiding the need of a rehydration solution (Wyckoff, Sherlin, Ford, & Dalke, 2015).

A great deal has been understood about the brain functionality with the help of mapping the activity with statistical models. These statistical models have been developed with raw EEG data. This raw EEG data has been used to map certain areas of interest in the brain (Scherer, Moitzi, Daly, & Müller-Putz, 2013). Brain mapping has been performed to understand the functionality and physiology of different structures. In addition to EEG, Magnetoencephalography (MEG) has also been widely used to understand the brain structure. MEG measures the brain activity from the magnetic field created by the brain activity (Darvas et al. 2004). Every action that the external part of the human body is performed for example raising an arm, tapping fingers, answering a stressful question. Whenever an action is performed, a specific part of the brain cell is involved. These different tests such as EEG, MEG, MRI, PET and ECoG share a common characteristic for tests that aim to study brain activity through behavioral patterns in the brain.

2.2 BRAIN COMPUTER INTERFACE: BRAINWEAR

Section 2.2 examines the working of brain-computer interface (BCI) and the various brainwear types currently available for public use. The section starts with the introduction the architecture and the implementation of the brain-computer interface. Sub section 2.1.1 describes the notion of control signals and the implementation of these control signals in brain-computer interface. Subsequently section 2.2.2 studies the BCI hardware, the technical specifications and the interface. Section 2.2.3 briefly describes the BCI software, P300, a brain signal that is essential for the understanding the brain activity and its employment in the brainwear technology. Finally, section 2.2.4 explores the various features of the BCI2000 platform and its application in modern day EEG brainwear.

Today, technology has merged computers closer to human beings. Brain Computer Interface or BCI is the environment that bonds the interaction between computers and the human brain. It is an amalgamation of software and hardware platforms. A generic BCI comprises of a hardware that usually would be the device used to record and analyse EEG whereas the software performs the function of translating brain signals/neural signals to digital signals that can be interpreted through a personal computer or a laptop (Ramadan & Vasilakos, 2017). Figure 2.4 shows typical components of the brain computer interface.

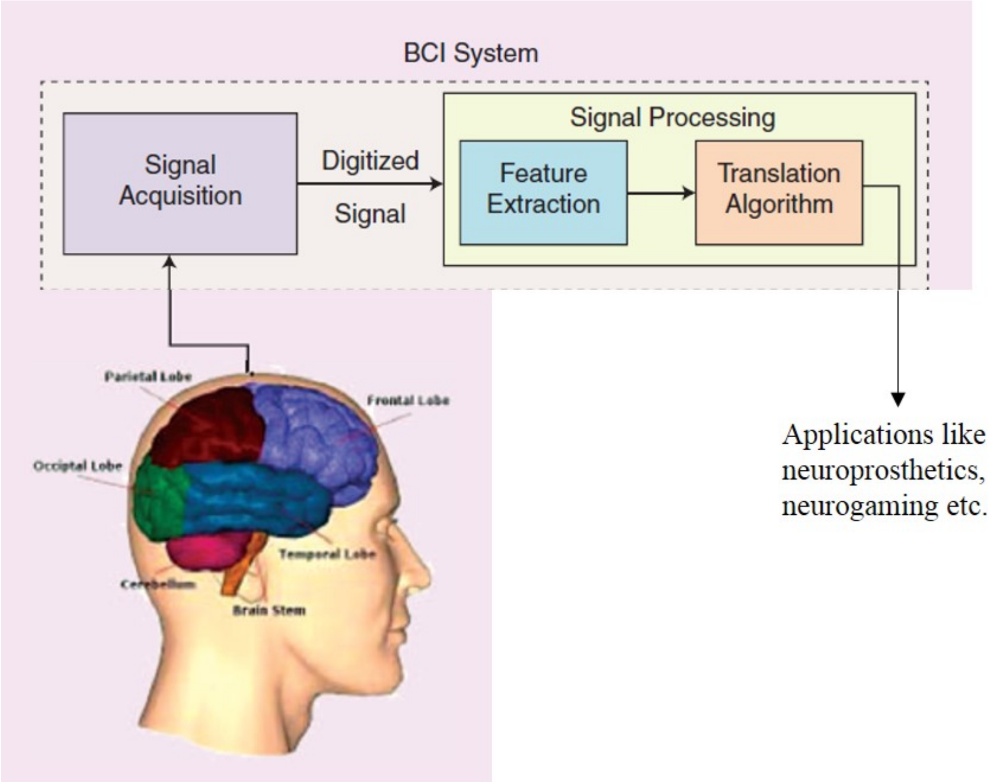


Figure 2.4. Components of a brain-computer interface (Bonaci, Calo, & Chizeck, 2014)

Figure 2.4 shows the architecture and the working behind a generic brain-computer interface. The interface encompasses signal acquisition from the brain activity and digitizing them in the form of digital signals using a signal processing mechanism. Signal processing comprises of signal extraction and a translation algorithm. Initially, the neural signals are digitised and then extracted. This extracted signal and then translated into an algorithm which can then be used to serve various applications such as neuroprosthetics and gaming (Bonaci et al. 2014). Donoghue (2002), suggest that brain machine interfaces have a major goal to utilize the brain signal to enable voluntary movements of prosthetics that control disabled parts in the human body (Pasqualotto, Federici, & Belardinelli, 2012). The number of companies and research groups have greatly increased in the last decade (Ramadan & Vasilakos, 2017). Brain computer interfaces have been classified by three main parameters (Ramadan & Vasilakos, 2017):

- Dependability
- Invasiveness

- Synchronization

BCI have been classified as having dependent and independent interfaces. The dependent brain computer interface requires the interface to be dependent on motor control from the subject whereas on the other hand, the independent brain computer interface does not require any motor control from the subject (Allison, Graimann, & Gräser, 2007). Some of the examples of dependant brain computer interface includes movements of neuro prosthetics such as a wheelchair controlled by the BCI, or playing video games. On the contrary, patients with severe disabilities require an independent brain computer interface without any motor movement (Ramadan & Vasilakos, 2017).

The second parameter for the classification is based on invasiveness. The three classes are invasive brain computer interface, semi-invasive and non-invasive brain computer interface. The classification depends on how measurement of the brain activity is done. As the name suggests invasive brain computer interface, involves microelectrodes being implanted under the skull through surgery. The only drawback with this type of brain computer interface is that, if there is a need to measure other areas of the brain, it is not feasible to move the BCI to other areas (Ramadan & Vasilakos, 2017). Non-invasive brain computer interfaces provide the advantage to move to any part of the scalp. The signals captured using a non-invasive brain computer interface are of lower quality when compared to an invasive brain computer interface. The advantage is that the use of non-invasive brainwear avoids the need for surgery (Millan, Renkens, Mourino, & Gerstner, 2004). Another type of brainwear is the semi-invasive brain computer interface which involves the implanting of electrodes underneath the skull. The brain activity is measured using Electrocorticography (ECoG) (Ramadan & Vasilakos, 2017).

The third classifying basis for brain-computer interface is based on synchronization. The two types are synchronous and asynchronous brain computer interfaces. In the synchronous brain-computer interface, the system must make the patient interact in a specific period. In the asynchronous brain-computer interface, the synchronization is self-paced and offers the liberty for the patient to interact any period of time. Whenever the interaction occurs in asynchronous, the system starts capturing the signals the subject starts to interact with the system (Ramadan & Vasilakos, 2017).

2.2.1 Mental Control Signals

Brain computer interface relies on the control signals which are directly extracted from the brain activity. Some of these control signals can be easily translated into digital signals using translation algorithms whereas some signals need more pre-processing. All these control signals from the brain activity can be categorized into three types. The first type is evoked signals or Visual Evoked Signal which are the signals produced involuntarily as a response to an external stimulus. The most common types of evoked signals include steady state evoked potentials (SSEP) and P300 (Ramadan & Vasilakos, 2017). Steady state potentials are signals captured in response to external stimuli such as a flickering image, mild vibrations or a moderated sound. Based on the sensation process, different areas of the brain can be observed. SSEP and the other type of evoked signal is P300 which is usually observed when the subject is involved in a surprising activity (Ramadan & Vasilakos, 2017).

The second type of control signal is a spontaneous signal which is produced in the absence of external stimulus. It usually involves the use of motor and sensorimotor rhythms. Further classified as slow cortical potentials or SCP and non-motor cognitive tasks (Golub, Chase, Batista, & Byron, 2016). The motor rhythms arise because of voluntary movements whereas slow cortical potentials can be mainly observed in the frontal cortex arising due to depolarization shift. The final type of spontaneous control signals are non-motor cognitive tasks that includes music imagination, visual counting and so on (Ramadan & Vasilakos, 2017).

The third type of control signals is known as hybrid signals, a mix of various signals generated by the brain. The main intention behind the use of hybrid signals is that there is no specific distinction or attention to a specific area. Multiple areas of the brain can be monitored reliably thereby avoiding the disadvantage for each types of signals (Ramadan & Vasilakos, 2017). In this way, all the BCIs have different types of control signal technology to monitor the brain activity.

2.2.2 BCI Hardware

With the improvement in design and with the replacement of electrodes with dry sensors, many companies have developed non-invasive brainwear. Some major companies that manufacture non-invasive brainwear include Emotiv, Neuroware, G-Tec and Neurosky (Bonaci et al. 2014). Emotiv and Neurosky offer low priced EEG headsets in comparison to Neuroware. For the purpose of this thesis, the Emotiv Insight EEG brainwear has been used due to the cost effectiveness and for the software development kit (SDK) provided by Emotiv. Emotiv is a bioinformatics powered with an advanced technology based company who have pioneered the use of EEG headsets in terms of simplicity and mobility (Emotiv, 2016). The motive behind designing these headsets is to offer access to an advanced level of monitoring the brain activity and assessing various cognitive functions.

Figure 2.5 shows an emotiv. The headset contains 5 channels namely AF3, AF4, T7, T8 and Pz. These channels are specific to every channel in this headset. AF3 measures the left frontal activity, AF4 measures the right frontal activity, T7 measures the left temporal activity, T8 measures the right temporal activity and finally Pz measures central parietal activity of the brain. All these channels focus on three lobes of the brain, but primarily the frontal lobe, temporal lobe and the parietal lobe. In addition to the five channels, there are two references as well, known as the Left Mastoid Process (Emotiv, 2016). These references provides a baseline to compare the readings of the brain activity at different times.

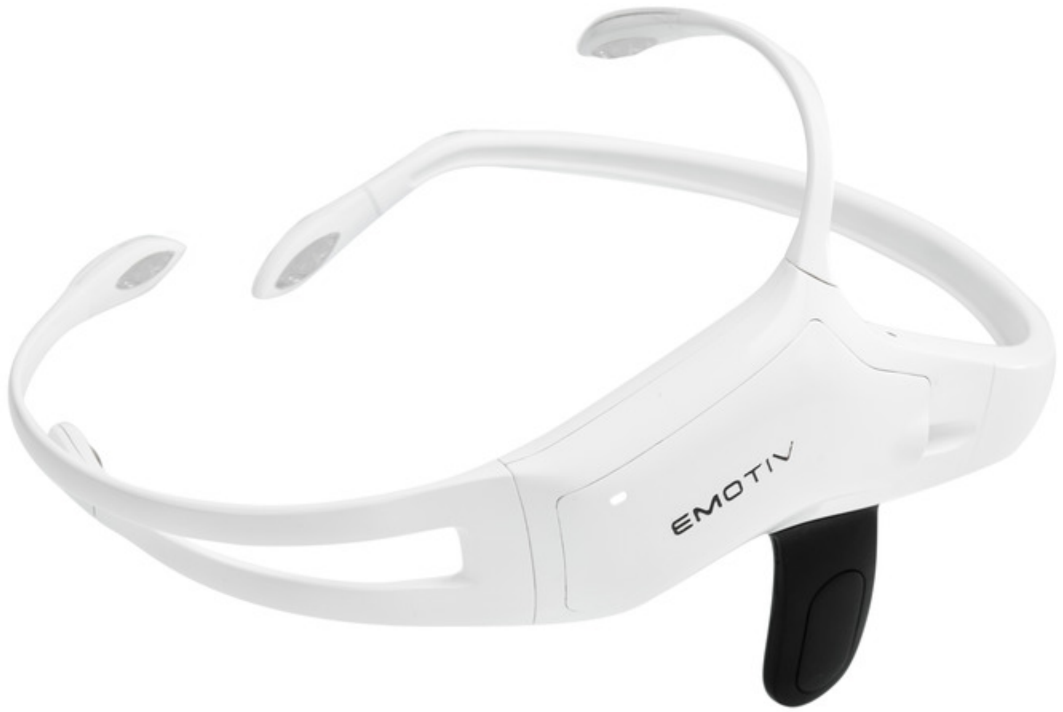


Figure 2.5. Emotiv Insight 5 channel EEG headset (Emotiv, 2016)

The Emotiv Insight is designed to detect performance levels of certain parameters that include the attention level, focus level, engagement level, interest level, relaxation level and stress level. In addition to detecting performance, it also detects mental commands and facial expressions. These expressions include blink, wink, frown surprise, clench and smile. All these parameters are recorded using a computer based interface called Emotiv Xavier Control Panel. The control panel comprises of enumerous features. These include signal quality of the brainwear, mental commands, facial expressions and the inertial sensors. In addition to these features, the control panel also provides connectivity to other platforms of Emotiv namely, Emotiv Xavier composer and Emotiv Emokey. Figure 2.6 shows the signal quality of the headset in the Xavier control panel. When all the five channels are green to denote the signal quality is good. The results are determined by the signal quality. After checking for signal quality, the interface requires a login.

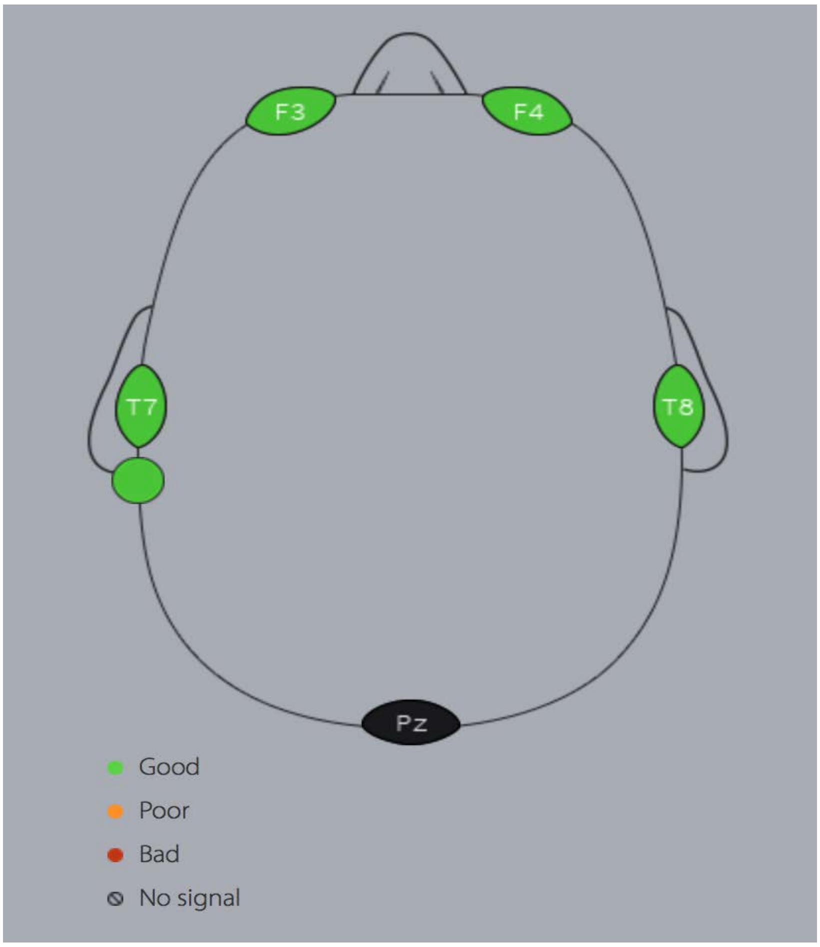
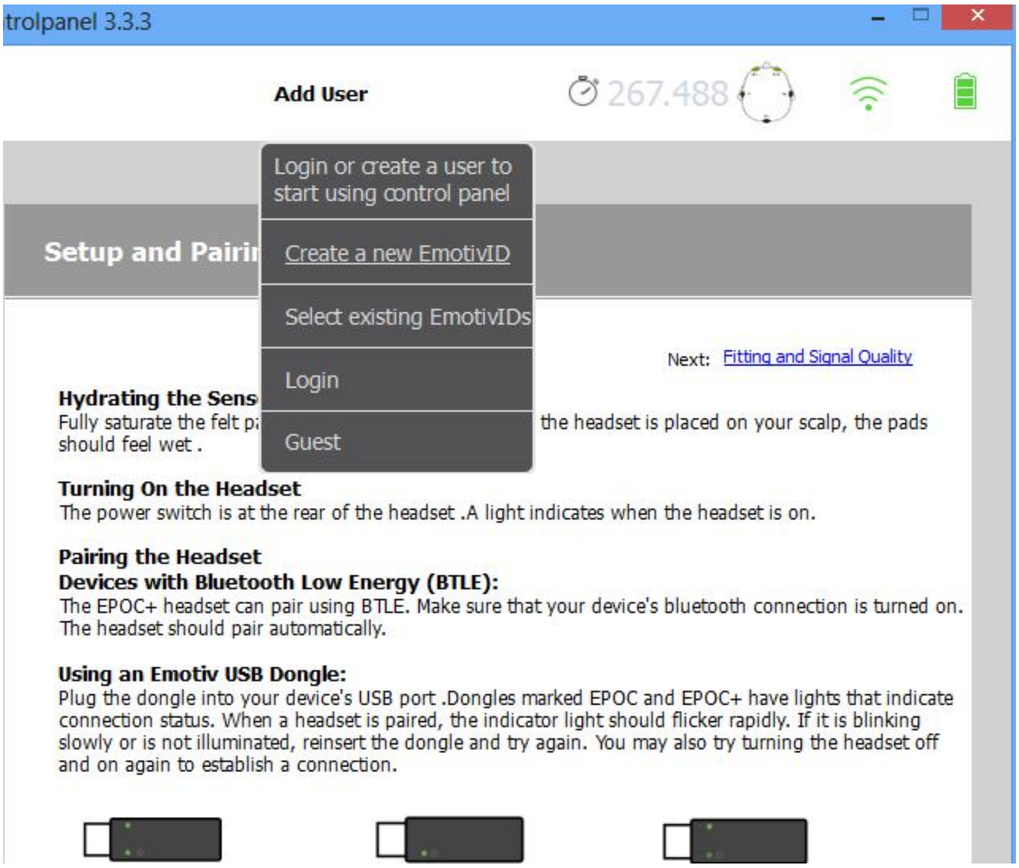


Figure 2.6. Signal Quality of the five channels in Emotiv Insight

Figure 2.7 presents the login screen, which requires a username and a password. A user can register for these details for free. This username enables the synchronization between the device and the computer interface. It is essential for the user to have an emotiv ID so as to connect the device to the Xavier Control panel.


trolpanel 3.3.3
Add User
267.488
Login or create a user to start using control panel
Create a new EmotivID
Select existing EmotivIDs
Login
Guest
Setup and Pairi
Next: Fitting and Signal Quality

Hydrating the Sens
Fully saturate the felt p the headset is placed on your scalp, the pads should feel wet .

Turning On the Headset
The power switch is at the rear of the headset .A light indicates when the headset is on.

Pairing the Headset
Devices with Bluetooth Low Energy (BTLE):
The EPOC+ headset can pair using BTLE. Make sure that your device's bluetooth connection is turned on. The headset should pair automatically.

Using an Emotiv USB Dongle:
Plug the dongle into your device's USB port .Dongles marked EPOC and EPOC+ have lights that indicate connection status. When a headset is paired, the indicator light should flicker rapidly. If it is blinking slowly or is not illuminated, reinsert the dongle and try again. You may also try turning the headset off and on again to establish a connection.

Figure 2.7. Login screen in Emotiv Xavier Panel

In order to make use of the complete functionality of the Emotiv Insight headset, the device needs to be trained with mental commands. These mental commands include an environment with a 3D image to push, pull, rotate and drag the object using an individual’s mental commands. The interface also include inertial sensors which aids the use of the headset to control the keyboard and the mouse. In this manner, once the device is trained, the full potential of the brainwear can be realized. This EEG headset has flexibility for usability and has powered capabilities aimed at helping human beings.

2.2.3 BCI Software

Brain computer interface technology works on the principle of signal acquisition and analysing these signals for research. In a native brain-computer interface, the hardware usually relies on three types of signals which are P300, steady state visual evoked potential (SSVEP) and event related desynchronization (ERD) (Fazel-Rezai et al. 2012). The P300 component is an essential component of event related potential (ERP) (Sutton, Tueting, Zubin, & John, 1967). An event related potential is the measure of electrophysiological response to an external or an internal response. The P300 component can be generated by presenting the subject to a series of events classified into two classes such that one of them is rarely presented. P300 is involved in the changes in the learning activity of the brain. It usually involves the process of memory modification, for instance learning and remembering things by a surprise if the activity is already learnt by the brain (Fazel-Rezai et al. 2012).

In recent years, research has revealed a great deal about P300. These studies and research about P300 has enabled the application of BCI for a greater range of applications such as assisting disabled people. One of the major reasons involved with the study of P300 has been the ease to measure the activity and making the brain-computer interface non-invasive (Nunez, 1981). Furthermore, P300 doesn't require too much time to be trained and works with majority of subjects who suffer from neurological problems. Finally, it provides a goal oriented control signal. This signal could be vital for spelling and control applications where there is a non-requirement for a continuous signal. The P300 speller has been a huge achievement for brain-computer interfaces as the results are produced by an endogenously attention based function. Another important approach being studied is to perfect the measurement of P300 activity and make it more accurate. Some of the factors include attentional blink, repetition blindness, target-to-target interval and habituation (Fazel-Rezai et al. 2012).

These factors are known to be a hindrances in the accurate measurement of the P300 thereby slowing future application development. One of the studies includes motion based stimuli instead of flashing stimulus. The results must be stable for the P300 component to assist the study. Emotiv offers a range of applications and software to monitor EEG raw data. This data can be essential in understanding the precise brain activity. For the raw data extraction, the P300 signal has a significant role for understanding the data quality and the brain activity in a more detailed fashion (Fazel-Rezai et al. 2012). Research is being carried to improve the quality of P300 evoked potential so that new techniques can be devised to treat a variety of neurological diseases.

2.2.4 BCI2000

One of the significant advances is the BCI2000. Even though, brain-computer interfaces have been an aid to treat with people suffering from neurological disabilities, BCI2000 has moved this technology forward (Schalk et al. 2004). Essential features for BCI2000 include the description of the brain-computer interface hardware and enabling communication through documented TCP/IP protocol which in turn enables programming in different languages for machines on different networks. The information that passes through various components has been designed to reduce dependency. All the functions are evenly distributed amongst the respective components. In addition, feedback mechanism is devised in the user application to view the functioning of each component (Schalk et al. 2004). Every brain-computer interface requires the software response to be quick because the brain activity is complex. Trillions of messages are passed through every synapse. BCI2000 has shown to have a very quick response time and ensures minimal pressure on the hardware thereby assuring accurate performance. Different components in the BCI2000 are known as modules. Modules serve the backbone for BCI2000. BCI2000 compromises of four main modules:

- Source Modules: The source modules are responsible for digitizing and storing brain signals. Furthermore, it passes these signals for further processing. The two major components that entail source modules are data acquisition and data storage. As the name suggests, data acquisition is responsible for acquiring the data which is the brain signal and the data storage highlights the function in the storage of these acquired brain signals (Schalk et al. 2004).
- Signal Processing Module: This module chiefly deals with the conversion of brain signals to usable output that can be further applied to an external device. The conversion happens in two stages which are feature extraction and then translation. In the first stage, the acquired digitized signals are exposed to extraction which involves recording certain features such as the neuron firing rate, frequency of an evoked response potential. Once extracted, an algorithm is dedicated to translate these features into control signals making them readable by the external devices (Schalk et al. 2004).
- User Application module: Once the control signals are established, a software or an application drive these control signals bridging the software and the hardware platform. The user interface normally is a computer screen and provides various

features such as gyroscope for cursor movement, virtual keyboard (Schalk et al. 2004). Research has focused on these control signals to drive prosthetics for disabled people (Lauer, Peckham, Kilgore, & Heetderks, 2000).

- Operator Module: This model defines various system parameters for the efficient execution of the software. It provides an investigator control of an experiment and access to areas which are limited in some other applications (Schalk et al. 2004).

All these modules drive the complete BCI2000 interface and provide access for monitoring various activities and the intricate details happening in the brain. A variety of applications have been made possible with the use of BCI2000. Some of these applications include the evaluating and comparing of different brain signals. This reduces the stress on machine power use, including the time and the effort invested in the testing of new devices. Two major factors that drive the BCI2000 are the four modules discussed above and the enabling independence and scalability of these modules. Many of the benefits of BCI2000 have been understood over time and testing. In addition, it is an open source product which gives developers opportunities to develop novel applications for people suffering from voluntary movement disability. Furthermore, it also provides a way to develop new applications to aid cognitively impaired individuals (Schalk et al. 2004).

2.3 SOCIAL APPLICATIONS OF BRAINWEAR

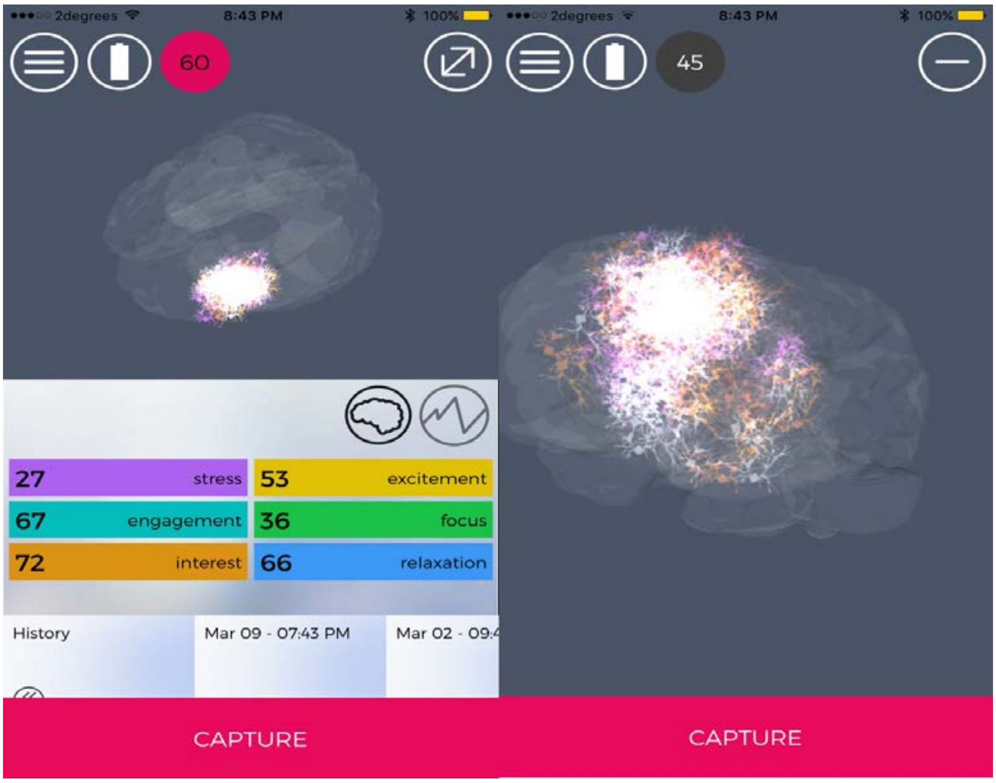
Modern day brainwear have made numerous tasks possible and a variety of companies have started to manufacture the simpler version of the EPOC and ECOG headsets. These EEG headsets have made life much easier and more beneficial by enabling individuals to monitor the brain activity and monitor stress levels on a finger tap. This section examines the Emotiv application and the various features offered with the application. The section 2.3.1 describes the MyEmotiv application and 2.3.2 describes the parameters explored by the application. Section 2.3.3 examines the gaming application and the various parameters that can be analyzed using the Emotiv application. Section 2.3.4 postulates various applications of the brain-computer interfaces in terms of clinical use, and the available BCI tools are described in 2.3.5. Finally, section 2.3.6 concludes with the challenges encountered with a brain-computer interface.

2.3.1 Emotiv Insight application

The Emotiv Insight application is currently available to download on smartphones and tablets running on iOS or Android operating system. The application MyEmotiv is free for download. Also, Emotiv offers a desktop application called Emotiv Xavier Control Panel for extended functionality. Once the application MyEmotiv is downloaded, the initial step is to pair the EEG headset with the smartphone. On completion, the application displays real-time brain activity. It also shows the levels of various parameters such as stress, interest, engagement and focus levels to name a few. These factors lead to an individual's ability to keep a constant eye on the brain activity and monitor cognitive health. A monitoring of these parameters will in turn help in optimizing brain function, manage stress levels and learn ways to improve brain fitness.

2.3.2 Parameters of Emotiv Insight

The six parameters that the MyEmotiv application offers are Stress, Excitement, Focus, Relaxation, Engagement and Interest levels. Figure 2.8 shows the various parameters recorded in the application MyEmotiv and Figure 2.9 shows the same levels recorded on the Emotiv Xavier Control Panel.



27	stress	53	excitement
67	engagement	36	focus
72	interest	66	relaxation

History

Mar 09 - 07:43 PM

Mar 02 - 09:4

Figure 2.8. Parameters monitored in the MyEmotiv application

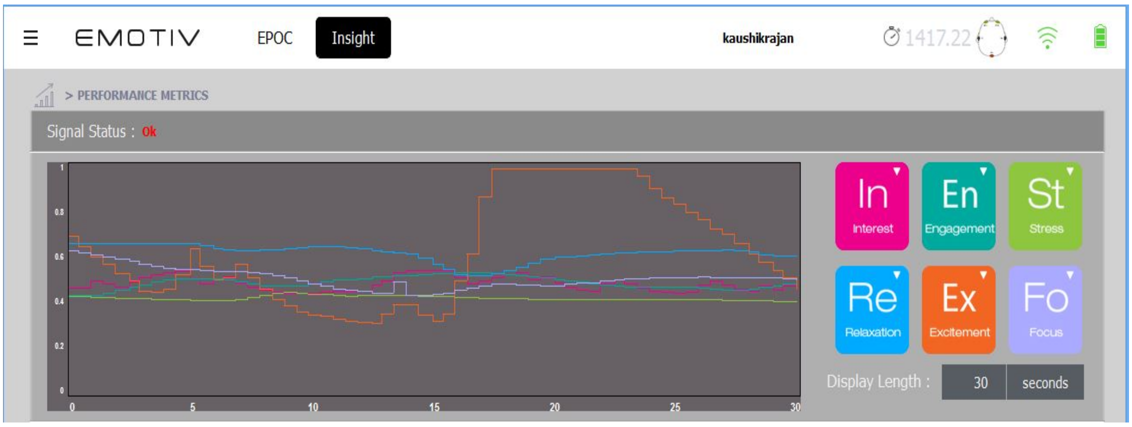


Figure 2.9. Parameters monitored in the Emotiv Xavier Control Panel

These parameters show the levels of each signal. Hence, the user has an option to come up with various strategies for getting the stress levels are down or to improve the focus levels. The six parameters are essential to determine the brain activity in real time.

2.3.3 Gaming using BCI

EEG based brain-computer interfaces have been widely used by disabled individuals to communicate with machines. Now, they are also being widely used in video games as controllers. Some of these games involve neurofeedback, a technique that relays feedback to the user with respect to the EEG signals in real time. Many neurofeedback games have shown to have promising effects on the healing of individuals with Attention Deficit Hyperactivity Disorder (ADHD) (Q. Wang, Sourina, & Nguyen, 2010). EEG based games can be split into two parts wherein the first one is the signal processing stage followed by the game implementation. Most EEG based games engines are based on three principles which are roll your own, mostly ready games and point and click (Q. Wang et al. 2010).

These games serve as a challenge to improve mental thinking ability. For non-mobile individuals, some of the games make use of cortical neuronal firing and translates them to the output device. In the paper by Scherer et al. (2013), the authors propose a new technology of gaming called kinetic based computer gaming. This type of game was suited only for individuals who were able-bodied. The results of the experiment show that Kinect sensor provides valuable information for dividing EEG data and the activity patterns for limb movements. Emotiv has also launched a game called Arena. This game aims at shooting fireballs using the mind. The game requires the user to be trained with a specific action which can further be used to play the game. Various other companies have released different variations of the game (Finke, Lenhardt, & Ritter, 2009). The EEG headsets have changed the gaming environment and it employs driving mental thoughts without physical contact with the keyboard or a mouse. One of the papers by Hjelm & Browall (2000) describes an experiment to compete in a completely relaxed state. The user plays a game called brainball wherein the game measures the real-time brain activity and presents situations wherein the user can only compete unless they are in a relaxed state of mind. The game has shown many of improvements with respect to stress relief and improving the control between stress and relaxation (Hjelm & Browall, 2000). Research has also concluded that BCI gaming interfaces have shown promising effects to allow epileptic teenagers to play games such as Space Invaders (Nijholt, Bos, & Reuderink, 2009). The Berlin Brain computer interfaces have employed the use of motor imagery to play games such as Ms Pacman & Pong, and similar games such as Tetris (Nijholt et al. 2009). One of the arcade games by Emotiv requires the user to push, rotate and arrange the stones to form a structure until the desired structure has been recreated. These games are making significant differences in the lives of people suffering from neurological disabilities.

2.3.4 Clinical Applications of BCI

Brain computer interfaces were designed for individuals with severe disabilities thereby enabling them to communicate in a fashion which could be interpreted easily. One of the significant reasons leading towards research of this technology was to bring hope to individuals who have been suffering from motor disabilities, Amyotrophic lateral sclerosis (ALS), spinal cord injury and other neuromuscular diseases (Mak & Wolpaw, 2009). In addition, it would reduce isolation, give them a better quality of life and significantly reduce the cost of caretaking. The clinical reasons which led to the research towards brain-computer interface have been enlisted below:

- Individuals with no detection of neuromuscular activity.
- Individuals who retain very limited muscular activity
- Individuals who retain substantial amount of neuromuscular activity.

The first point, concerns the strength of relationship between the BCI technology and health. Due to compatibility and complexity issues careful observations are required to manage the degradation of the disease variables, and the role in influencing effects. For the second and third points, BCIs can offer communication and control capabilities (Mak

& Wolpaw, 2009). The two-potential clinical uses that brain-computer interface has led to are neuroprosthetics and neurorehabilitation. Neuroprosthetics has been studied for long time and effective gains are evident. Initially, prosthesis would include the use of wood, metal pegs and hooks. Later, robotic arms were the biggest breakthrough, wherein the hand would look a bit more natural. Now, in today's modern technology, neuroprosthetics have created a natural and a more realistic hand powered with myoelectric prostheses (Bright, Nair, Salvekar, & Bhisikar, 2016).

Wheelchairs controlled by EEG were designed to treat individuals with locomotion problems. Directional commands were perceived by EEG and was relayed to the wheelchair but had the requirement of precise control signal. Later, P300 BCI wheelchairs were also reported where the individual was simply required about the directions (Mak & Wolpaw, 2009). Recent studies have also shown wheelchairs that are equipped with smarter algorithms thereby offering the individual with a better control using these wheelchairs.

On the other hand, the use of brain-computer interfaces can potentially serve as a therapeutic use to help individuals with impaired neuromuscular function to relearn useful motor functionality. Neurorehabilitation through brain-computer interfaces promotes functional recovery of neuromuscular action thereby offering to improve the quality of life. EEG signals from the brain-computer interface are required to activate the device in order to assist muscular movement (Mak & Wolpaw, 2009). Among all the neurological disabilities, stroke is known to be the leading cause of severe disabilities. One of the clinical study employed the use of motor imagery for stroke recovery and concluded that through fMRI study that motor function was activated in 20 hemiparetic subcortical patients. fMRI is functional Magnetic Resonance Imagining, a technique involved in measuring the brain activity with respect to changes in blood flow. The results also went on to show that 6 out of 8 patients were able to control the brain-computer interface (Ang et al. 2010). Brain-computer interfaces have proved to be beneficial to some individuals with these disabilities.

2.3.5 BCI tools

To make complete use of brain-computer interfaces, tools and applications are required that can drive external devices and can aid the well-being of an individual. This section examines various tools and the operating environment in relation to their capabilities to drive a BCI. Table 2.2 presents the current tools and the operating environment.

Table 2.2. BCI tools and the compatability (Ramadan & Vasilakos, 2017, p. 11)

Name of the Tool	Operating system		
	Windows	Linux	Macintosh
OpenVibe	Yes	Yes	No
TOBI	No	Yes	Yes
BCILAB	Yes	Yes	No
BCI++	Yes	No	No
xBCI	Yes	Yes	Yes
BF ++	Yes	Yes	Yes
OpenBCI	Yes	Yes	Yes
Pyff	Yes	Yes	Yes

These tools reviewed in this section. The tools are OpenVibe, TOBI, BCILAB, BCI++, xBCI, BF++, Pyff and OpenBCI.

- OpenVibe is an opensource platform that runs on Windows and Linux platforms. It includes many features including spell checker using P300, spaceship for motor imagery, handball and a shooting game based on Evoked Potential (Ramadan & Vasilakos, 2017).
- TOBI is a common implementation platform or CIP that runs on Linux and Macintosh platforms. Comprising of three platforms namely TiA, TiB and TiC, each of them are dedicated to signal acquisition. TiA is used to transmit several types of signals such as raw signals whereas on the other hand TiB is responsible for signal transmission. Finally, TiC is present to detect classes and labels within the BCI (Ramadan & Vasilakos, 2017).
- BCILAB is an open source toolbox for BCI research that runs on Windows and Linux platforms. BCILAB consists of various components such as signal processing, feature extraction, machine learning to name a few (Ramadan & Vasilakos, 2017).
- BCI++ designed for Windows platform contains two main modules namely Hardware Interface Module (HIM) and Graphical User Interface (AEnima). The HIM module is mainly responsible for acquisition of signals, storage and

visualization whereas the graphical user interface module is responsible for creating and managing computer-driven protocols (Ramadan & Vasilakos, 2017).

- xBCI is one of the cross-platform tool which runs on all Windows, Linux as well as Macintosh computers. In addition, the common tool is based on sophisticated graphical interface which mainly provides help for BCI developers to build their applications (Ramadan & Vasilakos, 2017).
- BF++ is a language framework entailing various software components, libraries and tools for brain-computer interface applications. It also runs across all the platforms which are Windows, Linux and Macintosh (Ramadan & Vasilakos, 2017).
- Pyff is a tool written in Python language that aids the exchange of experimental paradigms between research groups, reduce the need to reprogram standard paradigms and facilitate reproducibility of published results. Pyff is a cross-platform tool (Ramadan & Vasilakos, 2017).
- OpenBCI is an open platform mainly dedicated to help disabilities in a home environment. Due to its flexibility of multiplexer server, new modules and components can also be added. Runs on Windows and Linux platforms (Ramadan & Vasilakos, 2017).

2.3.6 Challenges and Disadvantages

As the previous sections have explained the advantages and the applications of brain-computer interface, section 2.3.6 evaluates the challenges of the brain-computer interface. Furthermore, some disadvantages have also been analyzed to understand the implications and devise ways to mitigate these disadvantages to have a better functional product beneficial to human beings. One of the biggest issues is the need to provide fast, accurate, and reliable control signals. Current brain-computer interfaces are only aimed at people with severe neurological disabilities which serves as a disadvantage for individuals facing little or no disability (Wolpaw et al. 2002). Non-invasive EEG require some level of training to place it and the need to constantly check the contact quality for better results. One of the daunting challenge faced by non-invasive EEG is the lack of a robust non-invasive sensor which can measure brain signals effectively and at high fidelity (Kroeker, 2011). Some potential challenges pertaining to the use of brain-computer interface are listed below:

- Signal acquisition hardware: The signal acquisition hardware needs to be upgraded constantly for nonmobile BCI applications is a core challenge (Pattnaik & Sarraf, 2016).
- Reliability: Brain-computer interfaces have poor reliability with most of the applications. It is essential for brain-computer interface system to be appropriate for real time execution for actions in the human body (Pattnaik & Sarraf, 2016).
- Training: The most time-consuming activity. The significance lies in either controlling the user through the different procedures and the sessions that have been recorded (Pattnaik & Sarraf, 2016).
- Information Transfer Rate (ITR): One of the most used parameters to measure the performance of brain-computer interface system is the information transfer rate. There are essentially three factors that can affect the transfer rate namely accuracy of target detection, number of classes and time to detect target. The Signal to noise ratio (SNR) is one of the hindrances that can result in an inaccurate detection of target. With increase in the information transfer rate, the number of classes keep increasing with an increase in complexity to handle class distribution. The time consumed to identify the target can also have an effect on information transfer rate (Ramadan & Vasilakos, 2017).
- Many P300 BCIs may be less effective in people who cannot gaze which is inclined to happen with severely disabled users (Fazel-Rezai et al. 2012).

In conclusion, the above-mentioned factors serve as challenges and issues and need to be overcome for an effective performance of brain-computer interfaces.

2.3.7 BCI Standards

One of the important aspects for a brain-computer interface system to work efficiently, are standards. The research community for brain-computer interface lacks specific standards, and so each company manufactures brainwear with their own procedures and policies. Although, the new dry electrodes have overridden the use of invasive electrodes that requires a surgery, there are no specific guidelines or standardized procedures which creates issues as far as usability is concerned (Ramadan & Vasilakos, 2017). Furthermore, numerous BCIs have already been developed by various companies and lack compatibility with each other. The lack of standards results in less reliability and creates brain-computer interface illiteracy (Jeunet, Jahanpour, & Lotte, 2016). Training becomes a daunting task and most of the subjects lack exposure and instruction for application of brain-computer interface. One of the experiments described in the paper (Jeunet et al. 2016) went on to conclude that half of the subjects were unable to control the brain-computer interface. The results determined with the experimentation also proved that there was no correlation between motor tasks and Motor Imagery – Brain Computer Interface (MI-BCI) due to absence of proper standard for brain-computer interface. The requirements for proper standards need to be established so that the brainwear can be used effectively with cross platform compatibility.

2.4 POTENTIAL SECURITY AND PRIVACY ISSUES

Brain-computer interface use has increased in terms of usability and the technology assisting individuals suffering with neuromuscular malfunction challenges. Brain-computer interfaces have gained popularity in both medical and non-medical areas. Section 2.4 describes the potential security and privacy issues in terms of applications such as gaming, neuromedical, smartphone, authentication applications. Section 2.4.1 lists the various vulnerabilities in terms of the application of brain-computer interfaces. Finally, section 2.4.2 has the possible security issues with a brain-computer interface. The application for polygraphs and lie detection is also discussed.

2.4.1 Security and Privacy Issues

The initial attacks were performed by the researcher on the Emotiv EPOC headset. A series of experiments were carried out. Random images, credit card images, bank logos were flashed on the computer screen to measure the peak of P300 to external stimulus. A peak in P300 tends to give away some personal information such as random PIN numbers, the specific bank with the account, automated teller machines. All these images were flashed for 250ms and an interval of 2 seconds was given with every change of image (Martinovic et al. 2012). The results went on to prove that the information could be extracted. It was not done on the first attempt but the probability of extracting the information kept on increasing with every attempt. It had better odds than a brute force attack (Martinovic et al. 2012). The first brain-computer interface enabled malicious activity was presented in 2012 USENIX Security Symposium. This application was referred to as “brain spyware” and designed to extract personal information such as date of births, credit card PINs and geographical locations of participants’ homes (Bonaci et al. 2014). Furthermore, EEGs are believed to be one of the most secure methods for authentication and application as a biometric security mechanism (Thomas & Vinod, 2016). There are many applications that can make use of raw EEG data to extract personal and intimate information. These are simple attacks but are indicators that sophisticated attacks can be achieved (Martinovic et al. 2012).

The security and privacy issues are described in detail below. They have been broadly classified into four types of application based attacks which are neuromedical applications, authentication application, gaming and entertainment, and finally smartphone-based application (Li, Ding, & Conti, 2015).

- Neuromedical applications: Brain-computer interface has enabled communication between the human brain and an external device. One of the scenarios of an attack has been explained with a neuromedical application for prosthetic limb. Though in this case, it is an implantable device, once the complete raw EEG data is established between the patient and the physician, an attacker can easily intercept the data despite the information being encrypted. The attacker can illicit commands and get the device to malfunction and give wrong movements to the prosthetic arm (Li et al. 2015)
- Authentication: A growing number of articles have put forward the use of brain signals to be used to for authentication purposes. These EEG brainwaves might pose privacy risks for the users. Attackers have tried to design an attack model such as the subject’s thought pattern and tries to perform deliberate attack. Eventually the attack can be achieved to break down the authentication using synthetic EEG signals (Li et al. 2015).
- Gaming and Entertainment: Most of the BCI controlled games are P300 based. Whenever there is a difficult stage or an excited stage, the shift in the P300 level is evident. BCI games extract personal and sensitive information using recorded EEG signals (Martinovic et al. 2012).
- Smartphone applications: The smartphone based BCI application are prone to attacks as well. It originates from the mobile phone itself. These applications can access all kinds of confidential data and the attacker can remotely transfer the data

as well. These data are acquired from the BCI device itself and also pose as a threat to attack smartphone based BCI applications (Li et al. 2015).

All these possible security flaws and privacy issues are a potential threat to a person using BCI technology. Efforts have been made to mitigate these issues but proper standards are yet to be set. In addition, the US Food and Drug Administration has specific governing laws for medical devices (*ISO* 13485:1996). They do protect information but on the other hand they cannot block third party applications and APIs that are designed for brain-computer interfaces. The literature identifies two types of attackers. The first type of attacker extracts an individual's information by completing hijacking the various components of the brain-computer interface. The second type of attacker tries to modify by either adding or replacing some of the components of the brain-computer interface. In this case, special algorithms are to be designed by the attacker to replace legitimate code (Bonaci et al. 2014).

Some methods of information extraction have also been described by various researchers. The oddball paradigm, guilty knowledge test and the priming technique to name a few. The oddball paradigm is a technique where a user is asked to react a target stimulus with hidden rare occurrence of non-target stimulus. The guilty knowledge test (GKT) has an operating hypothesis that it will evoke different responses to a similar stimulus (Martinovic et al. 2012). The priming technique makes use of implicit memory effect where one stimulus may have an influence on an individual's response to a later stimulus as well (Bonaci et al. 2014). These techniques can record neural signals which can be used to manipulate the individual or force him/her into doing something against their actions (Bonaci et al. 2014). One researcher also presented a case where the extracted neural information could be used to cause physical and mental damage. In this case, the attackers had placed flashing animations on epilepsy support webpages, eliciting seizures to individuals suffering from photosensitive epilepsy (Denning, Matsuoka, & Kohno, 2009).

2.4.2 Lie Detection and polygraph

Terrorist attacks have been a constant factor of fear and they often involve crime scene investigations. When caught, the terrorist or the criminal tries to hide his/her identity and the true motive to keep themselves safe (H. Wang, Chang, & Zhang, 2016). This required the need of a system which could find the criminal's intention and validate the information being provided by them. The traditional method that has been used is the polygraph test system based on autonomic nervous system activity (H. Wang et al. 2016). But lately, researchers have indicated the indirect and limited view of brain processing in polygraphs have to be validated (Verschuere, Crombez, Koster, & De Clercq, 2007). To overcome these limitations, modern EEG based brain computer interface with event related potential (ERP) have been introduced. In comparison to the existing methods, EEG based detections measure the level of event related potential which reflect the related changes in brain activities.

The principle behind using EEG based event related-potential makes use of P300 probes. A P300-based concealed information test (CIT) system makes use of target (T), irrelevant (I) and probes (P). The conventional method for feature extraction and selection in P300 based lie detection involves the comparison of amplitude of P300 response in probe and irrelevant stimuli. A brain-computer interface system can achieve accurate and efficient feature extraction using pattern recognition in combination with event related data. The use of brain computer interfaces in conjunction with CIT system and pattern recognition parameters have resulted in better interpretation during a lie detection investigation (H. Wang et al. 2016).

2.5 SUMMARY OF ISSUES AND PROBLEMS

Section 2.5 summarizes the issues and problems pertaining to the brain-computer interface from the literature reviewed. Non-invasive brain computer interfaces have had a promising growth and wide usability amongst common individuals. The need to address the security and privacy issues is noted of utmost importance at this stage. Brainwear should be cost-efficient but also secure. One of the major reasons to consider safety and security for these devices is essential as many of individuals are dependent on this brain-computer interfaces for their well-being. Patients suffering from Amyotrophic Lateral Sclerosis (ALS), Locked-in Syndrome (LIS), autistic individuals heavily rely on these devices as these brain-computer interfaces have offered these individuals a quality of life and the hope to overcome the barriers.

Some of the issues pertaining to brain-computer interfaces are summarized below:

- All brain-computer interfaces lack specific standards as far as the usability and other features are concerned.
- The information transmitted by the brainware could be captured passively (Bonaci et al. 2014).

- The authentication information involved in the pairing of the brainware and the smartphone application could be determined to extract private information (Li et al. 2015). This private information can lead to impersonation or identity theft.
- The data transmitted between the brainware and the smartphone application can be obtained using a malicious software (Martinovic et al. 2012).
- The communication between the brainware and the application could be eavesdropped and also be substituted with manipulated information thereby leading to compromise of the data (Rushanan, Rubin, Kune, & Swanson, 2014).
- A concealed attack utilizing the Event Related Potential (ERP) could be executed to capture, analyse and change the data to attack the brainware (Frank et al. 2013).

2.6 CONCLUSION

The literature reviewed has outlined the essential information for the foundation of this study. The review began by exploring the human brain, the essential regions, the activities related to these regions. After analysing the anatomical parts of the brain, the electroencephalogram was analyzed, and various parts of the human brain mapping was also reviewed. The next section covered the mental control signals associated with various brain activity followed by the review of Emotiv Insight 5 channel brainwear. In addition, P300 and BCI2000 platforms were also reviewed. After the description of the BCI2000 platforms, the MyEmotiv application and the Emotiv Xavier control panel were explored along with the features and the characteristics offered by both the software.

The second half of the literature reviewed covered the applications of the brain-computer interface in terms of gaming, neurological abilities and examined various tools and software in association with brain-computer interfaces. The last section concludes with the potential privacy and security issues with the use of brain-computer interface and the challenges associated with their usability. Chapter 3 will focus on the methods to find the vulnerabilities and the security issues related to the Emotiv Insight brainwear. Different techniques will be used to identify the possible attacks that can be performed and a research methodology will be defined.

Chapter 3

RESEARCH METHODOLOGY

3.0 INTRODUCTION

Chapter 2 provided an assessment of relevant literature and identified problem areas. The identified potential security vulnerabilities with the use of brain-computer interface have also been noted in Chapter 2. Chapter 3 derives a research methodology that is relevant to the security issues identified in Chapter 2. The focus of this chapter is on the derivation and building of a robust methodology. Chapter 3 strategizes a research plan that will be used to investigate the communication between the BCI EEG brainwear, in this case, the Emotiv Insight brainwear and the user interface. The important concepts for this study are security and privacy concerns with the use of brain-computers have been noted in Chapter 2.4.1. Section 3.1 reviews five similar studies related to my study to understand how others do this type of research. Section 3.2 specifies a researchable question that best fits the research problem. Section 3.3 lists the research sub-questions that focusses the study thereby leading to the construction of an effective methodology. Section 3.4 defines the data requirements and section 3.5 data analysis for the experimental stage. Subsequently, section 3.6 discusses the limitations of the methodology, and section 3.7 concludes the chapter.

3.1 REVIEW OF SIMILAR STUDIES

Five research studies pertinent to the topic of this thesis have been evaluated and then analytically reviewed in order to get an understanding of prevailing research methods and directions. Sections 3.1.1 to 3.1.5 reviews five research studies highlighting the methodology followed by the researchers to find potential vulnerabilities with the use of brain-computer interfaces and implantable medical devices. The five research studies have been evaluated to understand the methodology followed for each study. This knowledge will help instruct my approach to methodology and lead to the designing of the methodology for this research.

3.1.1 Bonaci, Calo, & Chizeck (2014)

Bonaci, Calo and Chizeck (2014) present various methods to determine the privacy and security issues in brain-computer interfaces. The study briefly begins with an introduction about the brain-computer interface and the various components associated with brain-computer interface. The P300 or simply P3 is a brainwave which is the brain's response to a specific event. This event may be a sensory, cognitive or a motor event. The study of the P300 wave led to the detection of an individual's four-digit PINs, sensitive information such as banking information, personal details including date of birth and respective locations of their residence. The authors have presented the possibility of a brain spyware designed to snip personal information.

To demonstrate the security and privacy issues, the authors have proposed a threat model. Two types of threat models have been presented. The first type of threat model describes that the attacker extracts an individual's confidential information by compromising the components associated with the brain-computer interface system. The second type of attack model extracts or compromises an individual's information by either adding or replacing genuine components. Three methods of extracting private information have been presented namely the oddball paradigm which is a stimulus based test, the Guilty Knowledge Test (GKT). This is a test based on an individual's attention to a specific piece of information and priming which is a technique for making use of stimulus to create a response that invokes implicit memory (Bonaci et al. 2014).

The first method of extracting private information is the oddball paradigm. In this method, 15 healthy subjects were selected free of any neurological injury or disease. The experiments were based on the shape of a stimulus presented to the participant. The task required the participants to classify the presented stimulus quickly on the basis of their shape. Furthermore, it also required participants to press the button with the left hand when the stimulus was presented with a circle and press the button with the right hand when the stimulus was presented with a square. Subsequently, the stimulus environment was presented in the opposite side of the screen as the response hand. The strategy of the brain's activity with response to an external stimulus evoked some brain signals which was captured by (Huettel & McCarthy, 2004). The captured signals were then analyzed to find the peaks and unusual rise in brain activity to retrieve useful information.

Figure 3.1 presents the stimulus environment chosen by (Huettel & McCarthy, 2004).

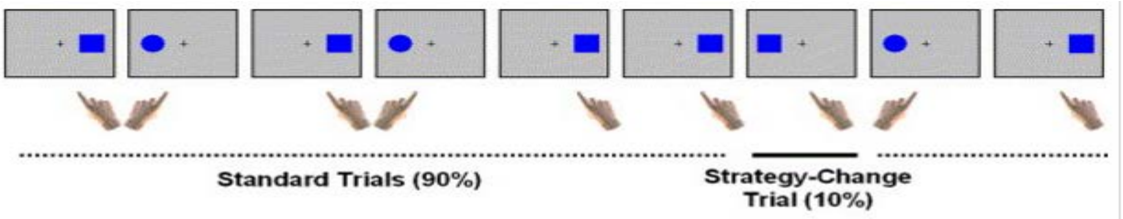


Figure 3.1. Experimental Stimulus Environment (Huettel & McCarthy, 2004, p. 2)

The second method of extracting information is the Guilty Knowledge Test (GKT). This method employs a technique that seeks to determine the attentional value of information to an individual by comparing his/her responses to relevant and neutral questions. The questions are chosen in a manner that subjects to the knowledge of an incident or a specific environment that would result in an amplified response to the relevant question. Though, the GKT has been widely useful for crime investigations, it serves as an effective method to retrieve information by observing the physiological response which is an involuntary reaction triggering a physical response to a specific stimulus. This test analyses the brainwave as an index to measure the recognition of a concealed information. The GKT makes use of different types of stimulus environment such as a familiar stimulus, an irrelevant stimulus and a stimulus that evokes the guilty response. The brainwave is recorded for all the stimuli and analyzed to retrieve hidden information. (Abootalebi, Moradi, & Khalilzadeh, 2009)

The third method described to extract private information is called Priming. Priming is a technique that employs implicit memory effect wherein, the response to one stimulus may influence the response to another stimulus. For this method, (Wolpe, Foster, & Langleben, 2005) introduced physical stimulus such as a book, a mug or a tomato to hold, to override the limitations of visual or an auditory stimuli environment. Three participants were selected for this experiment, where each participant was given an object allowed to be held and placed before them on the table. The recordings were made using a 32 channel EEG cap and 3 external electrodes placed in the middle of the forehead. In addition to P300, another brainwave was found to be potentially useful for information extraction. This brainwave was known as N400 which is the brain's response occurring exactly after 400 microseconds post the stimulus being presented in front of the individual. The exploration of N400 wave was studied to extract private information by mapping the peaks of the EEG reading and measuring the N400 wave (Wolpe et al. 2005). All these methods of information extraction depend on the stimulus environment presented to the individual. The methods employ the use of invoked responses such as push and pull and the brain's activity to a specific stimulus such as a visual stimulus or random numbers projected on a screen. The P300 wave is generated from the brain's response to a specific stimulus and fully elaborated by Bonaci, Calo, & Chizeck (2014).

3.1.2 Li et al. (2015)

Li et al, (2015) have chiefly focused on the security and privacy challenges with the use of brain-computer interface technology. Li et al, (2015) postulate that most of the modern-day Brain-computer interfaces focus more on the application development without paying much attention to security. Four applications have been presented along with the potential risks of an attack. These applications are Neuromedical applications, User Authentication and smart-phone applications.

Neuromedical applications mainly include the use of brain-computer interface technology to help patients with motor impairments. Mostly, physicians connect wirelessly to adjust the settings of the neural implant devices. For this specific attack, (Conti, Mancini, Spolaor, & Verde, 2015) have proposed an attack model by analysing traffic using android technology. In the framework postulated by Li et al. (2015), mobile applications rely on SSL/TLS to securely communicate with peers. Each TCP segment is embedded into an Internet Protocol datagram and exchanged with peers. Li et al. (2015) generate a model for traffic flow with time series to examine the outgoing and the incoming packets. Using this model, encrypted network traffic can be eavesdropped to breech the privacy of mobile users. In this manner, the transmission of brain signals can be intercepted, saved and can be decomposed to extract private information despite the communication being encrypted.

User authentication is the second application which is a process that confirms and verifies one's identity. Li et al (2015) has described the use of EEG brainwaves to authenticate might lead to privacy risks. The attack model described collected brain data from 15 university students based on mental tasks such as breathing, imagining a finger movement, imagining a repetitive movement from a sport. Li et al (2015) developed a 15-subject authentication system using the data collected. The best task and customizable threshold was determined, and the impersonation of the attack was carried out. Figure 3.2 presents a flow of the questions required to impersonate the attack.

A questionnaire was developed to categorize the actions into various groups and evaluated for the success probabilities within each. The results went on to show that individual thoughts can be impersonated thereby indicating the feasibility of a possible attack.

Smartphone-based application is the application interface described by Li et al. (2015). The attacks in such applications is believed to be originating from the mobile device itself. These applications can access confidential data which is acquired from the BCI device and stored in the phone memory or the SD card. To achieve the exploitation, a privileged escalation attack has been described by Davi et al. (2010).

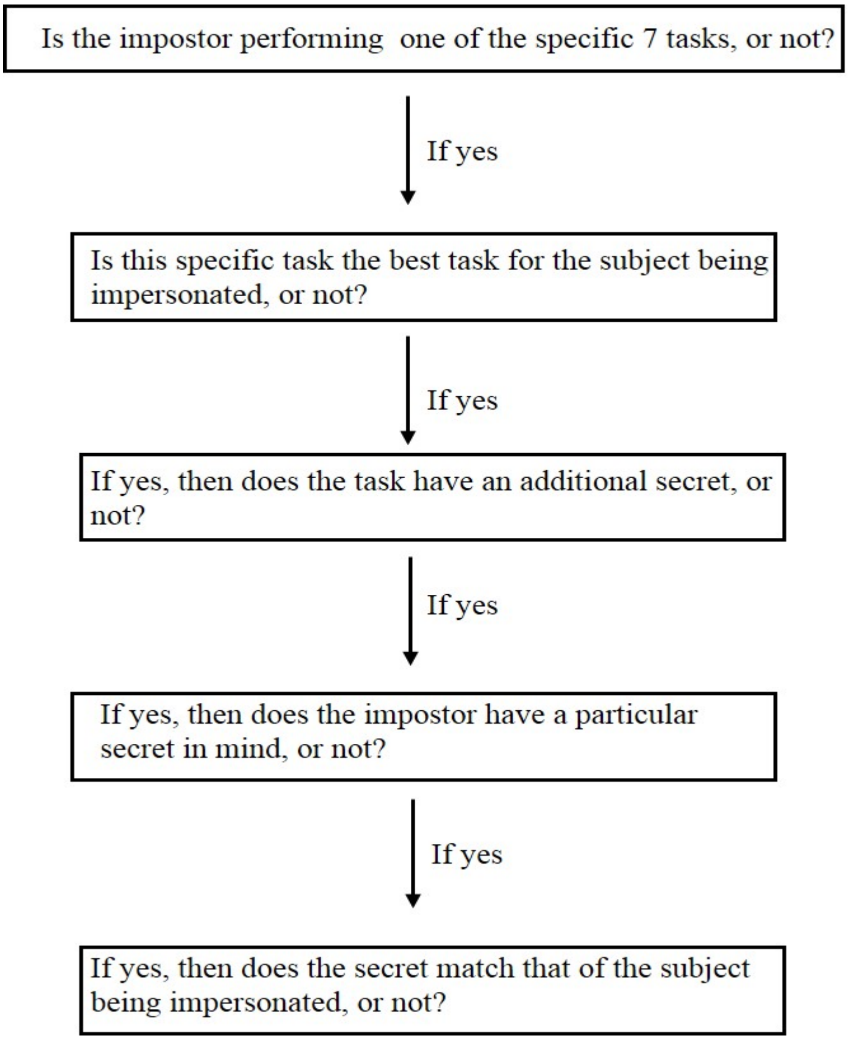

Is the impostor performing one of the specific 7 tasks, or not?
If yes
Is this specific task the best task for the subject being impersonated, or not?
If yes
If yes, then does the task have an additional secret, or not?
If yes
If yes, then does the impostor have a particular secret in mind, or not?
If yes
If yes, then does the secret match that of the subject being impersonated, or not?

Figure 3.2. Flow of questions for the attack (Johnson, Maillart, & Chuang, 2014)

When a user downloads a malicious application such as a game, the user grants permission to the game to access the internet. To achieve the attack, the adversary exploits the vulnerability in the application and performs a privileged attack using the flaw with Android Scripting Environment. The attack technique is referred as Return-Oriented

Programming (ROP) and allows the attacker to induce arbitrary program behavior by chaining small instructions sequence.

3.1.3 Martinovic et al. (2012)

The study notes the popularity of the use of non-invasive brain-computer interface technology in the gaming and the entertainment industries. Martinovic et al (2012) stress the security risks associated with the use of consumer-grade BCI devices as not much research has been performed about the impact of malicious software on these devices. The significance of recording neural signals provides a platform to improve patient care as brain-computer interfaces have been deployed to treat several neurological disabilities such as Parkinson's diseases, Attention Deficit Hyperactivity Disorder (ADHD) and epilepsy. This has been achieved by neurofeedback therapy. Furthermore, the cognitive activities captured by the brainwear enable the development of efficient adaptive games which are responsive to the individual's affective states.

The threat model described by Martinovic et al (2012) presents a scenario where the attacker is a third-party application developer. The assumption is that the attacker can read the EEG signals leading him/her to design specific stimulus environment to maximise the amount of information leaked while trying to hide the attacks. For this study, 28 computer science students were recruited, with computer screens in front of all the participants. The Emotiv EPOC 14-channel headset was used for this experiment. A base line was recorded and then a series of visual stimulus were presented and the brain activity was monitored. These visual stimuli were a mix of Automatic Teller Machine images, Credit and debit card images, bank logos, geographical locations and known people. The intent behind this experiment was to try to obtain information such as the 4-digit PIN, banking information, month of birth and geographical location. In this fashion, different visual stimuli were presented to the participants and the brainwave signal peak was monitored throughout the experiment. Each electrode is a channel in the Emotiv headset. With 14 channels present, the attacker exploited the occurrence of the P300 brainwave peaks in the EEG signal that were triggered by the stimulus environment and captured. The results were classified in two phases namely the training phase and the classification phase.

The study concludes with the results presented in statistical format using the BCI2000 P300 which is a spelling software showing a success ratio of 40% for various scenarios. Finally, the simplicity of the experiments suggests the possibility of sophisticated attacks. Martinovic et al (2012) summarize by stating that, with the ever-increasing quality of these brainwear, the success rates of attacks will also be more prevalent.

3.1.4 Rushanan, Rubin, Kune, & Swanson (2014)

Rushanan, Rubin, Kune, & Swanson (2014) highlight the privacy and security with the use of Implantable Medical Devices (IMD) and Body Area Networks (BANs). The significance of a secured communication and efficient use of hardware and sensor interface has been highlighted by the authors. Rushanan, Rubin, Kune, & Swanson (2014) have postulated the existing vulnerabilities with the security and privacy of the sensor interface and the requirement for further research. Subtle eavesdropping and injection attacks on sensor interfaces have proven to be emerging threats with the use of medical devices thereby compromising the privacy of physiological inputs to key generation mechanisms.

The FDA regulates the use of medical devices and has significant influence with numerous foreign government organizations. The study focusses on the privacy and security goals along with an adversarial model. Based on the capabilities and relationship, Rushanan, Rubin, Kune, & Swanson (2014) have distinguished various adversaries. An adversary can either be an active adversary who can read, modify and inject data over the communication channel whereas a passive adversary can only eavesdrop on the communication channel including side channels.

Rushanan, Rubin, Kune, & Swanson (2014) have also presented the existing and the emerging threats with the use of implantable medical devices. An implantable medical device circuitry includes:

- Analog front end for application-specific sensing and actuation.
- Memory and storage for storing personal health information.
- Telemetry interface for radio-based transmission of data from the device to the user interface.
- Power management, for monitoring for increased longevity.

One of the threats described by the authors include the telemetry interface which offer eavesdropping on wireless communication for a passive adversary. On the other hand, an active adversary also poses as a threat to jam or modify wireless communications. The second category of threats that have been presented are the software threats where an adversary could make use of vulnerabilities and alter the logic of the system. The final category of threats postulated by Rushanan, Rubin, Kune, & Swanson (2014) are the hardware and the sensor threats. In this scenario, an adversary can make use of vulnerabilities in the internal hardware architecture to attack the system.

Rushanan, Rubin, Kune, & Swanson (2014) have described two attacks that demonstrates the privacy and security issues with implantable medical devices. The first attack employs the use of two hardware tools to intercept the radio-frequency signals emitted by the Implantable Cardioverter Defibrillator (ICD). One of the tools included to intercept the radio frequency Universal Software Radio Peripheral (USRP). The experiment started by capturing Radio Frequency (RF) signals emitted around 175 kHz using the USRP and then reverse engineering the data into bits and further analysing these bits to discover key aspects of the ICDs protocols. This led to intercept the communication between the ICD programmer and the device. Halperin et al. (2008) also made use of a commodity software radio to eavesdrop with the open source GNU radio libraries. The data captured with the help of these GNU radios revealed a great deal of patient data in clear text and information was derived from the captured transmissions.

The second attack was described by Rushanan, Rubin, Kune, & Swanson (2014) on a commercial insulin pump designed with radio signal transmission. Both passive and active attacks have been presented by Li et al.., (2011). The communication was intercepted by the USRP by capturing the radio frequency signals at a specific frequency and then reverse engineer to launch the active attack. The operating frequency of the wireless link was determined which was 915 MHz. A 915 MHz daughter board and an antenna was attached to the USRP which received and generated signals at the 915 MHz band. After the interception of the wireless signals, Rushanan, Rubin, Kune, & Swanson (2014) observed an on-off keying in the communication. The analysis of these signals also revealed the transmitted PIN in plaintext captured by simple eavesdropping. Furthermore, the authors also demonstrated a replay attack by manipulating the packet information and substituting different values making use of a simple security mechanism.

Rushanan, Rubin, Kune, & Swanson (2014) recognize the security goals for medical devices with respect to the CIA triad which includes Confidentiality, Integrity and Availability. The confidentiality includes the accessibility of information to authorised entities only, integrity which denotes that the communication should not be modified by unauthorised entities and finally availability wherein the data should accessible when requested by an authorised entity. Rushanan, Rubin, Kune, & Swanson (2014) conclude the study by summing up the privacy and security issues with the use of implantable medical devices. Offloading heavy computations to another device such as a smartphone might improve the medical devices' battery life but opens venue for attacks as malware on mobile devices is common. In addition, key areas for possible attacks has been presented with respect to Electro Magnetic Interference (EMI) attacks and the physiological signals for passive eavesdropping. The reproducibility of results from various researchers goes to indicate that the availability of equipment and attention to detail in the report, may affect the ability of others to validate the work.

3.1.5 Frank et al. (2013)

Frank et al. (2013) show the increasing popularity of the use of brain-computer interfaces. Limitations associated with side-channel attacks have been analyzed and stated. These include the intrusiveness requiring a co-operating user, and the disclosure to users of the application are bound to realize an abnormal behavior with the application. Frank et al. (2013) describe a mode of attack with the use of brain-computer interface in a completely concealed way. The mode of attack presented by Frank et al. (2013) is a subliminal attack which aims at attacking the victim at a level below the individual's cognitive perception. The attack is similar to subliminal advertising which involves the idea of hiding visual stimuli within the screen content that the individual expects to see for a duration of 13.3 milliseconds. The success of the attack is in inferring private information without creating a suspicion in the individual's mind. Two major brainwear types have been used for the study namely the Neurosky and the Emotiv headsets.

The threat model described in Frank et al. (2013) is an application developer (the attacker) who provides the API for the device. Through the device's API, the application can access the raw EEG signal recorded by the device. The attacker makes use of Event Related Potentials (ERP) to run the attack strategy. Visual stimulus serves as the main target stimulus for the attack. The attack is executed from the minute the EEG signals is recorded whilst the user is exposed to different visual stimulus. The trigger is known to produce the strongest event-related potentials is analyzed by the attacker in a comparative way. The monitoring of ERP's leads to a peak in the P300 signal. Thus, the attacker implants his/her attack in an application that requires the calibration step to compare the baseline to the evoked ERP.

For the experiment, 29 undergraduate and graduate students were recruited succeeding the permission from Institutional Review Board (IRB). All participants were checked for any neurological diseases to avoid which could potentially interfere with the recording. The various tests conducted for this experiment included a series of numbers and video stimulus to record the EEG data. The concept presented by Frank et al. (2013) is the targeted probing and agnostic probing. In targeted probing, EEG data is contrasted against images that are mostly irrelevant to the user. On the other hand, agnostic probing involves the attacker confronting the user with a number of stimuli that are relevant to the individual. The biggest advantage is that the user is unaware when the attack is being carried out. With full access to raw EEG data constitutes a new attack vector on user privacy and user secrets.

3.2 RESEARCH DESIGN

The analysis of similar studies presented in Section 3.1 provides guidance on how to do security research in the BCI area. The review of the similar studies identifies areas where research has been completed and the identification of gaps has resulted in the generation of the research question, sub-questions and the hypotheses. All these questions are derived and presented in Section 3.2. Following Section 3.2, Section 3.3 presents the data requirements and with the data collection, processing, data analysis and a data map. The limitations are presented in Section 3.4, and the reliability and validity discussed. Finally, the conclusion is described in Section 3.5. The following sections 3.2.1, 3.2.2 and 3.2.3 present an analysis of the similar studies, the research question and the hypotheses for my study.

3.2.1 Summary of Similar Studies

Bonaci, Calo, & Chizeck (2014) have investigated the privacy and security issues with the use of Brain Computer Interface (BCI). The authors have presented three methods to extract private information using the Electroencephalogram (EEG) data. The methods described by the authors include oddball paradigm, guilty knowledge test and priming. These methods open gateways for the extraction of private and confidential information about an individual using a BCI. The attack is achieved by proposing two attack models. From the paper Bonaci, Calo, & Chizeck (2014), I would such as to adopt the following points into the proposed methodology:

- Cost effectiveness: One of the prime reason for choosing the Emotiv Insight for this thesis is due to budgetary constraints, the Emotiv Insight is cost effective. Furthermore, it is aimed for consumers due to its price and its functionality.
- Attack Model: The attack model for feature extraction will help me analyse the signals or the data sent across from the brainwear to the MyEmotiv application.

In the second research paper by Li, Ding, & Conti (2015), the authors have stressed the privacy and security challenges with the use of brain computer interfaces. Three chief applications Neuromedical, User authentication and smartphone based application have been described and the possible attacks on the application of brain computer interfaces. Neuromedical application has aided individuals with motor impairment and movement of prosthetic arms. User authentication using BCIs is a new addition for security as the brainwave is unique for every individual. The authors stress the need to address these challenges as many individuals depend on the use of BCI for a normal functionality. This applies to the greatest number of potential users who would not be using the advanced features of the more expensive professional models.

In the proposed methodology for my thesis, the following points have been adopted from this paper:

- Training Data: The device training data may provide a reference for the application to interpret real time neural signals. The methodology will include an investigation of the training data to derive any relevant information.
- Smartphone based application: The Emotiv Insight supports two different interfaces, for smartphones and desktops. The application is called MyEmotiv and an examination of the log files created when paired with the brainwear via Bluetooth will be integrated into the methodology.

The third paper reviewed as a similar study was Martinovic et al. (2012). Martinovic et al. (2012) present the use of BCIs in the gaming and the entertainment industry. The authors highlight the impact of malicious software on the BCI. The threat model proposed by the author is assumed to be an application developer. Visual stimulus has been used to extract private information such as bank details, date of birth and geographical locations. The unique brainwave has been used to find the spike on the EEG data to find a specific information. The study concludes by stating that these simple attacks present as a gateway for more sophisticated attacks to be performed. In the proposed methodology of my thesis, the following points have been adopted from Martinovic et al. (2012):

- Security Risks: The security risks associated with the use of consumer grade brain-computer interface are yet to be explored. This suggests that exploring more vulnerabilities is required.
- Non-invasiveness: The significant reason behind choosing the Emotiv Insight brainwear is the fact that it is non-invasive and doesn't require surgery or the use of any conductive gels. This makes the consumer's life easy as it doesn't require any special knowledge. The headset is simple to put on and is ready to use as soon as it paired with a smartphone or a laptop.
- Research question: The research question for Martinovic et al (2012) deals with the analysis of the captured signals from the device and how to derive sensitive information. These analysis forms a central concern for this thesis in order to get a better understanding of the captured signals
- Placement of electrodes: The electrode placement followed for the Emotiv Emotiv Insight which will be employed for this study, forms an essential component as no prior knowledge is required for specific placements of the dry electrodes on the scalp. This is essentially a very user-friendly feature about the Emotiv Insight contributing as a prime reason to be chosen for this study.
- Simplicity: The simplicity of the experimental setup for Martinovic et al. (2012) shows the feasibility of sophisticated attacks.

Rushanan, Rubin, Kune, & Swanson (2014) highlight the privacy and security issues with the use of Implantable Medical Devices (IMDs) and Body Area Networks (BANs). The authors note the significance of the involvement of the FDA and the regulation by the FDA for medical devices. The various components have been defined, the possible weakness listed, and the attacks that each component is prone. One of the significant components described in the study is the telemetry interface. The telemetry interface is responsible for the transmission of radio frequency data. The telemetry interface is hence a vulnerability. In addition vulnerability also lies amongst the software interface as more effort is dedicated to the development of the software application than the hardware. The emphasis on the hardware design is a compromise on the privacy of the individual.

The authors have summarized the existing threats with the use of IMDs. Furthermore, Rushanan, Rubin, Kune, & Swanson (2014) have also presented the attacks performed on insulin pumps and Implantable Cardiac Defibrillator (ICD). The authors present the possibility of eavesdropping communication between the device and the user interface. The eavesdropping could be achieved with the use of a Universal Software Radio. Tuning to the frequency of the insulin pump, data could be retrieved regarding the dosage of the insulin being pumped. The following points are adopted from this study:

- Passive eavesdropping: The idea behind passive eavesdropping presented and evaluated for this study by Li.et al. (2015) is a mode of attack I want to implement for this study.
- Telemetry Interface: The telemetry interface is one of the components I want to test in the Emotiv Insight as the data exchange is in the form radio frequency signals transmitted through Bluetooth Low Energy (BTLE).

Frank et al. (2013) presents the privacy and security issues with the use of brain-computer interfaces. The authors have briefly described the feasibility of a side-channel attack with the limitations. The threat model presented by Frank et al (2013) is a subliminal attack that aims to attack the victim at a level below the individual's cognitive perception. The authors define that the success behind an attack is in retrieving private information without creating a suspicion in the individual's mind. The attacker has been assumed to be an application developer who provides the Application Programming Interface (API) for the device. Upon reviewing the methodology used in Frank et al (2013), the following factors can be adopted into my thesis methodology:

- ERP: The evoked response potential (ERP) is one of the EEG reading that I want to capture and analyse to retrieve any private information.
- Smartphone application: The Application Programming Interface (API) is one of the significant factors that leads to the sniffing of the data through the data exchange between the application and the hardware. I want to examine the log files generated by the Smartphone application to find relevant information regarding the communication.

3.2.2 Research Question

The literature reviewed in Chapter 2 presents information that indicates that there are numerous privacy and security issues with the use of brain computer interfaces (BCIs). The problems described in the literature review in Section 2.5 are summarized in Section 3.2.1 in order to shape a research question. The critical concerns are the security and the privacy issues with the use of BCIs suggests that there may be potential vulnerabilities with the transfer of data from the brainwear to a laptop or a computer. A comprehensive research question has been proposed to investigate the potential vulnerabilities. The research question is supported by sub questions to provide an in-depth analysis of the technical context.

Research Question: (RQ) *What are the security and privacy vulnerabilities for information in the use of Brain Computer Interface devices?*

Thus, the research goal of this thesis is to determine whether the data sent from the BCI can be captured and analyzed to interpret meaningful information. Therefore, to answer the research question, three sub-questions have been postulated:

Sub Question 1: (SQ1) *What data can be captured from a communication session between the BCI and the user interface?*

Sub Question 2: (SQ2) *How can the pairing authentication information be interpreted?*

Sub Question 3 **(SQ3)** *How can the pairing between the BCI and the smartphone application be jammed?*

Sub Question 4: (SQ4) *How can captured information be substituted for a manipulated information exchange?*

3.2.3 Hypotheses

A hypothesis has been generated from the research questions presented in Section 3.2.2.

Hypothesis: That the data transmitted from a consumer grade Brain Computer Interface to the end user cannot be captured.

This hypothesis has been selected to determine the potential vulnerabilities in the use of brain computer interface.

3.2.3 Data Map

Figure 3.3 presents the interrelationships between different components of the proposed research methodology. The research question with the sub-questions summarized in

Section 3.2.2 are shown in the data map in Figure 3.3. Finally, the data collection phases have been linked to the hypothesis.

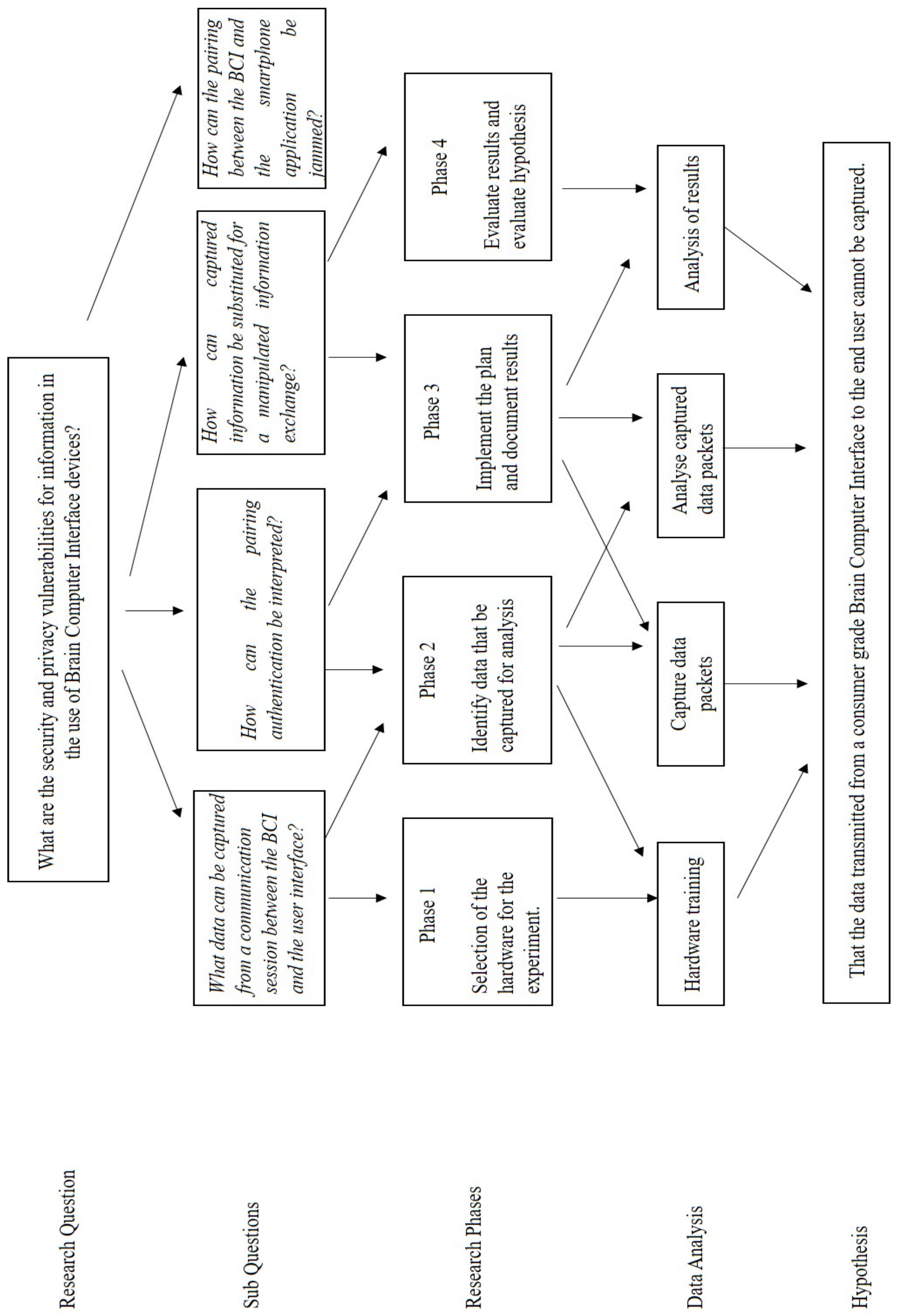

Research Question
What are the security and privacy vulnerabilities for information in the use of Brain Computer Interface devices?
Sub Questions
What data can be captured from a communication session between the BCI and the user interface?
How can the pairing authentication be interpreted?
How can captured information be substituted for a manipulated information exchange?
How can the pairing between the BCI and the smartphone application be jammed?
Research Phases
Phase 1
Selection of the hardware for the experiment.
Phase 2
Identify data that be captured for analysis
Phase 3
Implement the plan and document results
Phase 4
Evaluate results and evaluate hypothesis
Data Analysis
Hardware training
Capture data packets
Analyse captured data packets
Analysis of results
Hypothesis
That the data transmitted from a consumer grade Brain Computer Interface to the end user cannot be captured.

Figure 3.3 Data Map

3.3 DATA REQUIREMENTS

Information derived from Phase 1 of the research (see figure 3.3) will contribute to the selection of the required software and hardware platform for further additions and analysis. Secondly, Phase 2 includes the identification of the data to be captured and assertions leading to further plans to investigate the information captured. The results will be analyzed in Phase 3 with the evaluation of the results and the analysis in Phase 4. The strategy planned will provide a basis for postulating different methods to analyse the captured information. All the tests are conducted on the Emotiv Insight EEG headset to check the security of the transmission of data to the end user, as regulated by Phase 2 and 3. This is to simulate real life examples of individuals who use this EEG device for health monitoring from an entry level use to an extent where individuals can control a wheelchair or the movement of prosthetic arms, and so on.

This section describes the various facets of data requirements. The sub-sections include Data generation, data collection, data processing, data analysis, and data presentation. The details are presented briefly in sub-sections 3.3.1, 3.3.2, 3.3.3 and 3.3.4.

3.3.1 Data Generation

The data generation forms the backbone of the proposed research. I have initially chosen Wireshark to investigate the data as it offers an extensive platform to investigate information exchange with network devices. Not only does Wireshark enable sniffing of Internet data but also captures Bluetooth data. The capture of the Bluetooth data will be performed using the Ubertooth-one Bluetooth sniffer. The Ubertooth-one is an open source 2.4 GHz wireless development platform for Bluetooth experimentation developed by Michael Ossman in 2015. The Ubertooth-one is a sniffer capable of sniffing data exchange between two devices communicating in Bluetooth low energy. Furthermore, the Ubertooth-one sniffs the data flow passively and is capable of not only receiving but also transmitting data packets.

Bluetooth Low Energy (BTLE) is a recent standard of Bluetooth Special Interest Group (SIG). Also known as Bluetooth 4.0 and Bluetooth Smart, it is found in the majority of the Fitbit products, medical devices and other critical devices; to ensure longevity of the battery life. With the use of Ubertooth-one sniffer, data packets will be captured and saved as a PCAP file for a later examination in Wireshark to derive relevant information with the data. Although, Bluetooth 4.2 is available, it is generally not used because of the associated energy costs.

In addition, Wireshark can also capture Bluetooth Low Energy (BTLE) data which is going to be the prime filter to be used throughout this research. Wireshark is known to capture information such as pairing information. The pairing information in BTLE includes the exchange of a Temporary Key followed by the establishment of a Long Term Key (LTK). Once the LTK can be encrypted, the entire communication for that specific communication can be decrypted. Furthermore, additional tools such as Kismet, Spectools and CrackLE will be used for decrypting and examining the data packets captured through Wireshark. Kismet is a plugin used for network detection, sniffing traffic and intrusions detection systems (IDS). The essential feature for using Kismet in this research is the ability of the plugin to passively monitor and capture traffic. Kismet works with the Ubertooth-one as a plugin.

Spectools is a utility that provides a spectrum view of the network and communication being transmitted at 2.4 GHz. Finally, CrackLE will be used to decrypt BTLE packets captured by Wireshark. It exploits a fault in the Bluetooth low energy pairing that allows an intruder to guess or try to brute force the temporary key. After cracking the temporary key, it is possible to crack the LTK and further down the communication between the brainwear and the user interface, including the smartphone application.

3.3.2 Data collection

Once the hardware and the software tools to be tested have been determined, the collection of the data begins as per Phase 2. The initial stage of data collection would include the transmission pattern of the data from the Emotiv Insight to the end user. This analysis will help to understand the mode by which information is transmitted. It can later be examined using a network protocol analyser such as Wireshark. This captured data will be compared to the initial capture data to understand the underlying mechanism of data communication sent from the Emotiv Insight. Thus, the requirement of this stage is to determine if the captured data is to be tangible and to be useful for further investigation. The results will include BTLE packets, the advertising data, and the authentication of key exchange for secure connections.

After decrypting the LTK, the data captured will be investigated to interpret the packet containing the data for a mental command sent by the brainwear. Once the pattern of the packet is determined, then the Ubertooth-one will be used to transmit and inject a data packet into the stream of the data exchange between the brainwear and the user interface. In addition, the Ubertooth-one can fake a slave mode and trick the smartphone into believing the presence of genuine device and it also can be used as a source of interference to disturb on ongoing communication between the brainwear and the user interface.

3.3.3 Data Processing

The raw data generated by Ubertooth-one will be saved as PCAP and PCAPng files which will be imported into Wireshark to analyse the information transmitted and received by the Emotiv Insight EEG headset. To make meaningful interpretation of the data captured it will be related to the training and action of the user. This data will lead to the understanding of the method by which data is being transmitted from the EEG headset will also show the communication mechanism used by the EEG headset. Certain parameters which will be required for a successful decryption of the data will be the LL_ENC_REQ which is an encrypted requested sent from the brainwear to the smartphone. Additionally, the LL_ENC_RSP is also a significant data that needs to be captured in order for crackLE to decrypt the pairing key.

3.3.4 Data Analysis and Presentation

The data to be analyzed are the PCAP captured by Ubertooth-one. This analysis will help to gauge the information transmitted by the Emotiv Insight. This information includes the mental commands processed by the device and the triggers used by the Emotiv Insight headset. The results obtained from the analysis will be presented in a graphical form designed to showcase the interpretation of data sent and received during the communication session. The data packets will also be examined using CrackLE to find if there is any encrypted data which could be decrypted to obtain meaningful information. The resultant graphical presentation will indicate the means by which information is being transmitted between two devices operating on Bluetooth low energy.

The captured data will be initially processed to decrypt the encryption key used to decode the data sent from the brainwear to the user interface. The next series of tests will be conducted to determine the Bluetooth address of the headset. The information will lead to the transmission of manipulated packets. For packet injection in a Bluetooth connection, it is essential to determine the Lower Address Part which is the 24 bit address of the entire Bluetooth address. An example of Bluetooth Address is 11:22:33:44:55:66 where in 11:22 is considered to Non-significant Address part which is not required for this study. The Upper Address Part (UAP) 33 is to be determined from the Lower Address Part (LAP) which would be 44:55:66. The table 3.1 shows the different components of a Bluetooth address.

Table 3.1. Various components of a Bluetooth mac address

11:22	33	44:55:66
NAP	UAP	LAP

The Ubertooth-one will be used to determine the LAP address of the brainwear which can be achieved by the command Ubertooth-rx. The sniffer will start capturing all the data broadcasted by the brainwear. Determining the LAP and the UAP will provide a gateway to transmit data to that specific Bluetooth address. The results will be presented in a tabular format. There will be three tables containing a series of pcap files and the pairing information. The first table will contain all possible data including advertisement data and possible scanning request broadcasted by the brainwear. The second table will entail the Temporary Key and the Long-Term Key obtained from a few data packets containing the pairing information. The final table will include the data that will be injected in the data stream flowing to and from the brainwear and the user interface.

3.4 LIMITATIONS

The aim of this thesis is to determine the potential vulnerabilities with the use of Brain Computer Interfaces such as the Emotiv Insight. The capturing of data with respect to the Emotiv Insight poses limitations that define the scope of my thesis. There are a limited number of software tools available to test the feasibility of a BCI. Therefore, the tools that have been picked for this methodology have been adopted from open source and modified for individual use. The software chosen for this study have been determined on the basis of their functionality and the significance associated. The hardware Emotiv

Insight also presents limitations for the research as it has 5 channels and the data transmitted through the headset is minimal.

The prime reason to have chosen the Emotiv Insight is its common use amongst consumers rather than for research. The Emotiv Insight is aimed for consumer use and yet is relatively inexpensive and affordable for this research. The results derived from this study might be limited in terms of captured information but it does provide the technical issues associated with the use of this hardware. The data transmission is not secure and anyone owning a Bluetooth Low Energy Sniffer (BLE) will be able to sniff the communication passively. The limitation is the proximity of the attacker to cause harm but there are adjustments including aerial extension to the sniffer that can sniff data transmission from bigger distances. The experimental work has scope limitations but it can show that it is feasibility to cause harm to an individual depending on this brainwear for daily personal support.

3.4.1 Reliability

This sub-section assesses the reliability of the results obtained which may be affected by the limitations. The framework designed for testing the Emotiv Insight was derived chiefly through an analysis of similar studies. Martinovic et al. (2012) proposed a design for side channel attacks. The framework showed the feasibility of side channel attacks and information could be retrieved from the Brain Computer Interface. Though, the hardware setup used to perform the attack was different from this research, the attack model was similar. Furthermore, the threat model proposed by Rushanan et al. (2014) was also another adoption for this research. The model proposed for the attack is the telemetry interface, but the device tested is an implantable medical device whereas a noninvasive wearable device has been used in this thesis. The advertising and the pairing information can only be captured at specific channels which does pose challenges for data reproducibility but every time when the packet is captured along with the pairing challenges, the encryption is possible to be cracked. The captured files could only be examined by Wireshark as Wireshark is currently one of the versatile network protocol analyzer and supports analysis of Bluetooth Low Energy Packets. Though, Wireshark was the only tool prominently used to investigate the captured packets, the software has been peer reviewed and widely recommended for network analysis.

The results obtained using a different sniffing devices produced the same results ensuring that they have been constructed from the same content. This type of reliability metrics are established by parallel-forms for reliability estimators. These results can be correlated to examine the results for stability over time as instituted by this form of test-retest reliability.

3.4.2 Validity

The external validity is an important aspect in addition to the internal reliability for a research study. Validity ensures that the requirements for the research methodology have been followed during the generation of results. The Ubertooth-one has been used widely in research and the results obtained using this sniffer benchmarked to create a generalizability amongst the data populations. The results obtained using the Adafruit BLE sniffer and the Ubertooth-one can be replicated if used with the right versions of the software proposed for the testing. The Adafruit BLE sniffer works on a specific version of Wireshark (Ver 1.12). Similarly, the Adafruit one worked flawlessly on the Windows platform whereas the Ubertooth-one required a Linux platform specifically Kali Linux. The Btlejuice framework only worked on Ubuntu (Linux distribution). The drivers required for Btlejuice to run successfully had to be installed in a specific order. If installed correctly and in the order, the Btlejuice framework results can also be replicated.

There was interference from other devices operating at the 2.4 GHz, creating noise, but the isolated environment filtered the disruption. The tools and the research design proposed in Chapter 3 can be used as a benchmark to test future wearable devices as most wearable devices are still equipped with Bluetooth 4.0. The reason behind the implementation of Bluetooth 4.0 is that it provides cost effectiveness and longevity of the device resulting a huge compromise of information transferred to and from the Brain Computer Interface. In addition, the framework for testing the Emotiv Insight has proven beneficial to reveal the flaws for security for information and also shows the feasibility of various forms of attacks.

3.5 CONCLUSION

Chapter 3 provides an overview of the proposed research methodology for this study. Section 3.1 provides a review of similar studies that influenced the selection of methodology. Section 3.2 briefly outlines the research question, the sub-questions and the hypothesis. The research question has been derived from the challenges presented in Chapter 2. Subsequently, Sections 3.3 presents the data requirements for the research split in to various stages that include Data generation, Data collection, data processing and analysis. Furthermore, a data map has been presented in sub-section 3.2.3 connecting the essential components of this study. The data map also represents the interrelationships between various components thereby creating a research design for my thesis. Section 3.4 presents the limitations associated with this study. Chapter 4 will present the results of the study and the data analyzed will be reviewed based upon the methodological framework developed in Chapter 3.

CHAPTER 4
RESEARCH FINDINGS

4.0 INTRODUCTION

Chapter 3 has outlined the research methodology to investigate the privacy and security vulnerabilities in the use of a consumer grade Brain Computer Interface (BCI). Chapter 4 presents the findings derived by applying the methodology developed in Chapter 3. Section 4.1 identifies the variations between the proposed Chapter 3 specifications and the actual implementation of the research design. Section 4.2 describes the final hardware setup and the test bed for the experiment, and section 4.3 presents the experimental tests that gave the results. Section 4.4 presents the results with the analysis reported in section 4.5

4.1 VARIATIONS IN RESEARCH

It is unavoidable that several variations have been made during the implementation of the proposed methodology to make the testing work in practice. These variations are significant for reporting and were required in order to make the experiment function in practice. The variations are discussed with respect to data generation and data analysis. Section 4.1.1 and section 4.1.2 outline the specific variations.

4.1.1 Adafruit BLE Sniffer

The initial hardware chosen for sniffing the Bluetooth packets was the Adafruit BLE sniffer. Upon experimenting with the Adafruit sniffer, a limitation was observed that impacted the research objectives. The limitation identified was that the sniffer could not capture data if the Emotiv Insight was already paired with the smartphone application or the desktop interface. The experiment requires a sniffer that could capture Bluetooth packets in a promiscuous mode. Promiscuous mode is a capture device setting which enables Wireshark to sniff active connections between various devices. Hence, the Ubertooth-one was substituted as it was able to sniff an active and an ongoing communication between two Bluetooth Low Energy devices.

Figure 4.1 presents an image of the Adafruit BLE sniffer and figure 4.2 presents an image of an Ubertooth-one sniffer.

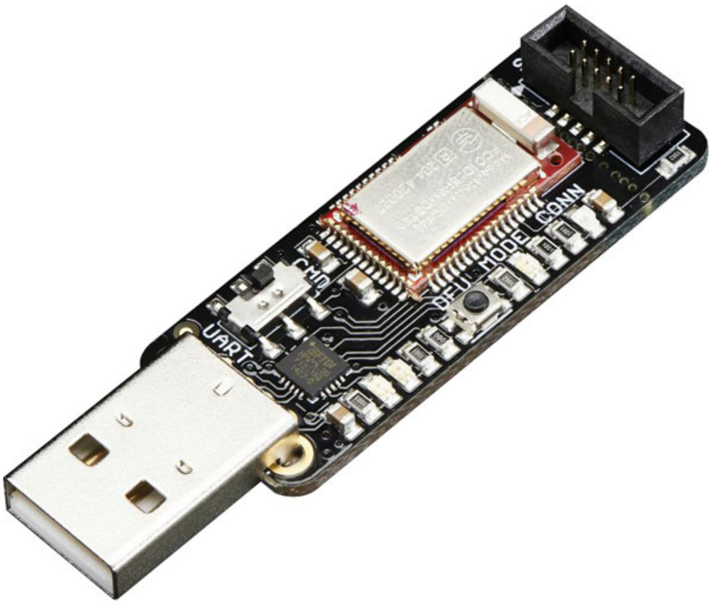


Figure 4.1 Adafruit BLE sniffer

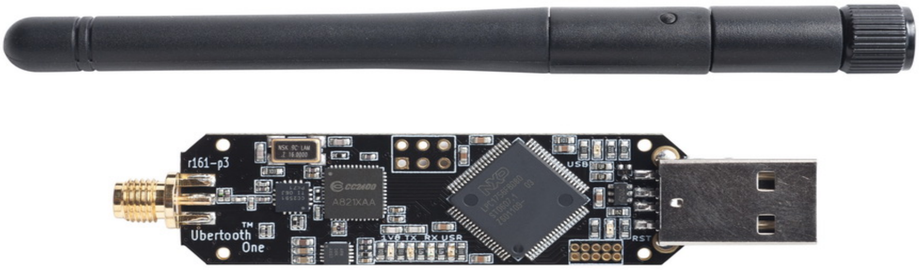


Figure 4.2 Ubertooth-one

4.1.2 Multiple Bluetooth dongles

The second variation that was made to the proposed methodology is the use of two additional Bluetooth dongles from Cambridge Silicon Radio (CSR 4.0). The Ubertooth-one can capture Bluetooth data passively and also interfere with an active connection but was not capable of injecting data packets back in to the data stream. The use of multiple

Bluetooth dongles facilitated a test of the Man-In-The-Middle (MITM) framework called Btlejuice developed by Cauqill (August 2016). The variation adopted enabled the performance of replay attacks and on-the-fly data modification.

4.2 HARDWARE SETUP

In order to successfully implement the research methodology, the hardware setup was identified as the most important facet of this thesis. Apart from the Emotiv Insight EEG headset, there were two laptops used for the experiment. Both the laptops had a 4GB DDR3 RAM with i5 processors. One of the laptops was running Windows 10 and Ubuntu 16.04 and the other laptop was running Ubuntu 16.04 and KALI Linux 2017 dual boot. In addition to the laptops, two Bluetooth sniffers were deployed to capture Bluetooth data, the Adafruit BLE sniffer and the Ubertooth-one. Also, two Bluetooth dongles CSR 4.0 version have also been used. Figure 4.3 presents an image of the hardware setup for this thesis.

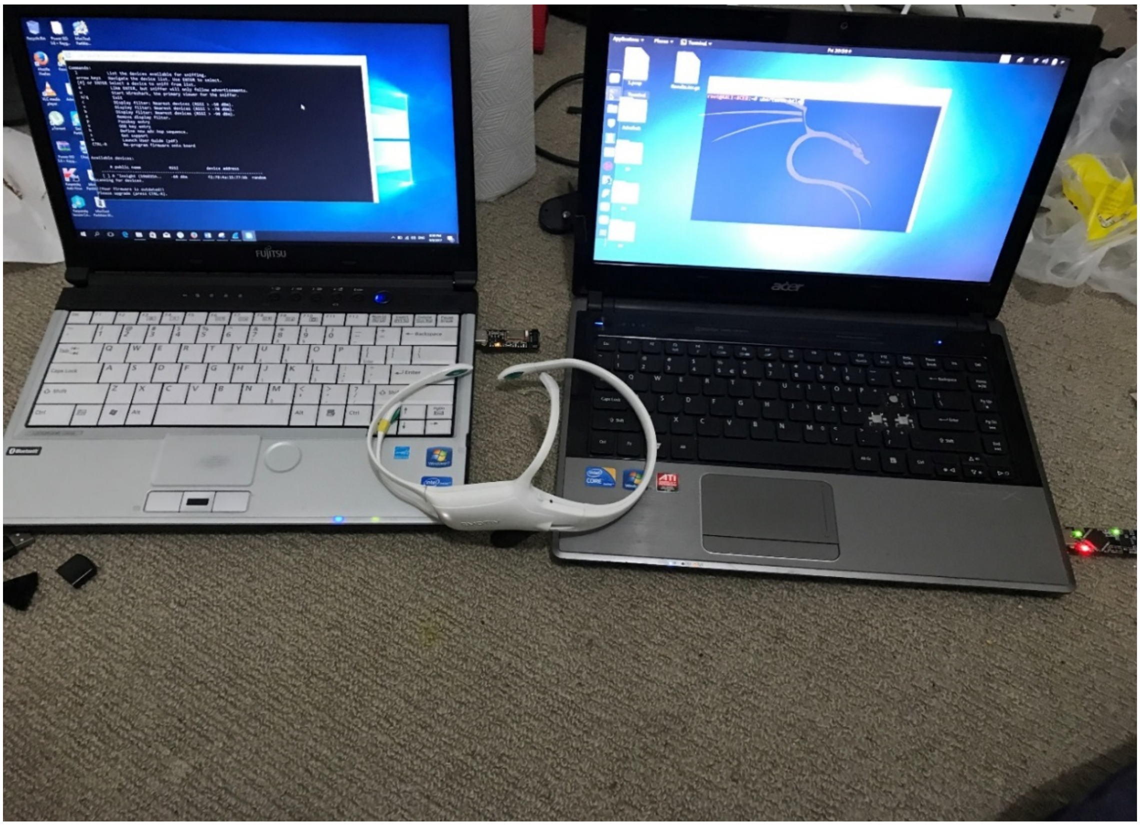


Figure 4.3 Hardware setup for the experiment

4.3 EXPERIMENTAL DESIGN

The experimental design for this thesis was implemented to obtain the pairing information, to sniff active and ongoing communication and to then try to modify the data captured. This section is divided into two sub sections. Section 4.3.1 describes the Bluetooth protocol stack used, and Section 4.3.2 describes the key elements required for the successful derivation of the results.

4.3.1 Bluetooth Protocol Stack

The Bluetooth protocol stack presented in Figure 4.4 specifies the presentation of data and the separation of the data in its layers when it was captured. The stack allows planning and analysis in the experimental design for both control and the development of meaningful information.

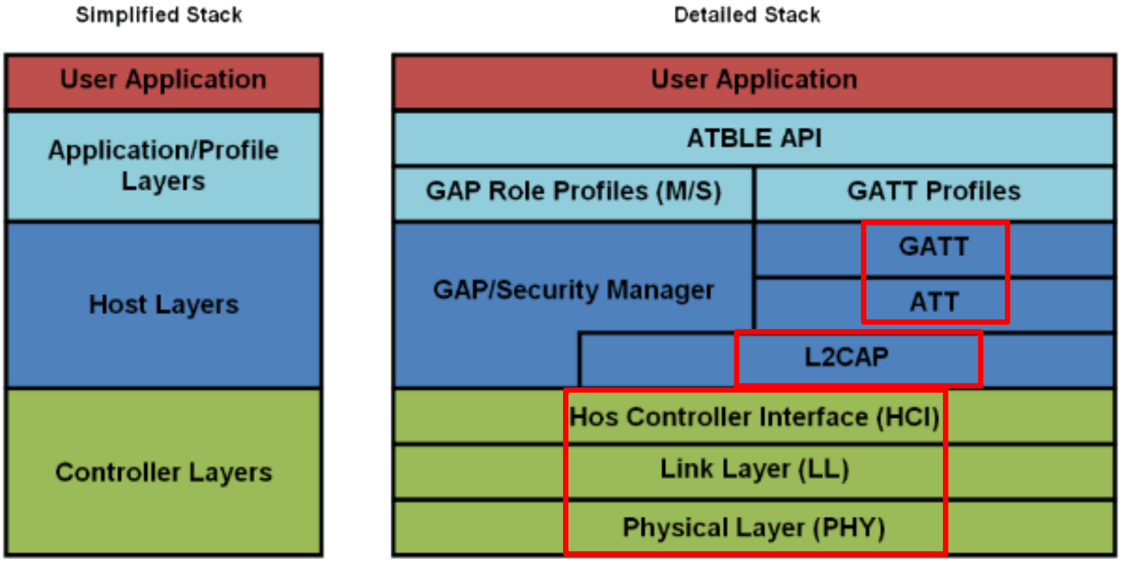


Figure 4.4 Bluetooth Protocol Stack (Chang, 2014)

The plan for the experiment is designed to reverse engineer the data from the Physical Layer (PHY), Link Layer (LL), L2CAP, Security Manager Protocol (SMP), Attribute (ATT) and Generic Attribute Profile (GATT). GATT is the application layer that connects the Bluetooth Low Energy device to the smartphone application. SMP manages the key exchange information including the cryptographic mechanism behind the pairing of the Bluetooth device to the smartphone.

4.3.2 Key Requirements

This section presents the key requirements for the successful implementation of the research design. The key selections made are described as follow:

- Emotiv Insight: The data transmitted from the headset is one of the most essential requirements. The headset sends digital commands to the application on the smartphone for capture.
- Adafruit BLE sniffer: The sniffer enables the sniffing of the Bluetooth data broadcasted by the Emotiv Insight headset.
- Ubertooth-One: The sniffer attempts the capture the pairing information and is used to cause interference between the smartphone application and the brainware.
- CSR 4.0: Cambridge Silicon Radio Bluetooth dongles version 4.0 is used to spoof the mac address of the laptop. Two dongles are employed of which one dongle connects to the application acting as the brainware whereas the other dongle is used as a relaying bridge to communicate the data back to the headset.
- Btlejuice: The MITM framework which enables active interception and data modification if correctly installed. Btlejuice is a program scripted in Java which needs to be installed on both the laptops. One laptop runs the Btlejuice proxy and the other laptop runs the websocket layer for intercepting the data exchange between the smartphone application and the brainware.
- Btlejuice-proxy: One of the laptops needs the Btlejuice proxy to be running continuously, further enabling the other laptop to connect to the proxy and bridge the communication between the two laptops through the Bluetooth dongles.
- Wireshark: The latest version of Wireshark supports the Bluetooth Low Energy plugins. For the Adafruit BLE sniffer to function effectively, Wireshark 1.12 needs to be installed. Furthermore, Wireshark is deployed to capture the pairing information and the exchange of the Long Term Key (LTK).
- GATT: Generic Attribute Profile or GATT is the application layer of the Bluetooth protocol stack. The GATT data contains all exclusive signals exchanged between the application and the brainware. The GATT data defines the way information is transferred back and forth in a Bluetooth Low Energy device. The brainware is the GATT server which holds the ATT lookup data and the services associated with it whereas the smartphone is the GATT client which sends request to the server.
- LTK: The communication for Bluetooth connection is a 128-bit AES CCM security. The initial connection begins with the peripheral broadcasting the data, exchanging the Short Term Key (STK) to establish the exchange of the Long-

Term Key (LTK). Once the LTK is exchanged, a secure connection is created between the peripheral and the central device.

Bluetooth communication usually takes place in the 2.4 GHz spectrum. This spectrum has a total of 40 channels. Of the 40 channels, 37 channels are data channels and 3 are advertising channels. Figure 4.5 presents a screenshot of the Bluetooth low energy channels and the wireless channels.

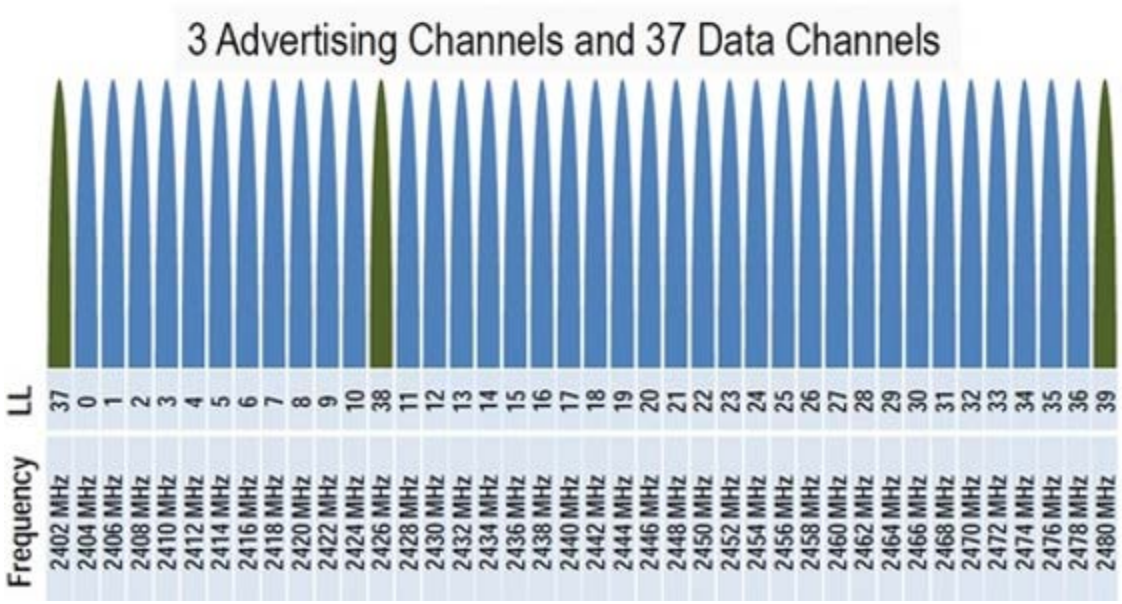


Figure 4.5 Bluetooth Low Energy Channels (Chang, 2014)

Once the connection is established between the brainware and the smartphone application, the smartphone informs the brainware of the hopping sequence and subsequent exchange of data is performed over the 37 channels. It takes about 3 ms for a data transfer to be completed. The important parameters include CONNECT_REQ, LL_ENC_CONNECT_REQ, LL_UPDATE_REQ and LL_TERMINATE. These are exchanged and Ubertooth one is used to capture them. Figure 4.6 presents a flow of the message exchange between the Bluetooth Low Energy device and the smartphone.

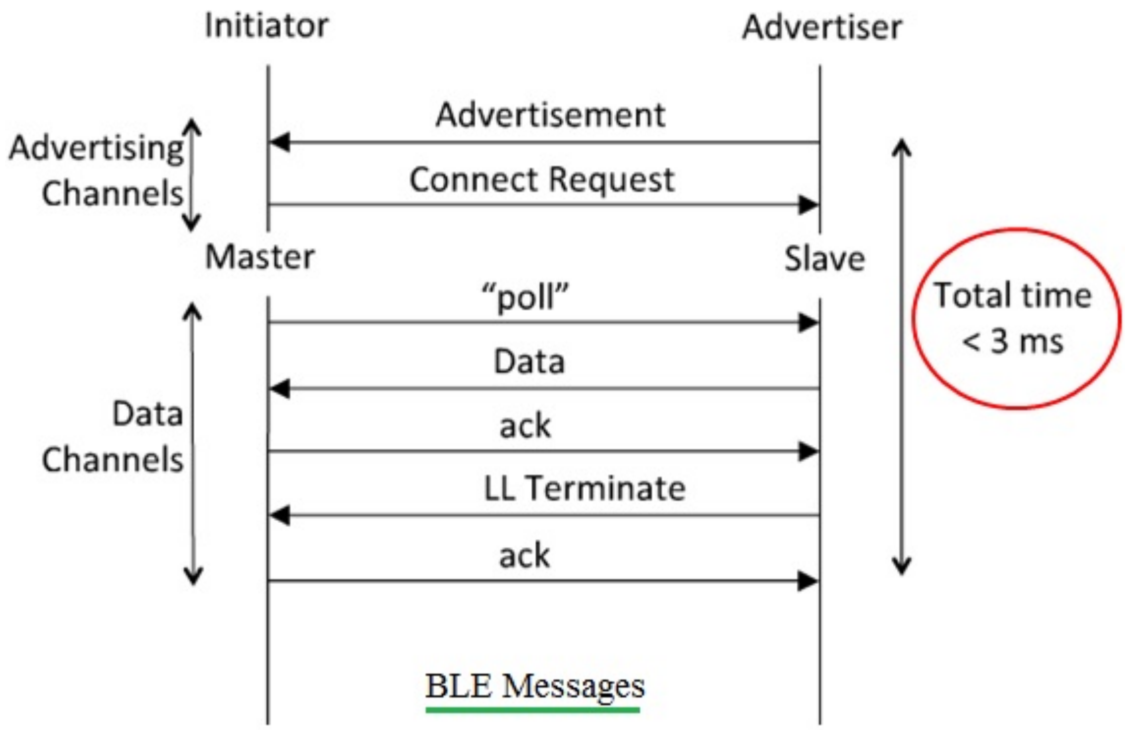


Figure 4.6 Bluetooth Low Energy message exchange

The first test results included the data obtained from the Adafruit BLE sniffer followed by the second test results obtained using the Ubertooth-one. Finally, the last test included the MITM framework using the two Bluetooth dongles. The Ubertooth-one will be used to capture active communications passively, interfere with an ongoing connection and determine the encryption keys exchanged during the pairing mechanism. Finally, Btlejuice is used to capture the GATT, the application layer data, and check the feasibility for a replay attack or data modification.

4.4 RESULTS

Section 4.4.1 presents the results obtained through the implementation of the methodology that has been outlined in Chapter 3 and the variations noted above. Section 4.4 is divided into three sub-sections. Section 4.4.1 describes the results obtained using the Adafruit BLE Sniffer. Section 4.4.2 presents the results derived using the Ubertooth-one sniffer. Section 4.4.3 presents the results using the Btlejuice framework for performing a replay attack and the Man In The Middle (MITM) attack.

4.4.1 Adafruit BLE Sniffer

Section 4.4.1 presents the Bluetooth data captured by the Adafruit BLE sniffer. The Adafruit BLE sniffer runs on all platforms including Windows, Linux and Macintosh. The version for Windows is the most stable. After downloading the executable file blesniffer.exe from the Adafruit directory, a command terminal is presented which shows the list of active Bluetooth devices. Figure 4.7 presents a screenshot of the two LED lights on the Adafruit BLE sniffer showing the connection lights. The blue light indicates the Bluetooth is active on the device and is searching for nearby devices. The orange light indicates the device capturing live packets from the assigned device to be sniffed. The blue light goes on to prove that the device is active throughout the experiment and the orange light shows that data can be captured from a Bluetooth Low Energy device, in this case the Insight headset.

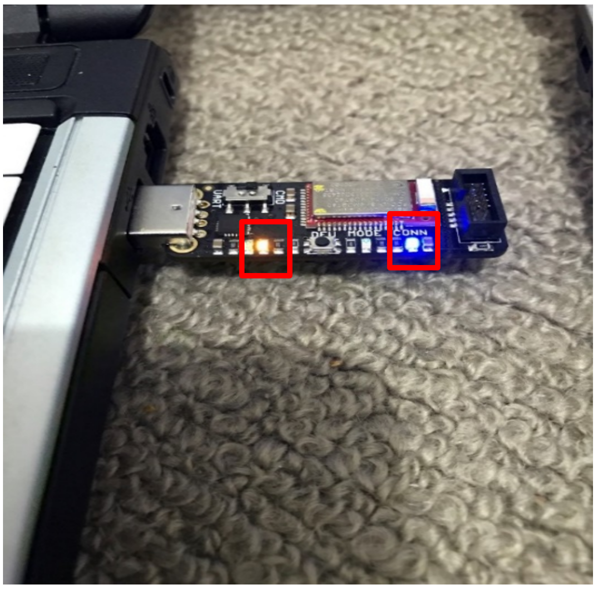
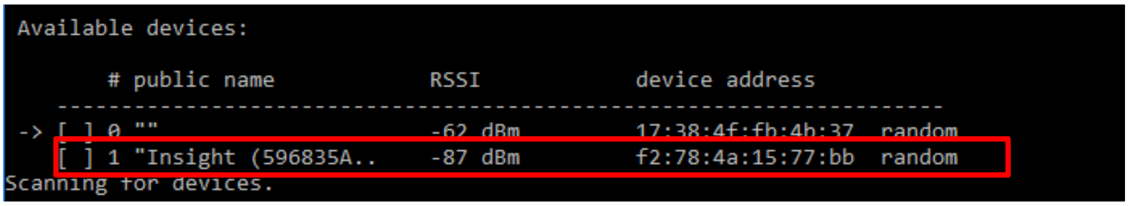


Figure 4.7 Adafruit BLE sniffer connection LED

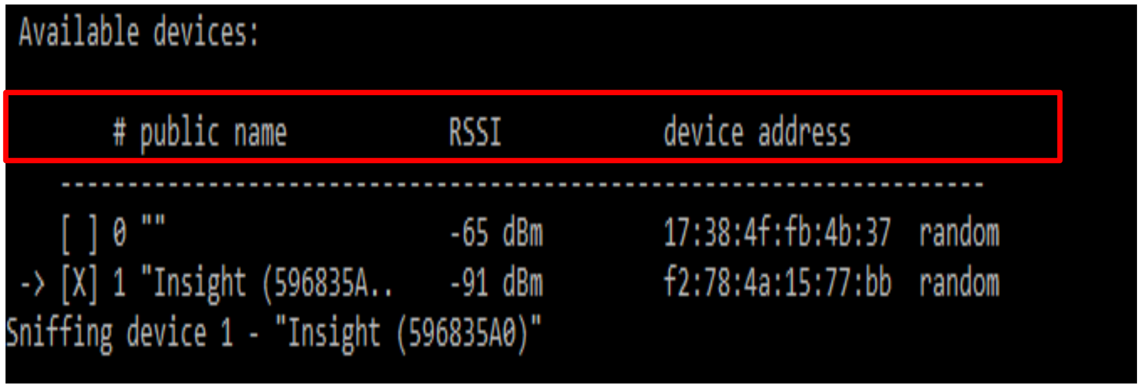
Figure 4.8 presents a screenshot of the command that identifies the Insight headset and the mac address of the device.



```
Available devices:

      # public name           RSSI            device address
   ------------------------------------------------------------------
-> [ ] 0 ""                   -62 dBm         17:38:4f:fb:4b:37  random
   [ ] 1 "Insight (596835A..  -87 dBm         f2:78:4a:15:77:bb  random
Scanning for devices.
```

Figure 4.8 Insight headset with the Bluetooth address

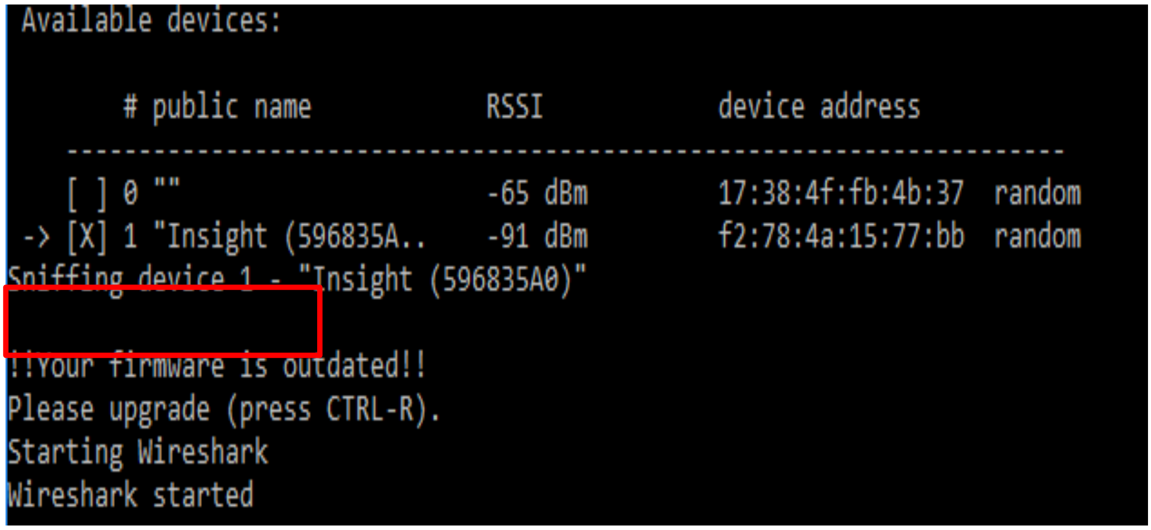
Figure 4.8 shows available devices for which the Insight headset is highlighted and with the Bluetooth mac address f2:78:4a:15:77:bb. Figure 4.9 presents a screenshot where the Insight device is selected and is ready to be sniffed. In addition, the message also confirms that the Insight has been selected for sniffing data.



```
Available devices:

     # public name             RSSI          device address
  ------------------------------------------------------------------
  [ ] 0 ""                     -65 dBm       17:38:4f:fb:4b:37  random
-> [X] 1 "Insight (596835A..   -91 dBm       f2:78:4a:15:77:bb  random
Sniffing device 1 - "Insight (596835A0)"
```

Figure 4.9 Insight headset selected to be sniffed

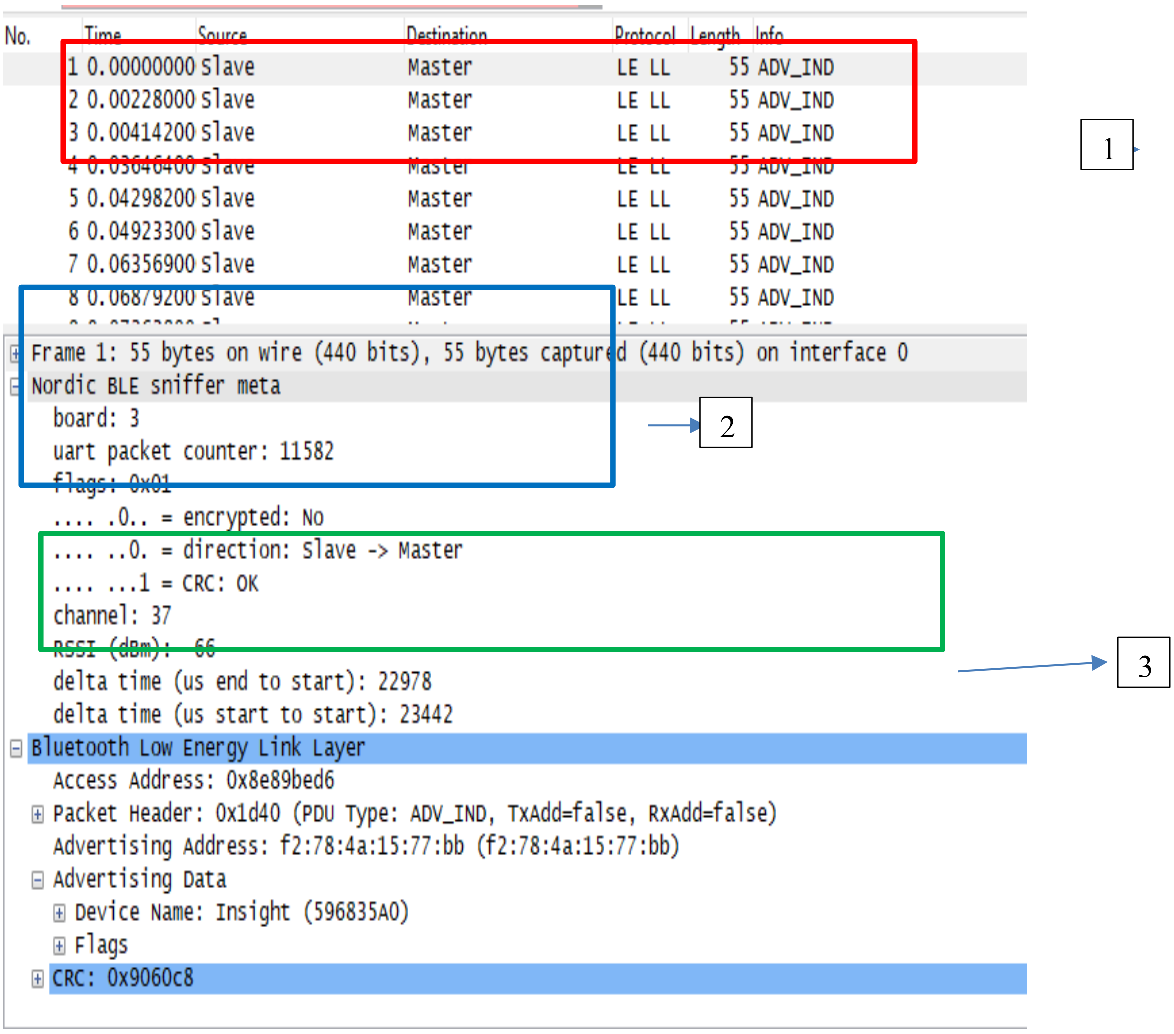
After selecting the device, the Wireshark application was used to start the dumping of captured Bluetooth data into a format that could be analyzed. Figure 4.10 presents a screenshot of the command terminal launching the Wireshark application.



```
Available devices:

     # public name             RSSI          device address
  ------------------------------------------------------------------
  [ ] 0 ""                     -65 dBm       17:38:4f:fb:4b:37  random
-> [X] 1 "Insight (596835A..   -91 dBm       f2:78:4a:15:77:bb  random
Sniffing device 1 - "Insight (596835A0)"

!!Your firmware is outdated!!
Please upgrade (press CTRL-R).
Starting Wireshark
Wireshark started
```

Figure 4.10 Command terminal launching Wireshark

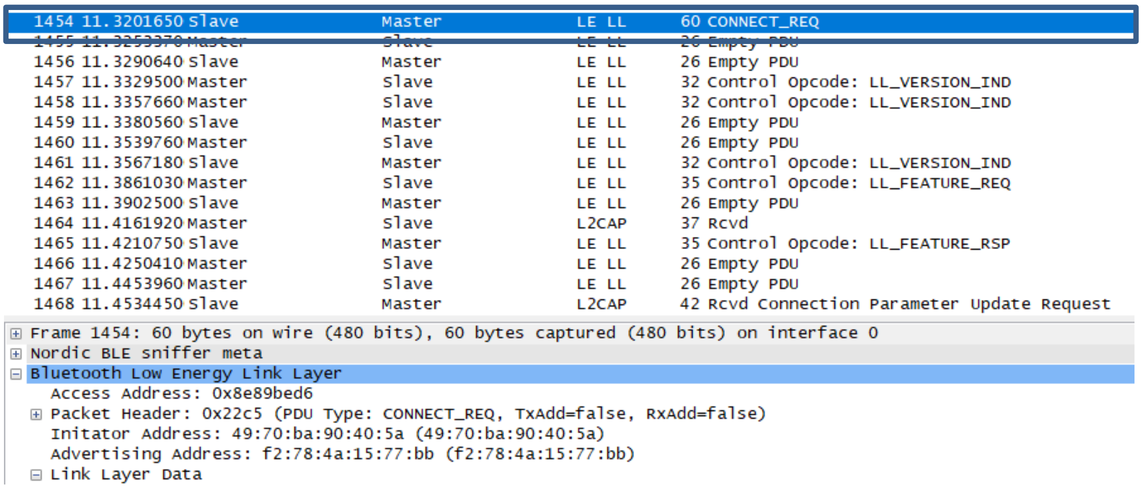
Wireshark identified data being captured by the Adafruit BLE sniffer. In this instance, the data captured by the Adafruit BLE sniffer is the advertising data broadcasted by the Insight headset. Figure 4.10 presents a screenshot of the Wireshark window showing advertising data transmitted by the Insight headset.



```
No.   Time        Source   Destination   Protocol  Length  Info
    1 0.00000000 Slave    Master        LE LL       55 ADV_IND
    2 0.00228000 Slave    Master        LE LL       55 ADV_IND
    3 0.00414200 Slave    Master        LE LL       55 ADV_IND
    4 0.03646400 Slave    Master        LE LL       55 ADV_IND
    5 0.04298200 Slave    Master        LE LL       55 ADV_IND
    6 0.04923300 Slave    Master        LE LL       55 ADV_IND
    7 0.06356900 Slave    Master        LE LL       55 ADV_IND
    8 0.06879200 Slave    Master        LE LL       55 ADV_IND

⊞ Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
⊟ Nordic BLE sniffer meta
    board: 3
    uart packet counter: 11582
    flags: 0x01
    .... .0.. = encrypted: No
    .... ..0. = direction: Slave -> Master
    .... ...1 = CRC: OK
    channel: 37
    RSSI (dBm): -66
    delta time (us end to start): 22978
    delta time (us start to start): 23442
⊟ Bluetooth Low Energy Link Layer
    Access Address: 0x8e89bed6
  ⊞ Packet Header: 0x1d40 (PDU Type: ADV_IND, TxAdd=false, RxAdd=false)
    Advertising Address: f2:78:4a:15:77:bb (f2:78:4a:15:77:bb)
  ⊟ Advertising Data
    ⊞ Device Name: Insight (596835A0)
    ⊞ Flags
  ⊞ CRC: 0x9060c8
```

Figure 4.11 Wireshark window showing the advertising data

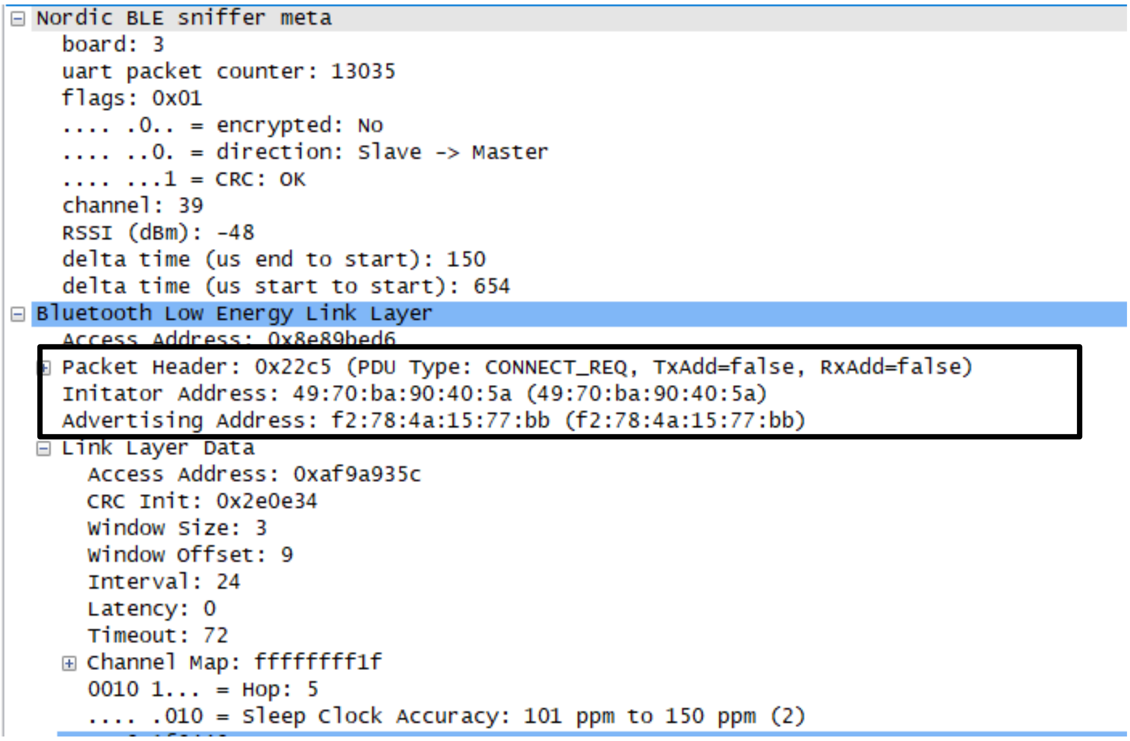
Figure 4.11 presents different tabs in Wireshark. The red tab displays the advertising data broadcasted by the Insight headset that includes the physical layer (PHY) and the Link Layer (LL). The blue tab shows the meta data captured by the sniffer. The green tab shows the Bluetooth address of the Insight headset and confirms the advertising data is being transmitted from the headset. Figure 4.12 presents a screenshot of the Wireshark window with the CONNECT_REQ parameter, contained with the red outline. The CONNECT_REQ is one of the important parameters that is required for a successful pairing between two devices. CONNECT_REQ is a request initiated by the smartphone application to the brainware by displaying its services and characteristics. Figure 4.13 presents a screenshot of the entire CONNECT_REQ window. This window displays various components.



```
1454 11.3201650 Slave          Master        LE LL      60 CONNECT_REQ
1455 11.3253370 Master         Slave         LE LL      26 Empty PDU
1456 11.3290640 Slave          Master        LE LL      26 Empty PDU
1457 11.3329500 Master         Slave         LE LL      32 Control Opcode: LL_VERSION_IND
1458 11.3357660 Master         Slave         LE LL      32 Control Opcode: LL_VERSION_IND
1459 11.3380560 Slave          Master        LE LL      26 Empty PDU
1460 11.3539760 Master         Slave         LE LL      26 Empty PDU
1461 11.3567180 Slave          Master        LE LL      32 Control Opcode: LL_VERSION_IND
1462 11.3861030 Master         Slave         LE LL      35 Control Opcode: LL_FEATURE_REQ
1463 11.3902500 Slave          Master        LE LL      26 Empty PDU
1464 11.4161920 Master         Slave         L2CAP      37 Rcvd
1465 11.4210750 Slave          Master        LE LL      35 Control Opcode: LL_FEATURE_RSP
1466 11.4250410 Master         Slave         LE LL      26 Empty PDU
1467 11.4453960 Master         Slave         LE LL      26 Empty PDU
1468 11.4534450 Slave          Master        L2CAP      42 Rcvd Connection Parameter Update Request
⊞ Frame 1454: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Nordic BLE sniffer meta
⊟ Bluetooth Low Energy Link Layer
    Access Address: 0x8e89bed6
  ⊞ Packet Header: 0x22c5 (PDU Type: CONNECT_REQ, TxAdd=false, RxAdd=false)
    Initator Address: 49:70:ba:90:40:5a (49:70:ba:90:40:5a)
    Advertising Address: f2:78:4a:15:77:bb (f2:78:4a:15:77:bb)
  ⊟ Link Layer Data
```

Figure 4.12 Wireshark window showing CONNECT_REQ

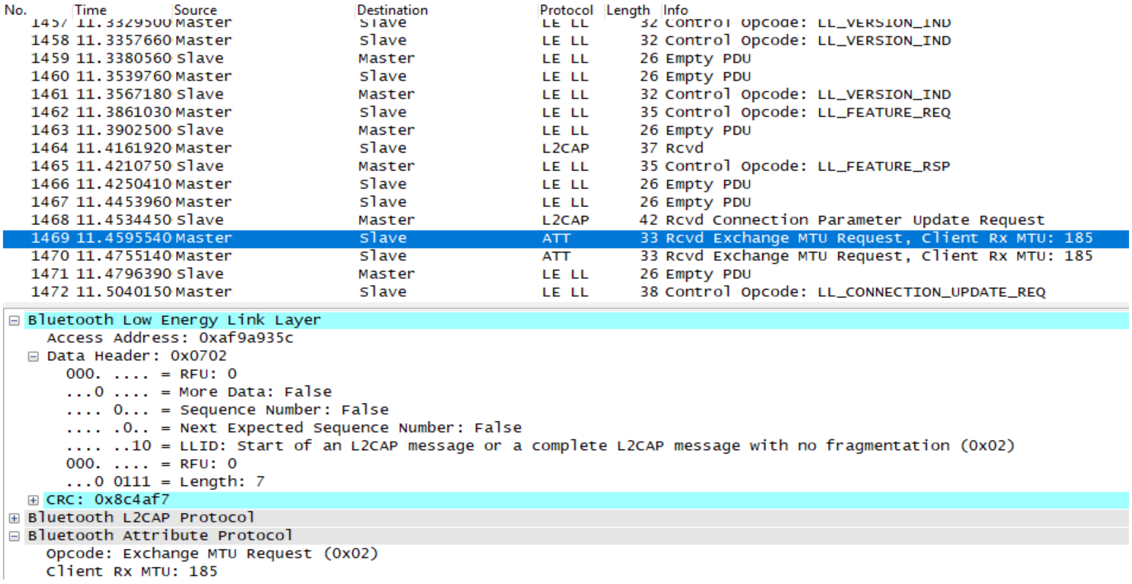
Figure 4.13 shows a screenshot of the expanded CONNECT_REQ window information. This window shows the pairing request has been initiated by the smartphone identified by the mac address. The CONNECT_REQ is sent as Protocol Data Unit (PDU) from the smartphone to the Insight headset.



```
⊟ Nordic BLE sniffer meta
    board: 3
    uart packet counter: 13035
    flags: 0x01
    .... .0.. = encrypted: No
    .... ..0. = direction: Slave -> Master
    .... ...1 = CRC: OK
    channel: 39
    RSSI (dBm): -48
    delta time (us end to start): 150
    delta time (us start to start): 654
⊟ Bluetooth Low Energy Link Layer
    Access Address: 0x8e89bed6
  ⊞ Packet Header: 0x22c5 (PDU Type: CONNECT_REQ, TxAdd=false, RxAdd=false)
    Initator Address: 49:70:ba:90:40:5a (49:70:ba:90:40:5a)
    Advertising Address: f2:78:4a:15:77:bb (f2:78:4a:15:77:bb)
  ⊟ Link Layer Data
      Access Address: 0xaf9a935c
      CRC Init: 0x2e0e34
      Window Size: 3
      Window Offset: 9
      Interval: 24
      Latency: 0
      Timeout: 72
    ⊞ Channel Map: ffffffff1f
      0010 1... = Hop: 5
      .... .010 = Sleep Clock Accuracy: 101 ppm to 150 ppm (2)
```

Figure 4.13 CONNECT_REQ window

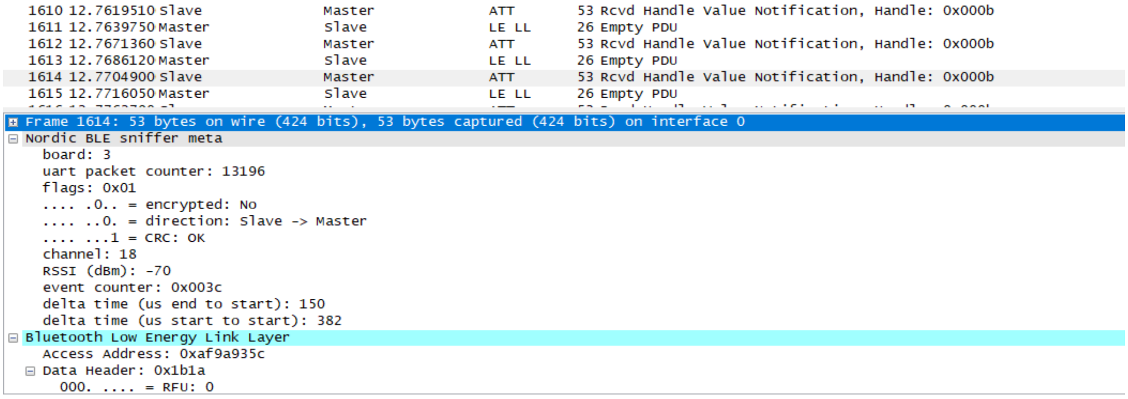
Figure 4.14 presents a screenshot of the Attribute (ATT) layer. The information indicates that the credentials have been exchanged and the connection has been established on both the devices, the smartphone and the brainware. The highlighted frame in the screenshot indicates the Maximum Transmission Unit (MTU) for the Bluetooth connection. The MTU payload length is for the particular transmission media.



```
No.     Time       Source            Destination       Protocol  Length  Info
   1457 11.3329500 Master            Slave             LE LL        32 Control Opcode: LL_VERSION_IND
   1458 11.3357660 Master            Slave             LE LL        32 Control Opcode: LL_VERSION_IND
   1459 11.3380560 Slave             Master            LE LL        26 Empty PDU
   1460 11.3539760 Master            Slave             LE LL        26 Empty PDU
   1461 11.3567180 Slave             Master            LE LL        32 Control Opcode: LL_VERSION_IND
   1462 11.3861030 Master            Slave             LE LL        35 Control Opcode: LL_FEATURE_REQ
   1463 11.3902500 Slave             Master            LE LL        26 Empty PDU
   1464 11.4161920 Master            Slave             L2CAP        37 Rcvd
   1465 11.4210750 Slave             Master            LE LL        35 Control Opcode: LL_FEATURE_RSP
   1466 11.4250410 Master            Slave             LE LL        26 Empty PDU
   1467 11.4453960 Master            Slave             LE LL        26 Empty PDU
   1468 11.4534450 Slave             Master            L2CAP        42 Rcvd Connection Parameter Update Request
   1469 11.4595540 Master            Slave             ATT          33 Rcvd Exchange MTU Request, Client Rx MTU: 185
   1470 11.4755140 Master            Slave             ATT          33 Rcvd Exchange MTU Request, Client Rx MTU: 185
   1471 11.4796390 Slave             Master            LE LL        26 Empty PDU
   1472 11.5040150 Master            Slave             LE LL        38 Control Opcode: LL_CONNECTION_UPDATE_REQ

⊟ Bluetooth Low Energy Link Layer
    Access Address: 0xaf9a935c
  ⊟ Data Header: 0x0702
      000. .... = RFU: 0
      ...0 .... = More Data: False
      .... 0... = Sequence Number: False
      .... .0.. = Next Expected Sequence Number: False
      .... ..10 = LLID: Start of an L2CAP message or a complete L2CAP message with no fragmentation (0x02)
      000. .... = RFU: 0
      ...0 0111 = Length: 7
  ⊞ CRC: 0x8c4af7
⊞ Bluetooth L2CAP Protocol
⊟ Bluetooth Attribute Protocol
    Opcode: Exchange MTU Request (0x02)
    Client Rx MTU: 185
```

Figure 4.14 Pairing confirmation request

Figure 4.15 presents a screenshot of the ATT layer which shows the raw data pushed to the Generic Attribute (GATT), the top most layer of the Bluetooth protocol stack. All the data transmitted between the headset and the smartphone application is not encrypted.



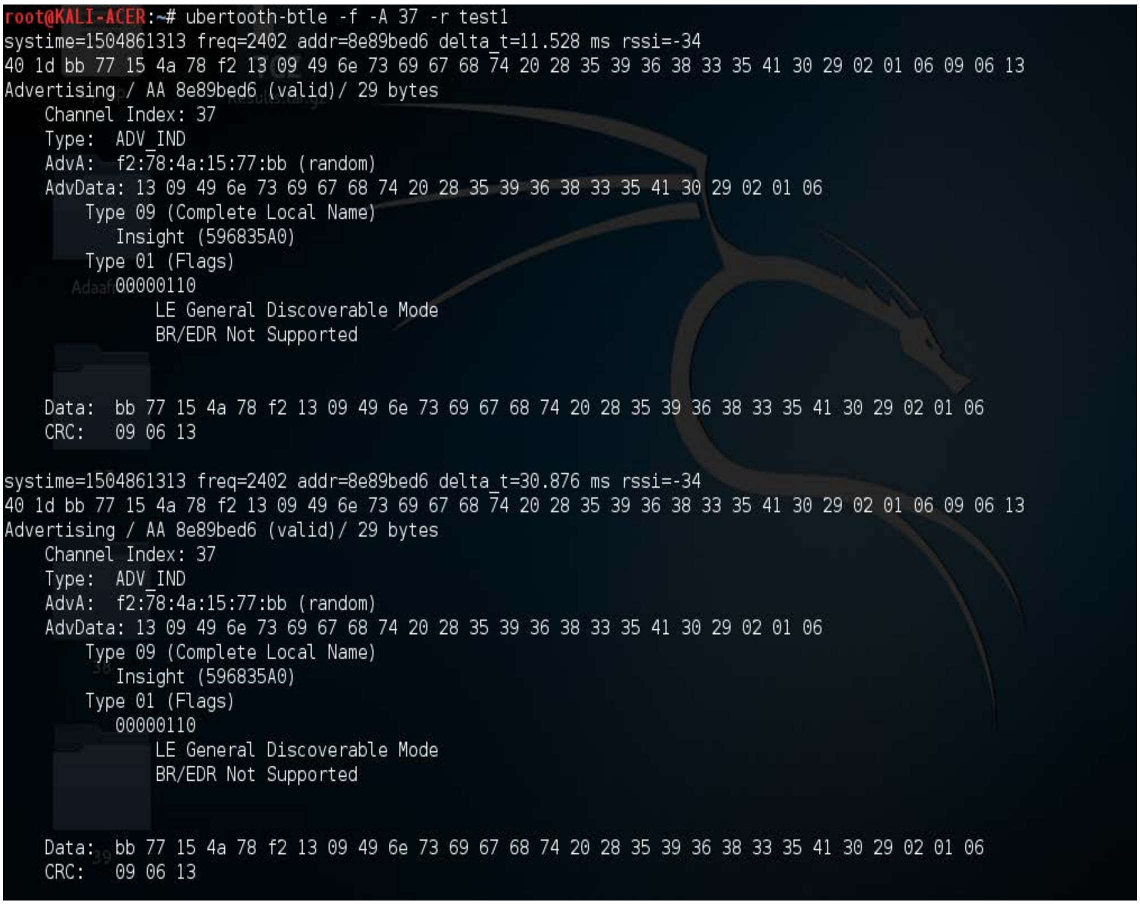
```
   1610 12.7619510 Slave             Master            ATT          53 Rcvd Handle Value Notification, Handle: 0x000b
   1611 12.7639750 Master            Slave             LE LL        26 Empty PDU
   1612 12.7671360 Slave             Master            ATT          53 Rcvd Handle Value Notification, Handle: 0x000b
   1613 12.7686120 Master            Slave             LE LL        26 Empty PDU
   1614 12.7704900 Slave             Master            ATT          53 Rcvd Handle Value Notification, Handle: 0x000b
   1615 12.7716050 Master            Slave             LE LL        26 Empty PDU

⊞ Frame 1614: 53 bytes on wire (424 bits), 53 bytes captured (424 bits) on interface 0
⊟ Nordic BLE sniffer meta
    board: 3
    uart packet counter: 13196
    flags: 0x01
    .... .0.. = encrypted: No
    .... ..0. = direction: Slave -> Master
    .... ...1 = CRC: OK
    channel: 18
    RSSI (dBm): -70
    event counter: 0x003c
    delta time (us end to start): 150
    delta time (us start to start): 382
⊟ Bluetooth Low Energy Link Layer
    Access Address: 0xaf9a935c
  ⊟ Data Header: 0x1b1a
      000. .... = RFU: 0
```

Figure 4.15 ATT layer of the data transmission

The Adafruit BLE sniffer was capable of capturing data when the headset was not paired with the smartphone but once it was connected only partial data could be captured. The data capturing process fluctuated when the headset was connected and then stopped completely. In order to capture active data transmission, a second Bluetooth sniffing device, the Ubertooth-one was deployed. Section 4.4.2 gives the results derived using the Ubertooth-one

4.4.2 Ubertooth-one

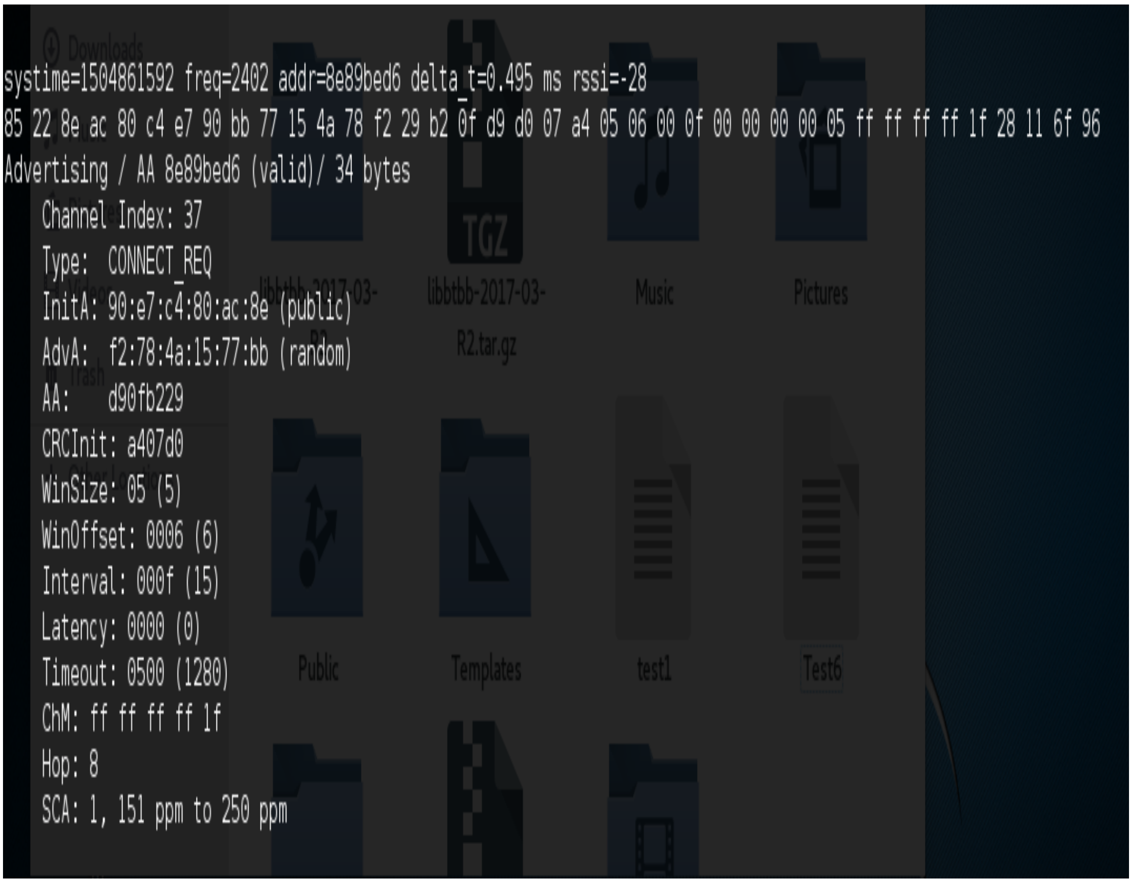
The Adafruit BLE sniffer could only capture connection data to a limited extent. The capturing process halted upon the device connection. Furthermore, the Adafruit BLE sniffer was not able to capture the Long-Term Key (LTK). The Ubertooth-one was found to be the most effective Bluetooth sniffer and was capable of capturing promiscuous connection information. The Ubertooth-one has been used to capture an ongoing communication and decrypt the communication using the encryption key or the LTK. The exchange of encryption key takes place at 3 channels of the Bluetooth spectrum which are 37, 38 and 39. Initial tests were captured for specifically 37 and then the channel was changed as the Ubertooth-one can only listen to one channel at a time. Figure 4.16 presents a screenshot of the data captured from an ongoing communication between the Insight headset and the smartphone application.



```
root@KALI-ACER:~# ubertooth-btle -f -A 37 -r test1
systime=1504861313 freq=2402 addr=8e89bed6 delta_t=11.528 ms rssi=-34
40 1d bb 77 15 4a 78 f2 13 09 49 6e 73 69 67 68 74 20 28 35 39 36 38 33 35 41 30 29 02 01 06 09 06 13
Advertising / AA 8e89bed6 (valid)/ 29 bytes
    Channel Index: 37
    Type:  ADV_IND
    AdvA:  f2:78:4a:15:77:bb (random)
    AdvData: 13 09 49 6e 73 69 67 68 74 20 28 35 39 36 38 33 35 41 30 29 02 01 06
        Type 09 (Complete Local Name)
           Insight (596835A0)
        Type 01 (Flags)
           00000110
               LE General Discoverable Mode
               BR/EDR Not Supported


    Data:  bb 77 15 4a 78 f2 13 09 49 6e 73 69 67 68 74 20 28 35 39 36 38 33 35 41 30 29 02 01 06
    CRC:   09 06 13

systime=1504861313 freq=2402 addr=8e89bed6 delta_t=30.876 ms rssi=-34
40 1d bb 77 15 4a 78 f2 13 09 49 6e 73 69 67 68 74 20 28 35 39 36 38 33 35 41 30 29 02 01 06 09 06 13
Advertising / AA 8e89bed6 (valid)/ 29 bytes
    Channel Index: 37
    Type:  ADV_IND
    AdvA:  f2:78:4a:15:77:bb (random)
    AdvData: 13 09 49 6e 73 69 67 68 74 20 28 35 39 36 38 33 35 41 30 29 02 01 06
        Type 09 (Complete Local Name)
           Insight (596835A0)
        Type 01 (Flags)
           00000110
               LE General Discoverable Mode
               BR/EDR Not Supported


    Data:  bb 77 15 4a 78 f2 13 09 49 6e 73 69 67 68 74 20 28 35 39 36 38 33 35 41 30 29 02 01 06
    CRC:   09 06 13
```

Figure 4.16 Active communication captured using the Ubertooth-one

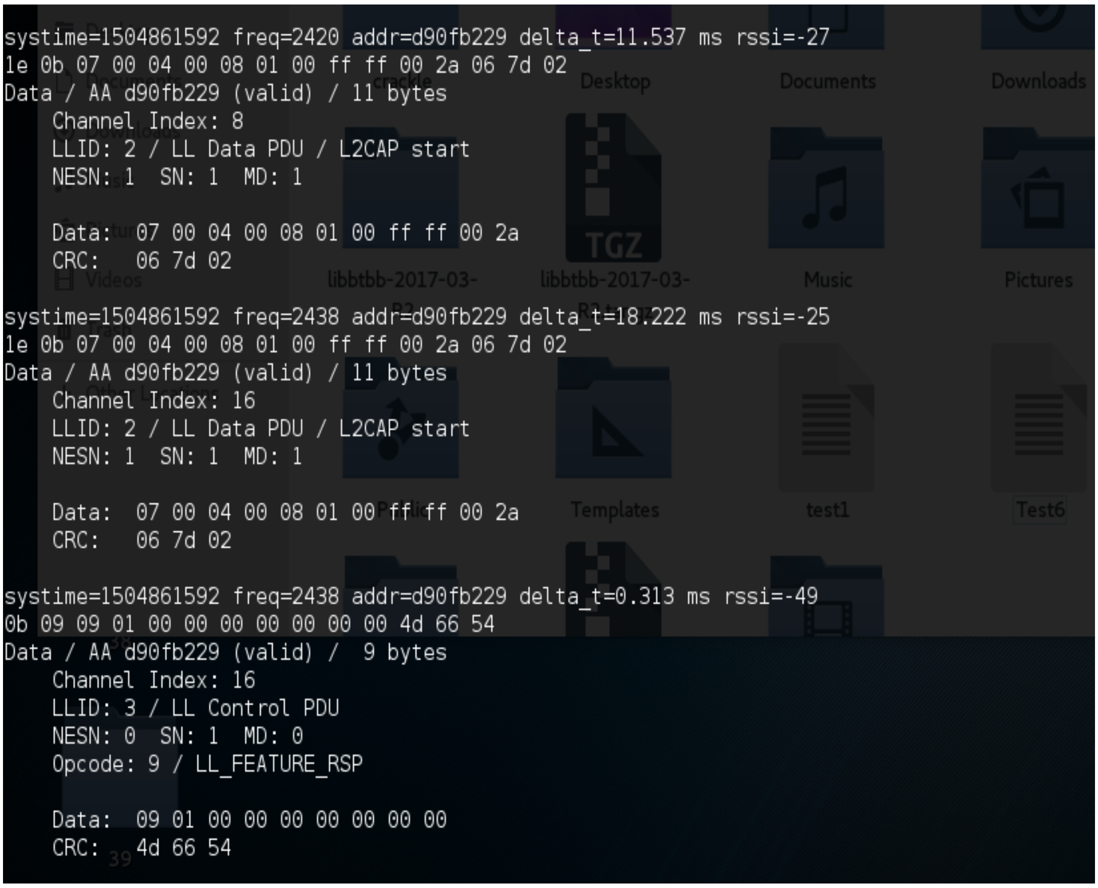
The result was displayed at the terminal which was also be dumped to a Wireshark file for later inspection. The command used to capture Bluetooth data was ubertooth-btle –f –A37|38|39 –r test1 wherein –f follows an active connection, -A sets the advertising channel of the Ubertooth-one which could be 37, 38 and 39; -r dumps the file into a pcapng file which can be later examined in Wireshark. Figure 4.17 presents a screenshot of the CONNECT_REQ initiated from the smartphone with the Bluetooth address 90:e7:c4:80:ac:8e attempting to connect to the Insight headset with the address f2:78:4a:15:77:bb. It can also be seen that the hop interval is 8 indicating that the information exchange will occur on the 8th channel from the CONNECT_REQ channel which is 37 in this case.



```
systime=1504861592 freq=2402 addr=8e89bed6 delta_t=0.495 ms rssi=-28
85 22 8e ac 80 c4 e7 90 bb 77 15 4a 78 f2 29 b2 0f d9 d0 07 a4 05 06 00 0f 00 00 00 00 05 ff ff ff ff 1f 28 11 6f 96
Advertising / AA 8e89bed6 (valid)/ 34 bytes
    Channel Index: 37
    Type:  CONNECT_REQ
    InitA: 90:e7:c4:80:ac:8e (public)
    AdvA:  f2:78:4a:15:77:bb (random)
    AA:    d90fb229
    CRCInit: a407d0
    WinSize: 05 (5)
    WinOffset: 0006 (6)
    Interval: 000f (15)
    Latency: 0000 (0)
    Timeout: 0500 (1280)
    ChM: ff ff ff ff 1f
    Hop: 8
    SCA: 1, 151 ppm to 250 ppm
```

Figure 4.17 Terminal showing CONNECT_REQ using Ubertooth-one

Figure 4.18 presents a screenshot of the active communication from the headset and the smartphone application in the L2CAP layer. The data is in the form of PDU. From the screenshot, the channel index is shown which is the specific channel for the data being transmitted. Furthermore, the data size is shown as 11 bytes, LLID which is the payload header and the Cyclic Redundancy Check (CRC) value.



```
systime=1504861592 freq=2420 addr=d90fb229 delta_t=11.537 ms rssi=-27
1e 0b 07 00 04 00 08 01 00 ff ff 00 2a 06 7d 02
Data / AA d90fb229 (valid) / 11 bytes
    Channel Index: 8
    LLID: 2 / LL Data PDU / L2CAP start
    NESN: 1  SN: 1  MD: 1

    Data:  07 00 04 00 08 01 00 ff ff 00 2a
    CRC:   06 7d 02

systime=1504861592 freq=2438 addr=d90fb229 delta_t=18.222 ms rssi=-25
1e 0b 07 00 04 00 08 01 00 ff ff 00 2a 06 7d 02
Data / AA d90fb229 (valid) / 11 bytes
    Channel Index: 16
    LLID: 2 / LL Data PDU / L2CAP start
    NESN: 1  SN: 1  MD: 1

    Data:  07 00 04 00 08 01 00 ff ff 00 2a
    CRC:   06 7d 02

systime=1504861592 freq=2438 addr=d90fb229 delta_t=0.313 ms rssi=-49
0b 09 09 01 00 00 00 00 00 00 00 4d 66 54
Data / AA d90fb229 (valid) /  9 bytes
    Channel Index: 16
    LLID: 3 / LL Control PDU
    NESN: 0  SN: 1  MD: 0
    Opcode: 9 / LL_FEATURE_RSP

    Data:  09 01 00 00 00 00 00 00 00
    CRC:   4d 66 54
```

Figure 4.18 Active communication captured using Ubertooth-one in the L2CAP layer

There were 10 test files captured on each channel 37, 38 and 39; and, the pairing request was captured in order to deduce the encryption key. For a successful determination of the encryption key, there are certain parameters that need to be captured by the Ubertooth-one. These components are:

- CONNECT_REQ
- LL_ENC_CONNET_REQ
- LL_UPDATE_REQ

Once all these parameters were captured during the process, the connection was then cracked and the encryption key determined.

In addition, the Ubertooth-one also has a spectrum analyzer. Figures 4.19 and 4.20 present a spectrum analysis of the active Bluetooth connections. Figure 4.19 presents a screenshot of the spectrum with no Bluetooth devices switched on. Figure 4.20 presents a screenshot of the fluctuation when the Bluetooth was switched on at the headset and the smart phone.

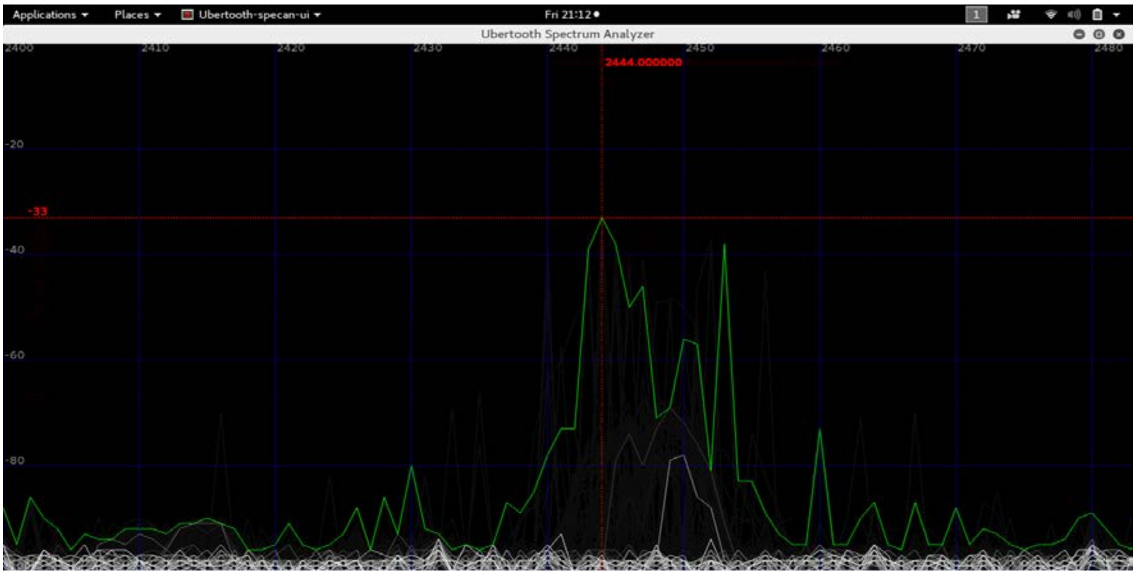


Figure 4.19 Spectrum analyser with no Bluetooth

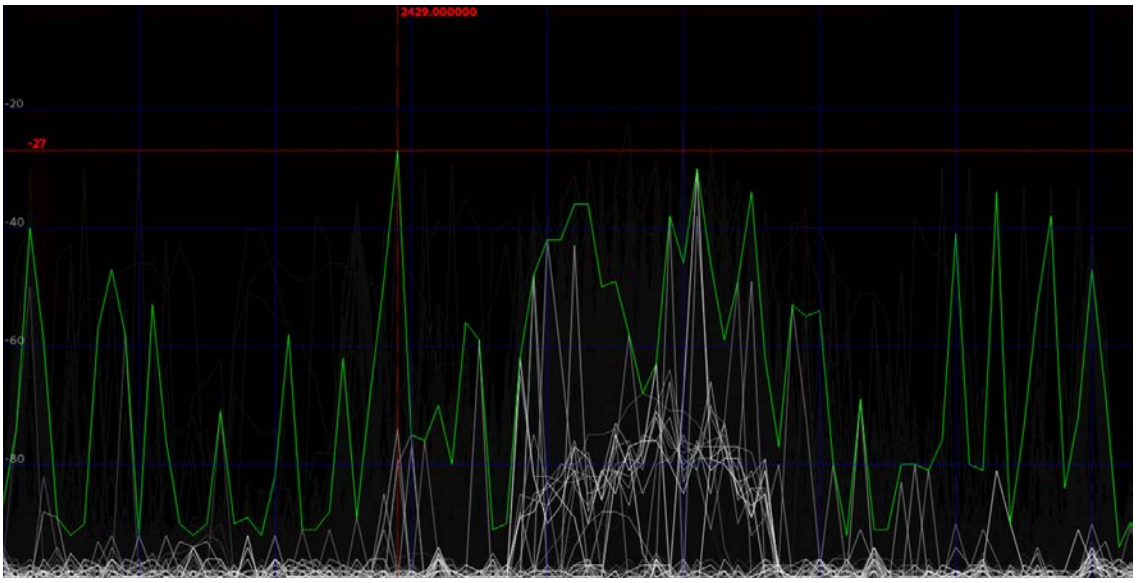
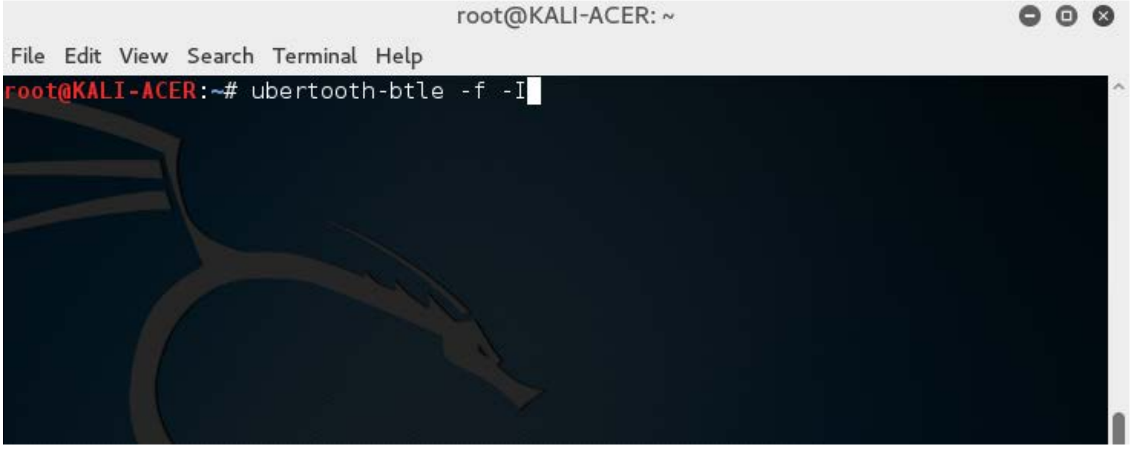


Figure 4.20 Spectrum analyzer with Bluetooth switched on

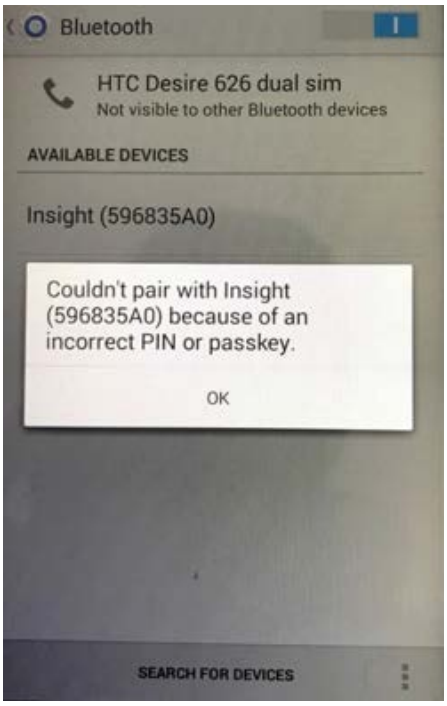
In addition to capturing data passively, the Ubertooth-one was effective in interfering with a specific connection request which therefore rendered a Denial Of Service (DoS) attack. In this case, Figure 4.21 presents a screenshot of the command used to create the interference, which is Ubertooth-btle -f –I, where -f follows an active communication, and -I creates an interference.



```
root@KALI-ACER:~# ubertooth-btle -f -I
```

Figure 4.21 Interference command using the Ubertooth-one

After entering the command, the Ubertooth-one started advertising nonsense data preventing the pairing between the Smartphone and the Insight. Figure 4.22 presents a screenshot of the error message showing the interference disrupting the pairing request.

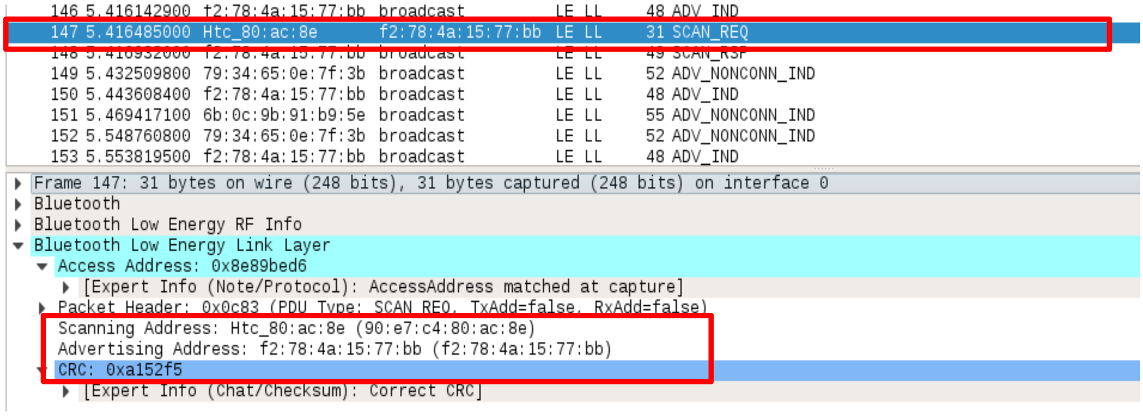


Couldn't pair with Insight (596835A0) because of an incorrect PIN or passkey.

Figure 4.22 Rejection of the pairing request.

There are three types of Bluetooth pairing which are Just Works, Out of Band pairing and Passkey. Just Works simply pairs off the box. There is no need to enter a PIN. Out of Band or OOB pairing involves Near Field Communication (NFC). Finally, the Passkey method involves entering a 6 digit PIN. The Emotiv Insight works on a Just Works pairing form, which does not require any kind of manual input of numbers or a specific

PIN/passkey. In this case, the error message proves the DoS was caused by the Ubertooth-one. After performing the interference, the Ubertooth-one was used to decrypt the Long-Term Key (LTK) which is the encryption key exchanged by Insight and the smartphone. The Ubertooth-one then decrypted the LTK and the communication between Insight and the smartphone. Figure 4.23 presents a screenshot of the pairing request in Wireshark.

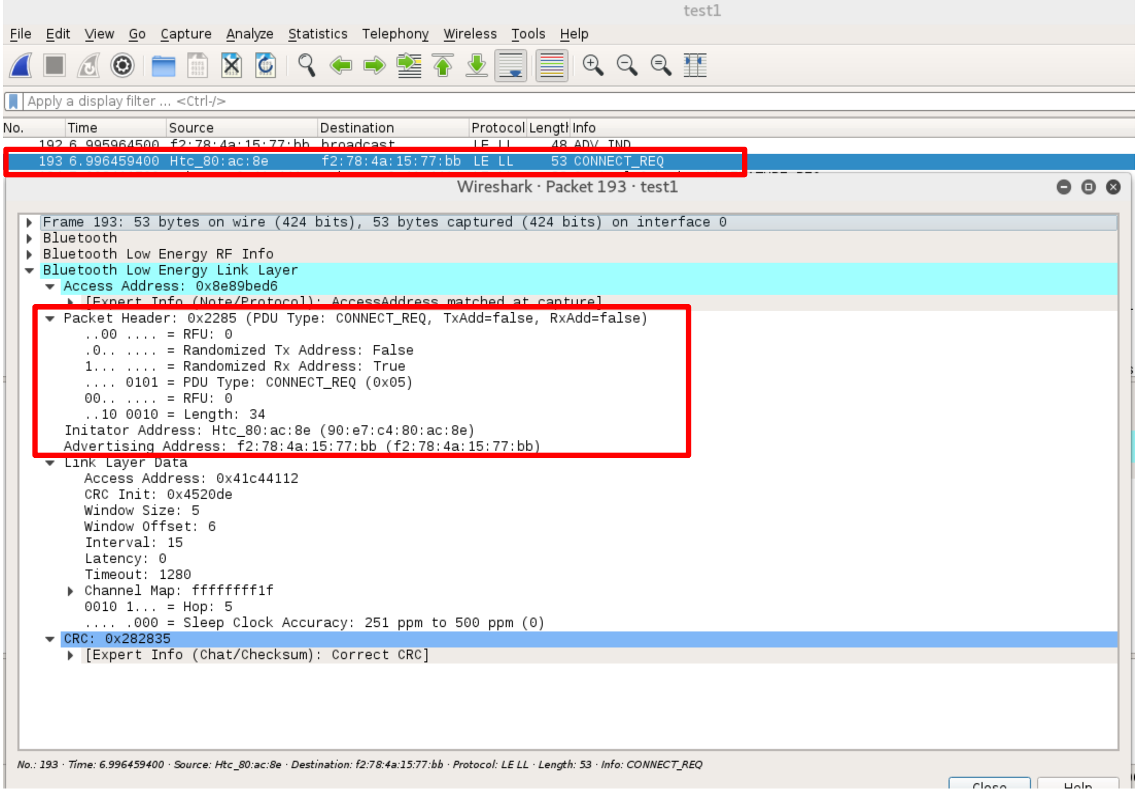


```
146 5.416142900 f2:78:4a:15:77:bb broadcast         LE LL   48 ADV_IND
147 5.416485000 Htc_80:ac:8e      f2:78:4a:15:77:bb LE LL   31 SCAN_REQ
148 5.416932000 f2:78:4a:15:77:bb broadcast         LE LL   49 SCAN_RSP
149 5.432509800 79:34:65:0e:7f:3b broadcast         LE LL   52 ADV_NONCONN_IND
150 5.443608400 f2:78:4a:15:77:bb broadcast         LE LL   48 ADV_IND
151 5.469417100 6b:0c:9b:91:b9:5e broadcast         LE LL   55 ADV_NONCONN_IND
152 5.548760800 79:34:65:0e:7f:3b broadcast         LE LL   52 ADV_NONCONN_IND
153 5.553819500 f2:78:4a:15:77:bb broadcast         LE LL   48 ADV_IND
```

```
▸ Frame 147: 31 bytes on wire (248 bits), 31 bytes captured (248 bits) on interface 0
▸ Bluetooth
▸ Bluetooth Low Energy RF Info
▾ Bluetooth Low Energy Link Layer
  ▾ Access Address: 0x8e89bed6
    ▸ [Expert Info (Note/Protocol): AccessAddress matched at capture]
  ▸ Packet Header: 0x0c83 (PDU Type: SCAN_REQ, TxAdd=false, RxAdd=false)
    Scanning Address: Htc_80:ac:8e (90:e7:c4:80:ac:8e)
    Advertising Address: f2:78:4a:15:77:bb (f2:78:4a:15:77:bb)
  ▾ CRC: 0xa152f5
    ▸ [Expert Info (Chat/Checksum): Correct CRC]
```

Figure 4.23 Pairing request captured by Ubertooth-one

Figure 4.24 shows the pairing request was initiated by the smartphone (90:e7:c4:80:ac:8e) to the headset Insight (f2:78:4a:15:77:bb), and it also presents a screenshot of the CONNECT_REQ parameter.



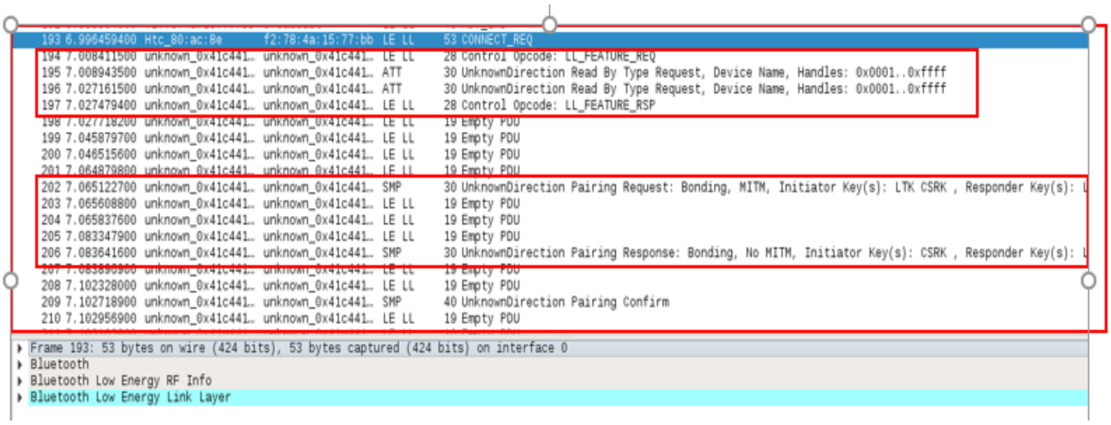
test1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Wireshark · Packet 193 · test1
Close
Help

```
No.  Time           Source            Destination        Protocol Length Info
192 6.995964500 f2:78:4a:15:77:bb broadcast         LE LL   48 ADV_IND
193 6.996459400 Htc_80:ac:8e      f2:78:4a:15:77:bb LE LL   53 CONNECT_REQ
```

```
▸ Frame 193: 53 bytes on wire (424 bits), 53 bytes captured (424 bits) on interface 0
▸ Bluetooth
▸ Bluetooth Low Energy RF Info
▾ Bluetooth Low Energy Link Layer
  ▾ Access Address: 0x8e89bed6
    ▸ [Expert Info (Note/Protocol): AccessAddress matched at capture]
  ▾ Packet Header: 0x2285 (PDU Type: CONNECT_REQ, TxAdd=false, RxAdd=false)
      ..00 .... = RFU: 0
      .0.. .... = Randomized Tx Address: False
      1... .... = Randomized Rx Address: True
      .... 0101 = PDU Type: CONNECT_REQ (0x05)
      00.. .... = RFU: 0
      ..10 0010 = Length: 34
    Initator Address: Htc_80:ac:8e (90:e7:c4:80:ac:8e)
    Advertising Address: f2:78:4a:15:77:bb (f2:78:4a:15:77:bb)
  ▾ Link Layer Data
      Access Address: 0x41c44112
      CRC Init: 0x4520de
      Window Size: 5
      Window Offset: 6
      Interval: 15
      Latency: 0
      Timeout: 1280
    ▸ Channel Map: ffffffff1f
      0010 1... = Hop: 5
      .... .000 = Sleep Clock Accuracy: 251 ppm to 500 ppm (0)
  ▾ CRC: 0x282835
    ▸ [Expert Info (Chat/Checksum): Correct CRC]

No.: 193 · Time: 6.996459400 · Source: Htc_80:ac:8e · Destination: f2:78:4a:15:77:bb · Protocol: LE LL · Length: 53 · Info: CONNECT_REQ
```

Figure 4.24 CONNECT_REQ parameter captured by Ubertooth-one

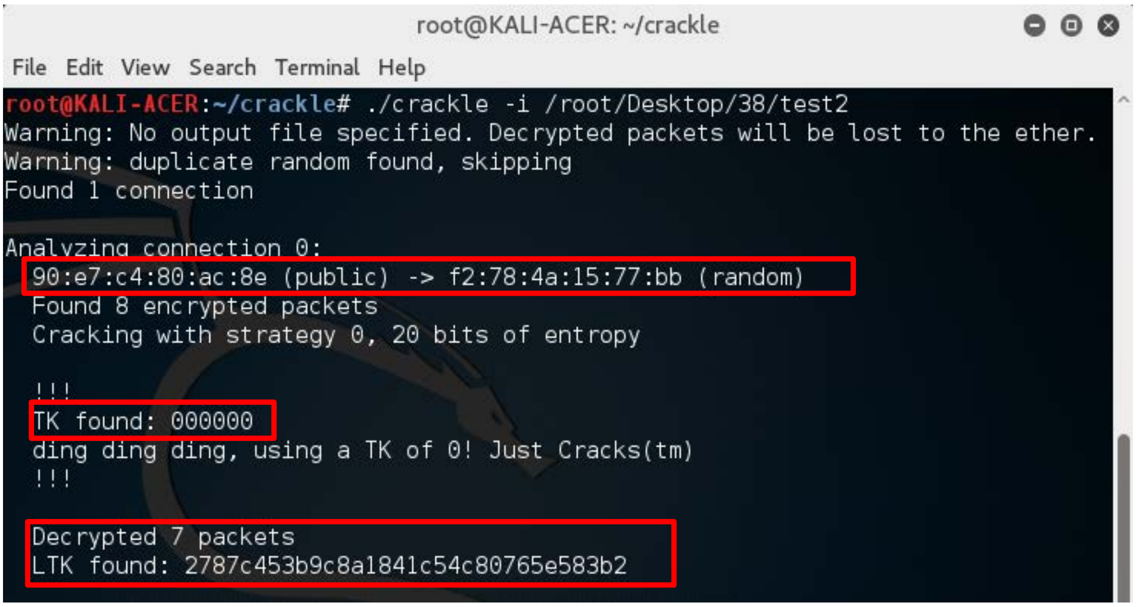
Figure 4.25 presents a screenshot of the CONNECT_REQ along with the exchange of the LTK and also shows 'No MITM' (Man In The Middle) indicating there is no protection to thwart a Man In The Middle (MITM) attack.



```
193 6.996459400 Htc_80:ac:8e        f2:78:4a:15:77:bb LE LL     53 CONNECT_REQ
194 7.008411500 unknown_0x41c441… unknown_0x41c441… LE LL     28 Control Opcode: LL_FEATURE_REQ
195 7.008943500 unknown_0x41c441… unknown_0x41c441… ATT       30 UnknownDirection Read By Type Request, Device Name, Handles: 0x0001..0xffff
196 7.027161500 unknown_0x41c441… unknown_0x41c441… ATT       30 UnknownDirection Read By Type Request, Device Name, Handles: 0x0001..0xffff
197 7.027479400 unknown_0x41c441… unknown_0x41c441… LE LL     28 Control Opcode: LL_FEATURE_RSP
198 7.027718200 unknown_0x41c441… unknown_0x41c441… LE LL     19 Empty PDU
199 7.045879700 unknown_0x41c441… unknown_0x41c441… LE LL     19 Empty PDU
200 7.046515600 unknown_0x41c441… unknown_0x41c441… LE LL     19 Empty PDU
201 7.064879800 unknown_0x41c441… unknown_0x41c441… LE LL     19 Empty PDU
202 7.065122700 unknown_0x41c441… unknown_0x41c441… SMP       30 UnknownDirection Pairing Request: Bonding, MITM, Initiator Key(s): LTK CSRK , Responder Key(s): L
203 7.065608800 unknown_0x41c441… unknown_0x41c441… LE LL     19 Empty PDU
204 7.065837600 unknown_0x41c441… unknown_0x41c441… LE LL     19 Empty PDU
205 7.083347900 unknown_0x41c441… unknown_0x41c441… LE LL     19 Empty PDU
206 7.083641600 unknown_0x41c441… unknown_0x41c441… SMP       30 UnknownDirection Pairing Response: Bonding, No MITM, Initiator Key(s): CSRK , Responder Key(s): L
207 7.083890900 unknown_0x41c441… unknown_0x41c441… LE LL     19 Empty PDU
208 7.102328000 unknown_0x41c441… unknown_0x41c441… LE LL     19 Empty PDU
209 7.102718900 unknown_0x41c441… unknown_0x41c441… SMP       40 UnknownDirection Pairing Confirm
210 7.102956900 unknown_0x41c441… unknown_0x41c441… LE LL     19 Empty PDU
▸ Frame 193: 53 bytes on wire (424 bits), 53 bytes captured (424 bits) on interface 0
▸ Bluetooth
▸ Bluetooth Low Energy RF Info
▸ Bluetooth Low Energy Link Layer
```

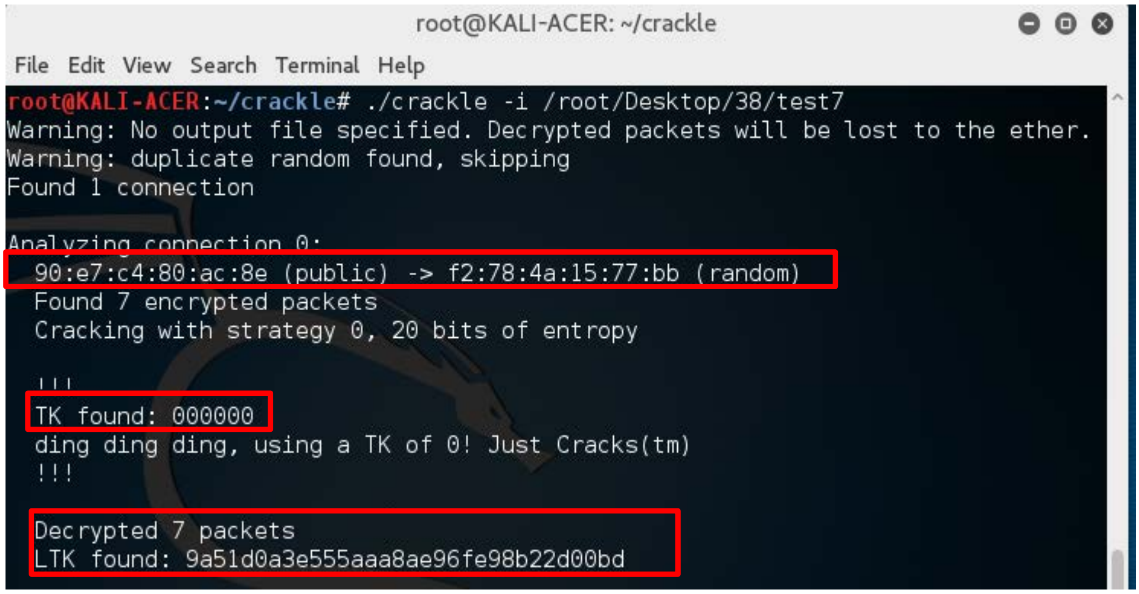
Figure 4.25 Exchange of the LTK

Wireshark packets were captured including 10 other packets on different advertising channels 37, 38 and 39. More than 80% of the packets captured at various advertising channels could be decrypted using the LTK. The LTK was decrypted using the CrackLE tool developed by Mike Ryan. CrackLE is a program that exploits a flaw in Bluetooth Low Energy pairing allowing the attacker to brute force the Short Term Key (STK), thereby decrypting the Long Term Key (LTK). Figure 4.26 presents a screenshot of the two test files with the LTK cracked along with the STK. The command used was ./crackle -i <testfile>



root@KALI-ACER: ~/crackle
File Edit View Search Terminal Help

```
root@KALI-ACER:~/crackle# ./crackle -i /root/Desktop/38/test2
Warning: No output file specified. Decrypted packets will be lost to the ether.
Warning: duplicate random found, skipping
Found 1 connection

Analyzing connection 0:
  90:e7:c4:80:ac:8e (public) -> f2:78:4a:15:77:bb (random)
  Found 8 encrypted packets
  Cracking with strategy 0, 20 bits of entropy

  !!!
  TK found: 000000
  ding ding ding, using a TK of 0! Just Cracks(tm)
  !!!

  Decrypted 7 packets
  LTK found: 2787c453b9c8a1841c54c80765e583b2
```

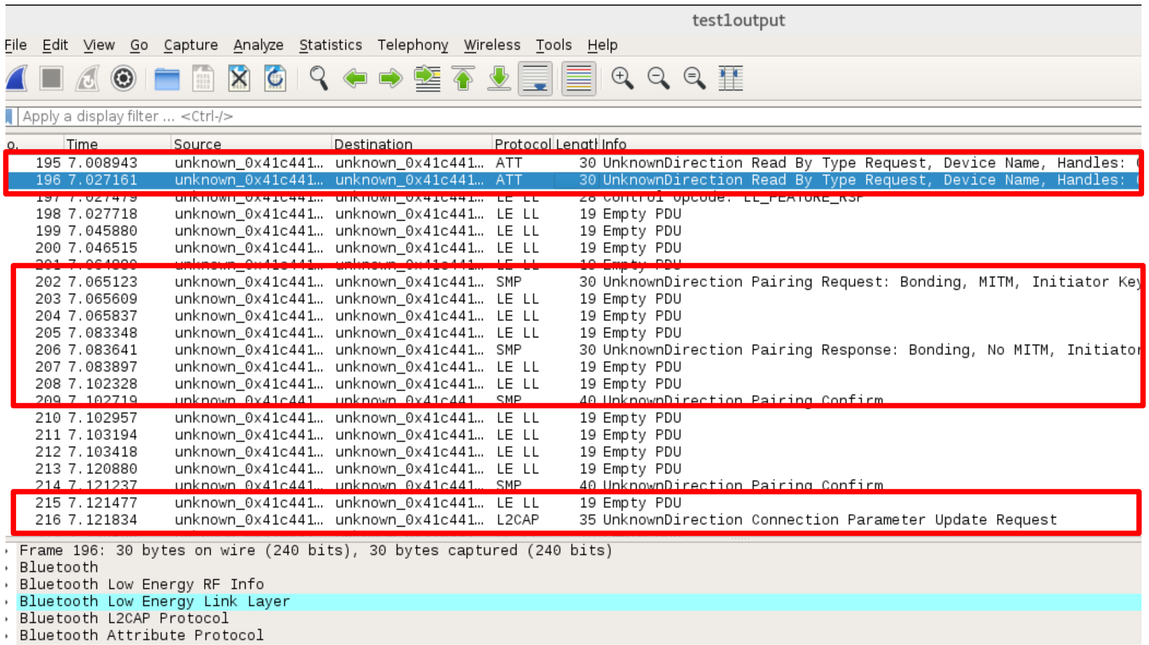


root@KALI-ACER: ~/crackle
File Edit View Search Terminal Help

```
root@KALI-ACER:~/crackle# ./crackle -i /root/Desktop/38/test7
Warning: No output file specified. Decrypted packets will be lost to the ether.
Warning: duplicate random found, skipping
Found 1 connection

Analyzing connection 0:
  90:e7:c4:80:ac:8e (public) -> f2:78:4a:15:77:bb (random)
  Found 7 encrypted packets
  Cracking with strategy 0, 20 bits of entropy

  !!!
  TK found: 000000
  ding ding ding, using a TK of 0! Just Cracks(tm)
  !!!

  Decrypted 7 packets
  LTK found: 9a51d0a3e555aaa8ae96fe98b22d00bd
```

Figure 4.26 STK and LTK

For a successful cracking of the LTK, all the essential pairing requests need to be captured without which the LTK cannot be cracked. Figure 4.27 presents a screenshot of the decrypted communication packet using the LTK in Wireshark. The three layers of the protocol stack for Bluetooth has been highlighted. Decrypting the entire communication shows the L2CAP, SMP and ATT layers in the higher layers of the Bluetooth protocol.



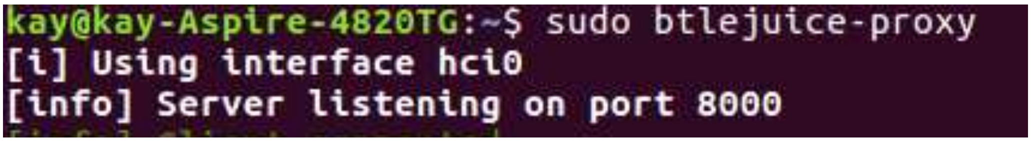
test1output
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
o.  Time      Source              Destination         Protocol Lengtl Info
195 7.008943  unknown_0x41c441…   unknown_0x41c441…   ATT      30 UnknownDirection Read By Type Request, Device Name, Handles: (
196 7.027161  unknown_0x41c441…   unknown_0x41c441…   ATT      30 UnknownDirection Read By Type Request, Device Name, Handles: (
197 7.027479  unknown_0x41c441…   unknown_0x41c441…   LE LL    28 Control Opcode: LL_FEATURE_RSP
198 7.027718  unknown_0x41c441…   unknown_0x41c441…   LE LL    19 Empty PDU
199 7.045880  unknown_0x41c441…   unknown_0x41c441…   LE LL    19 Empty PDU
200 7.046515  unknown_0x41c441…   unknown_0x41c441…   LE LL    19 Empty PDU
201 7.064880  unknown_0x41c441…   unknown_0x41c441…   LE LL    19 Empty PDU
202 7.065123  unknown_0x41c441…   unknown_0x41c441…   SMP      30 UnknownDirection Pairing Request: Bonding, MITM, Initiator Key
203 7.065609  unknown_0x41c441…   unknown_0x41c441…   LE LL    19 Empty PDU
204 7.065837  unknown_0x41c441…   unknown_0x41c441…   LE LL    19 Empty PDU
205 7.083348  unknown_0x41c441…   unknown_0x41c441…   LE LL    19 Empty PDU
206 7.083641  unknown_0x41c441…   unknown_0x41c441…   SMP      30 UnknownDirection Pairing Response: Bonding, No MITM, Initiator
207 7.083897  unknown_0x41c441…   unknown_0x41c441…   LE LL    19 Empty PDU
208 7.102328  unknown_0x41c441…   unknown_0x41c441…   LE LL    19 Empty PDU
209 7.102719  unknown_0x41c441…   unknown_0x41c441…   SMP      40 UnknownDirection Pairing Confirm
210 7.102957  unknown_0x41c441…   unknown_0x41c441…   LE LL    19 Empty PDU
211 7.103194  unknown_0x41c441…   unknown_0x41c441…   LE LL    19 Empty PDU
212 7.103418  unknown_0x41c441…   unknown_0x41c441…   LE LL    19 Empty PDU
213 7.120880  unknown_0x41c441…   unknown_0x41c441…   LE LL    19 Empty PDU
214 7.121237  unknown_0x41c441…   unknown_0x41c441…   SMP      40 UnknownDirection Pairing Confirm
215 7.121477  unknown_0x41c441…   unknown_0x41c441…   LE LL    19 Empty PDU
216 7.121834  unknown_0x41c441…   unknown_0x41c441…   L2CAP    35 UnknownDirection Connection Parameter Update Request

› Frame 196: 30 bytes on wire (240 bits), 30 bytes captured (240 bits)
› Bluetooth
› Bluetooth Low Energy RF Info
› Bluetooth Low Energy Link Layer
› Bluetooth L2CAP Protocol
› Bluetooth Attribute Protocol
```

Figure 4.27 LL, L2CAP, SMP and ATT layers

4.4.3 Btlejuice

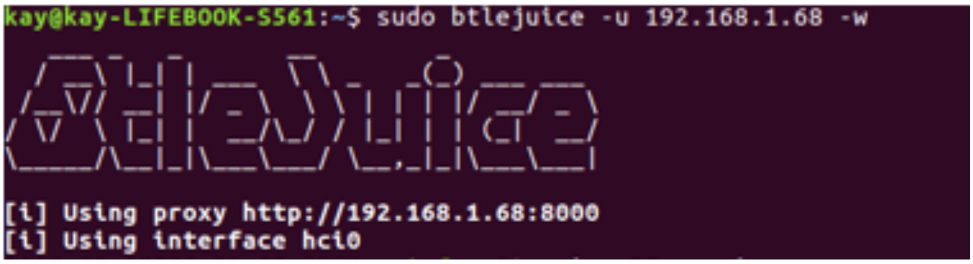
The Ubertooth-one could perform all the functions except sending packets into an ongoing communication. To check the feasibility of a much more complex form of attack such as a replay attack or a modification attack, a Man In The Middle (MITM) Framework called 'Btlejuice' was deployed. Btlejuice is the framework developed by Damien Cauquil which makes use of the external Bluetooth dongles CSR 4.0, and creates a clone of the target device (Insight). Two machines are required where one machine runs the btlejuice proxy and the other machine runs the client with the websocket layer. The intent is to intercept the General Attribute Profile (GATT), the top most layer of the Bluetooth protocol stack. Figure 4.28 presents a screenshot of the host running the proxy. The command used is sudo btlejuice-proxy



```
kay@kay-Aspire-4820TG:~$ sudo btlejuice-proxy
[i] Using interface hci0
[info] Server listening on port 8000
```

Figure 4.28 Btlejuice proxy

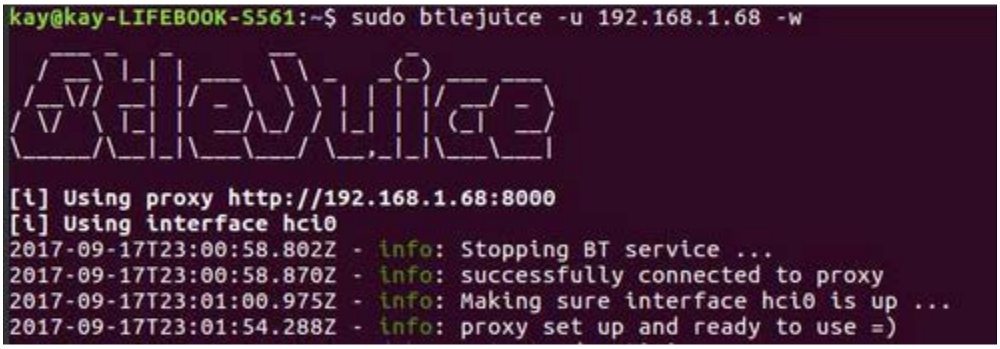
On the other machine, the web socket is connected to the proxy by connecting the second machine to the proxy's IP address. Figure 4.29 presents a screenshot of the client with the command sudo btlejuice -u 192.168.1.68 -w where -u links the proxy's IP address and -w opens the website interface.



```
kay@kay-LIFEBOOK-S561:~$ sudo btlejuice -u 192.168.1.68 -w
   ___ _   _       __       _
  / __\ |_| | ___  \ \_   _(_) ___ ___
 /__\// __| |/ _ \  \ \ | | | |/ __/ _ \
/ \/  \ |_| |  __/\_/ / |_| | | (_|  __/
\_____/\__|_|\___\___/ \__,_|_|\___\___|

[i] Using proxy http://192.168.1.68:8000
[i] Using interface hci0
```

Figure 4.29 Client connecting the proxy's IP address

Once the command is typed in to the client, the client and the proxy connect. This is presented in Figure 4.30.



```
kay@kay-LIFEBOOK-S561:~$ sudo btlejuice -u 192.168.1.68 -w

[i] Using proxy http://192.168.1.68:8000
[i] Using interface hci0
2017-09-17T23:00:58.802Z - info: Stopping BT service ...
2017-09-17T23:00:58.870Z - info: successfully connected to proxy
2017-09-17T23:01:00.975Z - info: Making sure interface hci0 is up ...
2017-09-17T23:01:54.288Z - info: proxy set up and ready to use =)
```

Figure 4.30 Client and proxy connection on the client machine

After this step, a web browser is launched to go to the localhost port open at 8080 by typing localhost:8080. Figure 4.31 presents a screenshot of the window showing 4 different options with capabilities to intercept data between the headset and the smartphone application. After the proxy and the client is connected, the webpage was opened. Switching on the headset and then clicking on the target button, displayed the headset with the Mac address. Figure 4.32 presents a screenshot of the Insight headset and with the mac address which is f2:78:4a:15:77:bb

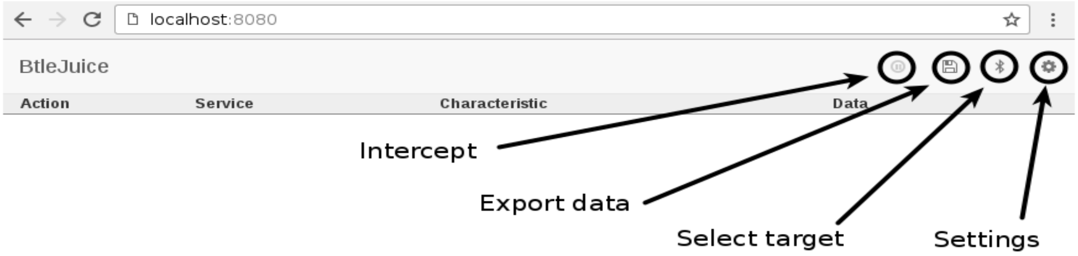
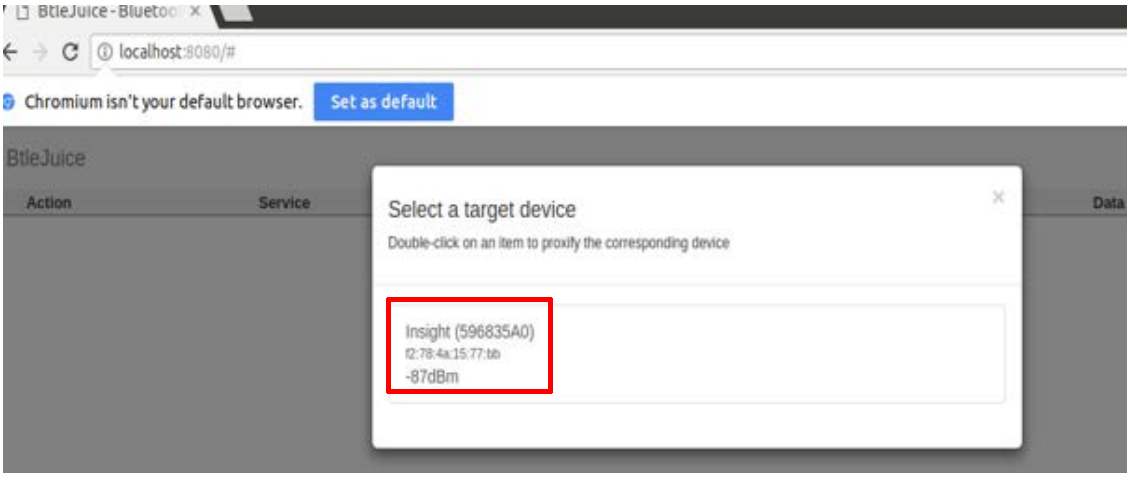


Figure 4.31 Btlejuice localhost website



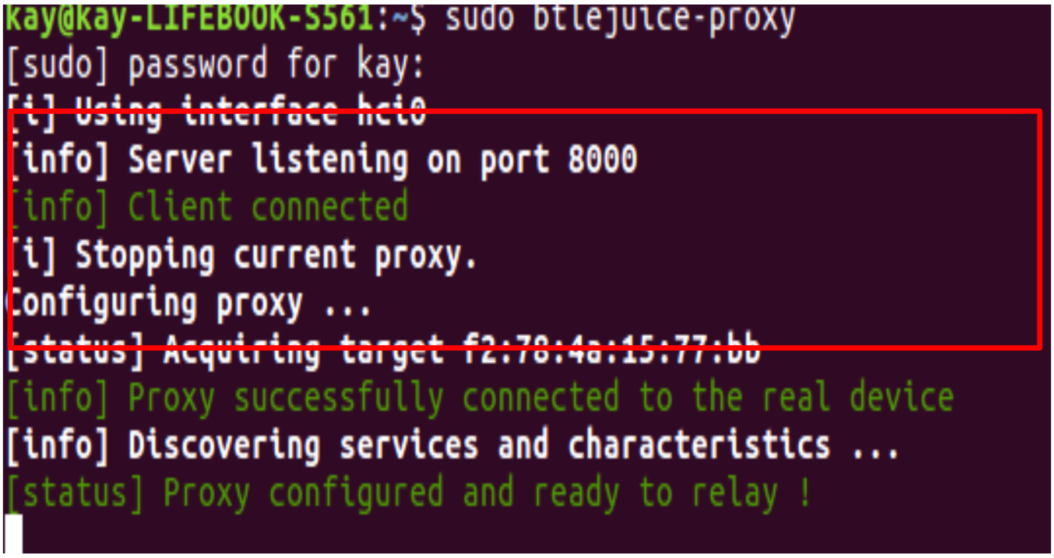
Select a target device

Double-click on an item to proxify the corresponding device

Insight (596835A0)
f2:78:4a:15:77:bb
-87dBm

Figure 4.32 Insight headset with the mac address

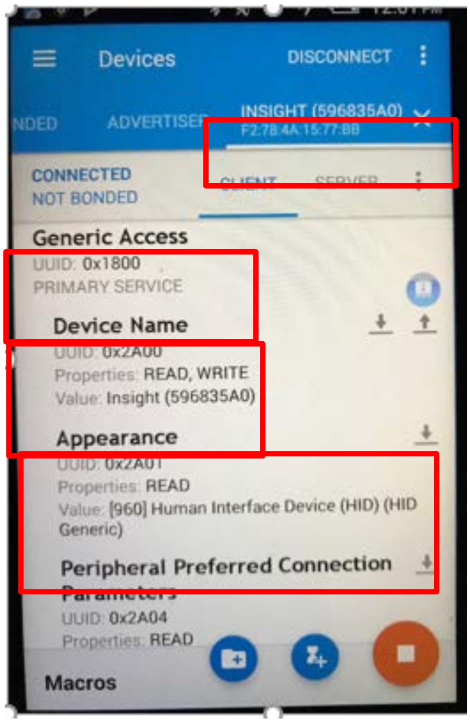
On selecting the headset, the Bluetooth dongle proxies the services and characteristics of the Insight headset and pairs with the headset. After selecting the target, Figure 4.31 the Bluetooth dongle acquires the real device and blocks the individual from pairing to the actual headset as presented in figure 4.33



```
kay@kay-LIFEBOOK-S561:~$ sudo btlejuice-proxy
[sudo] password for kay:
[i] Using interface hci0
[info] Server listening on port 8000
[info] Client connected
[i] Stopping current proxy.
Configuring proxy ...
[status] Acquiring target f2:78:4a:15:77:bb
[info] Proxy successfully connected to the real device
[info] Discovering services and characteristics ...
[status] Proxy configured and ready to relay !
```

Figure 4.33 The proxy connecting to the real device

Before, performing any other commands, an application on the smartphone called nrf Bluetooth shows the generic details of the Bluetooth Low energy device, in this case the Insight headset. Figures 4.34 and 4.35 present screenshots of the services and characteristics associated with the original headset which can be confirmed with the mac address of the headset.



CONNECTED
NOT BONDED

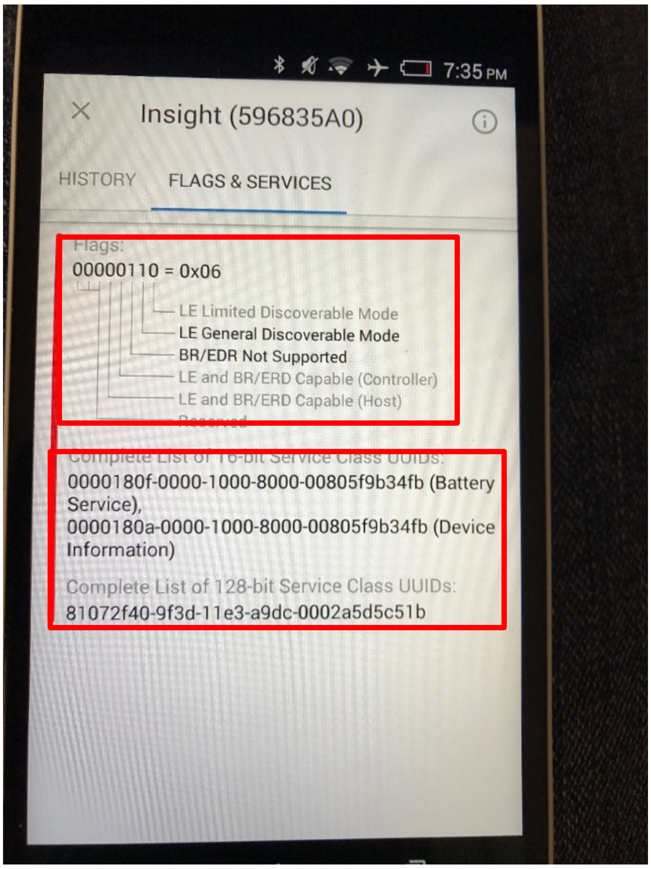
Generic Access
UUID: 0x1800
PRIMARY SERVICE

Device Name
UUID: 0x2A00
Properties: READ, WRITE
Value: Insight (596835A0)

Appearance
UUID: 0x2A01
Properties: READ
Value: [960] Human Interface Device (HID) (HID Generic)

Peripheral Preferred Connection Parameters
UUID: 0x2A04
Properties: READ

Figure 4.34 Original device and the characteristics of the Insight headset



Flags:
00000110 = 0x06
LE Limited Discoverable Mode
LE General Discoverable Mode
BR/EDR Not Supported
LE and BR/ERD Capable (Controller)
LE and BR/ERD Capable (Host)
Reserved

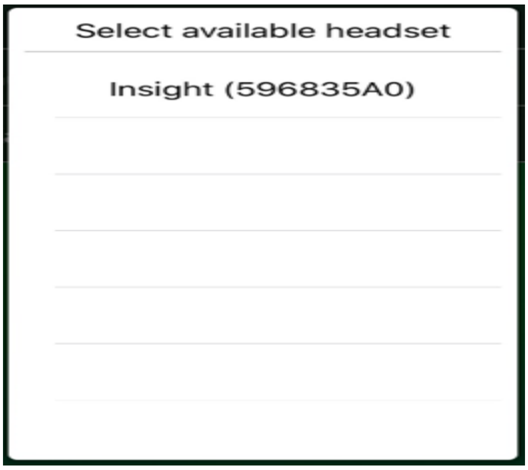
Complete List of 16-bit Service Class UUIDs:
0000180f-0000-1000-8000-00805f9b34fb (Battery Service),
0000180a-0000-1000-8000-00805f9b34fb (Device Information)

Complete List of 128-bit Service Class UUIDs:
81072f40-9f3d-11e3-a9dc-0002a5d5c51b

Figure 4.35 Flags and services of the Insight headset along with the UUID

In addition to the services, it also shows the device information and battery service. Furthermore, it also shows the device is a general Low Energy (LE) Discoverable mode. After exploring the features of the Insight headset, it was time to pair the device to the application. The nrf Bluetooth application is used to confirm the services associated with the brainware.

When the headset is connected to the proxy, the client machine has a Bluetooth adapter which has the same characteristics and services as the Insight headset. Upon launching the application called Mental Commands designed by Emotiv, the dummy headset is displayed on the list as the real device. Figure 4.36 presents a screenshot of the dummy device with the same name of the headset.

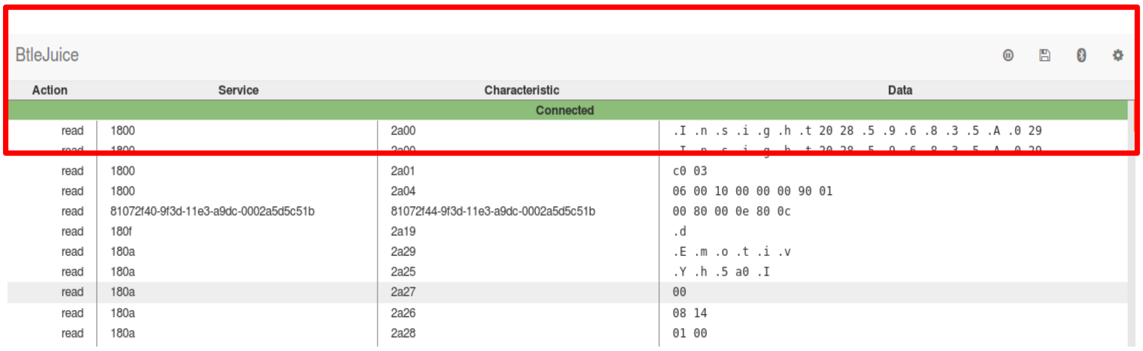


Select available headset

Insight (596835A0)

Figure 4.36 Dummy device listed by the application on the smartphone

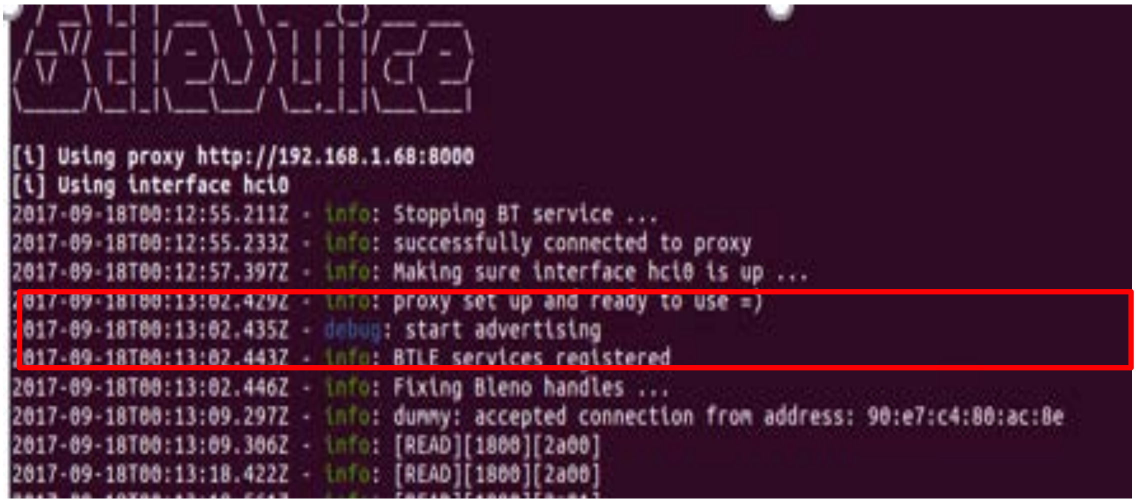
After the application connects to the dummy device, the Btlejuice starts to capture all the data sent from the application from the headset. Figure 4.37 presents a screenshot of the Btlejuice environment showing the Generic Attribute (GATT) data and figure 4.38 presents a screenshot of the background process running in the terminal.



BtleJuice

Action	Service	Characteristic	Data
Connected			
read	1800	2a00	.I .n .s .i .g .h .t 20 28 .5 .9 .6 .8 .3 .5 .A .0 29
read	1800	2a00	.I .n .s .i .g .h .t 20 28 .5 .9 .6 .8 .3 .5 .A .0 29
read	1800	2a01	c0 03
read	1800	2a04	06 00 10 00 00 00 90 01
read	81072f40-9f3d-11e3-a9dc-0002a5d5c51b	81072f44-9f3d-11e3-a9dc-0002a5d5c51b	00 80 00 0e 80 0c
read	180f	2a19	.d
read	180a	2a29	.E .m .o .t .i .v
read	180a	2a25	.Y .h .5 a0 .I
read	180a	2a27	00
read	180a	2a26	08 14
read	180a	2a28	01 00

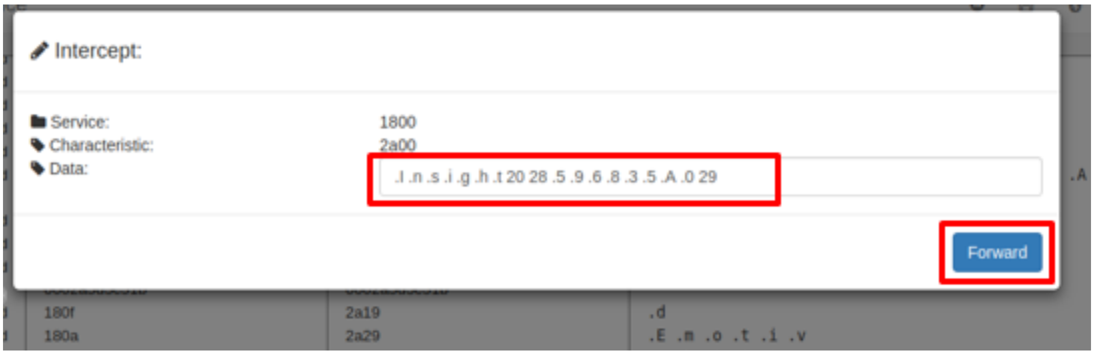
Figure 4.37 The application sending commands to the headset



```
[i] Using proxy http://192.168.1.68:8000
[i] Using interface hci0
2017-09-18T00:12:55.211Z - info: Stopping BT service ...
2017-09-18T00:12:55.233Z - info: successfully connected to proxy
2017-09-18T00:12:57.397Z - info: Making sure interface hci0 is up ...
017-09-18T00:13:02.429Z - info: proxy set up and ready to use =)
017-09-18T00:13:02.435Z - debug: start advertising
017-09-18T00:13:02.443Z - info: BTLE services registered
2017-09-18T00:13:02.446Z - info: Fixing Bleno handles ...
2017-09-18T00:13:09.297Z - info: dummy: accepted connection from address: 90:e7:c4:80:ac:8e
2017-09-18T00:13:09.306Z - info: [READ][1800][2a00]
2017-09-18T00:13:18.422Z - info: [READ][1800][2a00]
```

Figure 4.38 Terminal showing the smartphone accepting the dummy

This feature known as ‘on the fly modification’ was then performed. Initially, any command intended to the headset will be sent to the proxy to confirm whether the data should be forwarded to the headset or not. Figures 4.39 and 4.40 present screenshots of the active data intercepted with an option to forward the data or simply devoid the headset of that specific data. This intercepted data could also be modified to a different command which could be forwarded to the headset causing it to not work correctly.

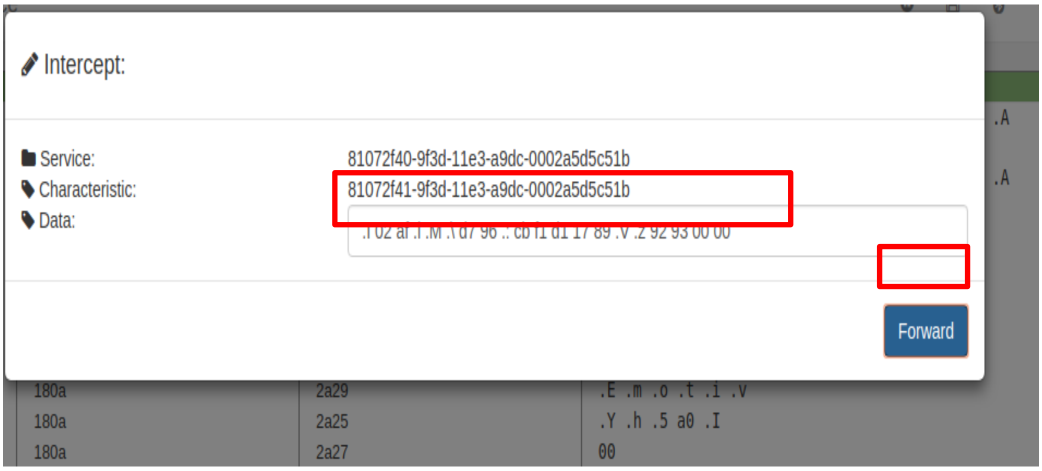


Intercept:

Service: 1800
Characteristic: 2a00
Data: .I .n .s .i .g .h .t 20 28 .5 .9 .6 .8 .3 .5 .A .0 29

Figure 4.39 Active data sent from the application to the Insight headset

All the data transmitted by the application on the smartphone destined for the Insight headset was then intercepted and was susceptible to data modification.



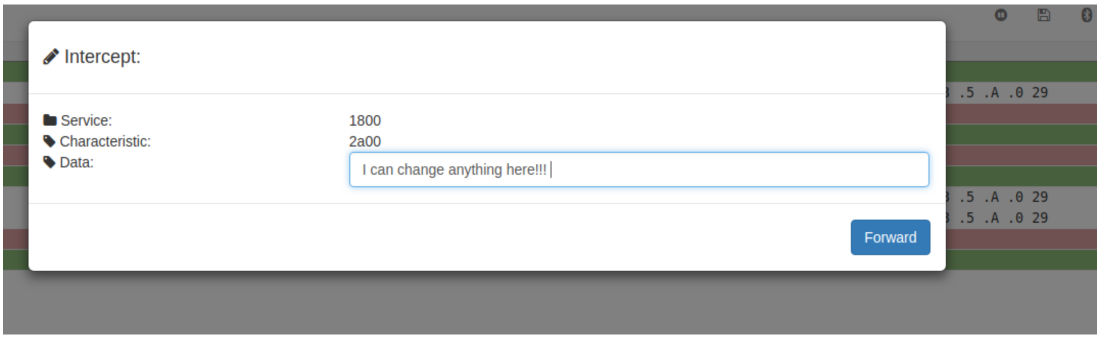
Intercept:

Service: 81072f40-9f3d-11e3-a9dc-0002a5d5c51b
Characteristic: 81072f41-9f3d-11e3-a9dc-0002a5d5c51b
Data: .f 02 af .f .M .\ d7 96 .: cb f1 d1 17 89 .V .z 92 93 00 00

```
180a        2a29        .E .m .o .t .i .v
180a        2a25        .Y .h .5 a0 .I
180a        2a27        00
```

Figure 4.40 Active data sent from the application to the Insight headset

Figure 4.41 presents a screenshot of the data for a specific command that is 1800. The data has been modified and was then forwarded to the original device causing it to malfunction.

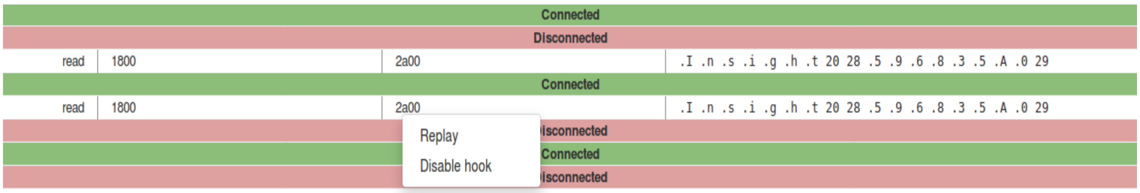


Intercept:

Service: 1800
Characteristic: 2a00
Data: I can change anything here!!!

Figure 4.41 Modification of the data

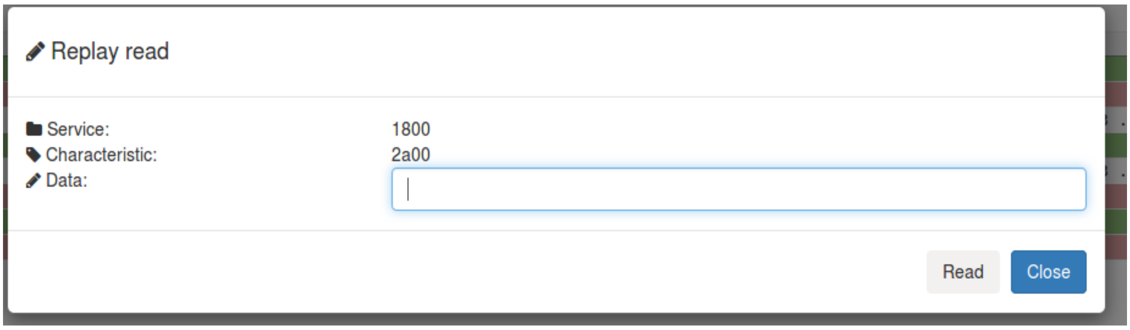
Figure 4.42 shows the possibility of a replay attack. Any data on the Btlejuice can be selected and upon right clicking on the data, two options were available. One allows the replay of data back to the headset and other one gives an option to enable or disable hooking the data or running the data as a loop.



```
                              Connected
                             Disconnected
read   1800         2a00         .I .n .s .i .g .h .t 20 28 .5 .9 .6 .8 .3 .5 .A .0 29
                              Connected
read   1800         2a00         .I .n .s .i .g .h .t 20 28 .5 .9 .6 .8 .3 .5 .A .0 29
                             isconnected
                              Connected
                             isconnected
```

Figure 4.42 Replay attack or enable/disable Hook

On clicking replay, a new dialogue option pops open, with the option to change the data and then click on read which sends the data back to the headset or notifies the headset to have a particular action to be performed. Figure 4.43 presents a screenshot of the replay read data showing the option to replay the specific data again.

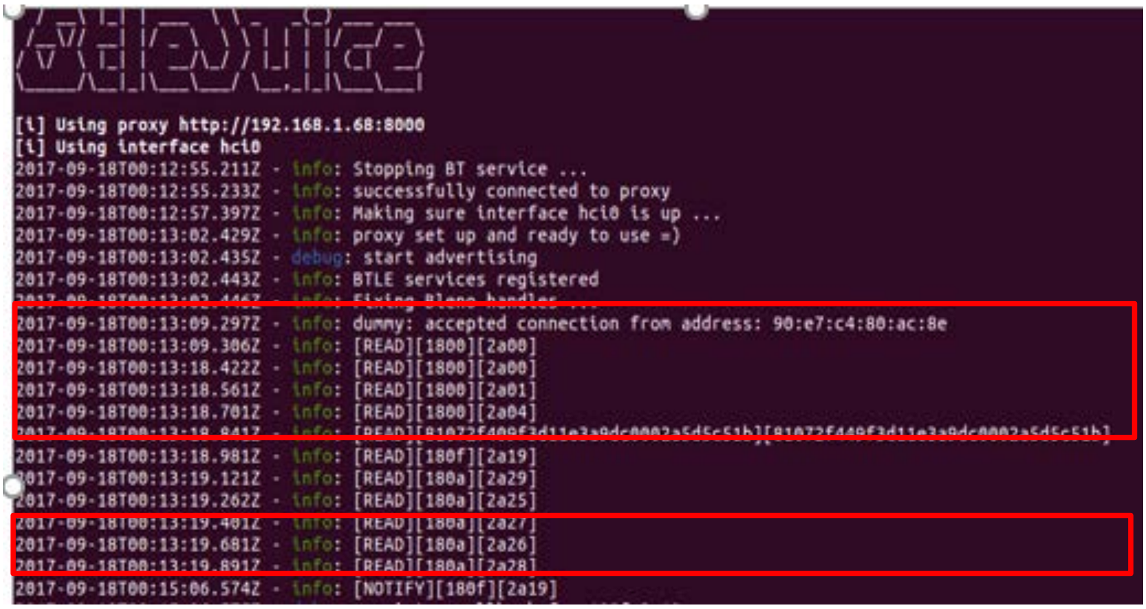


Replay read

Service: 1800
Characteristic: 2a00
Data:

Figure 4.43 Replay attack window

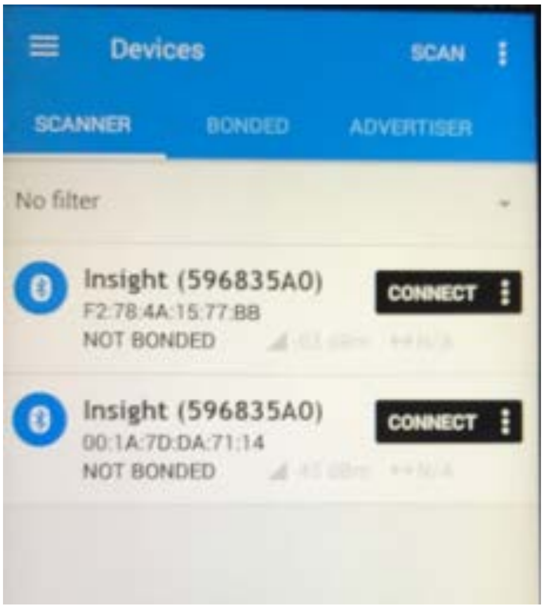
The specific command was changed to a different command using this process and can be seen in the terminal window. Figure 4.44 presents a screenshot of the terminal showing the regular push data and the modified data sent. In this case, 1800 refers to a specific command, 180f refers to a different command.



```
[i] Using proxy http://192.168.1.68:8000
[i] Using interface hci0
2017-09-18T00:12:55.211Z - info: Stopping BT service ...
2017-09-18T00:12:55.233Z - info: successfully connected to proxy
2017-09-18T00:12:57.397Z - info: Making sure interface hci0 is up ...
2017-09-18T00:13:02.429Z - info: proxy set up and ready to use =)
2017-09-18T00:13:02.435Z - debug: start advertising
2017-09-18T00:13:02.443Z - info: BTLE services registered
2017-09-18T00:13:02.446Z - info: Fixing Bleno handler ...
2017-09-18T00:13:09.297Z - info: dummy: accepted connection from address: 90:e7:c4:80:ac:8e
2017-09-18T00:13:09.306Z - info: [READ][1800][2a00]
2017-09-18T00:13:18.422Z - info: [READ][1800][2a00]
2017-09-18T00:13:18.561Z - info: [READ][1800][2a01]
2017-09-18T00:13:18.701Z - info: [READ][1800][2a04]
2017-09-18T00:13:18.841Z - info: [READ][81072f409f3d11e3a9dc0002a5d5c51b][81072f449f3d11e3a9dc0002a5d5c51b]
2017-09-18T00:13:18.981Z - info: [READ][180f][2a19]
2017-09-18T00:13:19.121Z - info: [READ][180a][2a29]
2017-09-18T00:13:19.262Z - info: [READ][180a][2a25]
2017-09-18T00:13:19.401Z - info: [READ][180a][2a27]
2017-09-18T00:13:19.681Z - info: [READ][180a][2a26]
2017-09-18T00:13:19.891Z - info: [READ][180a][2a28]
2017-09-18T00:15:06.574Z - info: [NOTIFY][180f][2a19]
```

Figure 4.44 Modified data sent back to the headset

These images (figures 4.38, 4.39, 4.40, 4.41, 4.42, 4.43 and 4.44) demonstrated the data modification attack and a replay attack. On further analysis, the nrf Bluetooth application listed both the devices, the real Insight headset with the mac address f2:78:4a:15:77:bb and with the fake Insight headset with the mac address 00:1a:7d:da:71:14..



Devices SCAN

SCANNER BONDED ADVERTISER

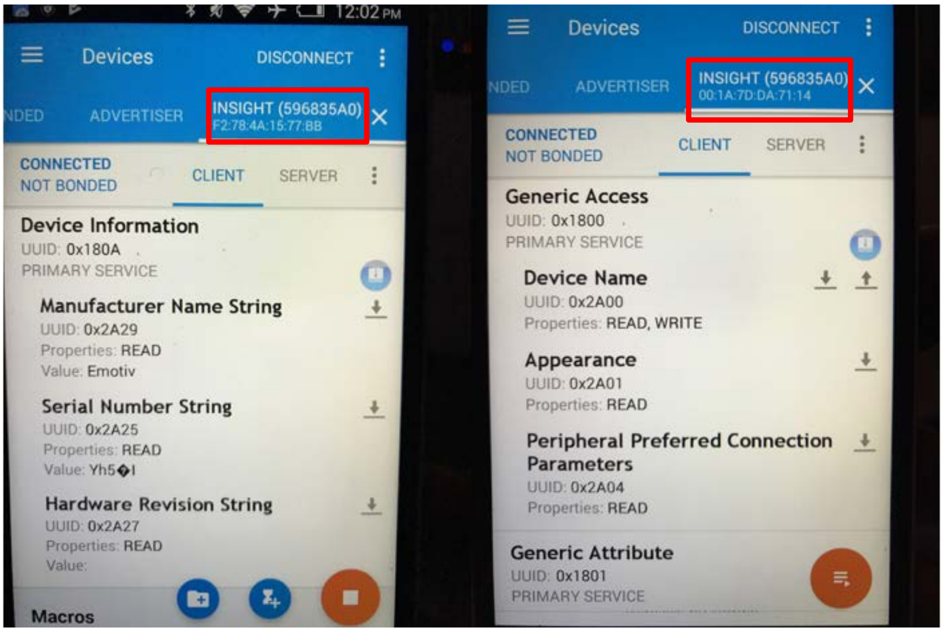
No filter

Insight (596835A0)
F2:78:4A:15:77:BB
NOT BONDED
CONNECT

Insight (596835A0)
00:1A:7D:DA:71:14
NOT BONDED
CONNECT

Figure 4.45 nrf Bluetooth application showing the real and the fake device

The original headset is connected to the proxy and the fake device connects to the application on the smartphone. The fake device has been cloned with the same features and characteristics as the original device which fools the application to think that the fake device is the real device.



12:02 PM

Devices DISCONNECT

NDED ADVERTISER INSIGHT (596835A0) F2:78:4A:15:77:8B

CONNECTED
NOT BONDED
CLIENT SERVER

Device Information
UUID: 0x180A
PRIMARY SERVICE

Manufacturer Name String
UUID: 0x2A29
Properties: READ
Value: Emotiv

Serial Number String
UUID: 0x2A25
Properties: READ
Value: Yh5�I

Hardware Revision String
UUID: 0x2A27
Properties: READ
Value:

Macros

Devices DISCONNECT

NDED ADVERTISER INSIGHT (596835A0) 00:1A:7D:DA:71:14

CONNECTED
NOT BONDED
CLIENT SERVER

Generic Access
UUID: 0x1800
PRIMARY SERVICE

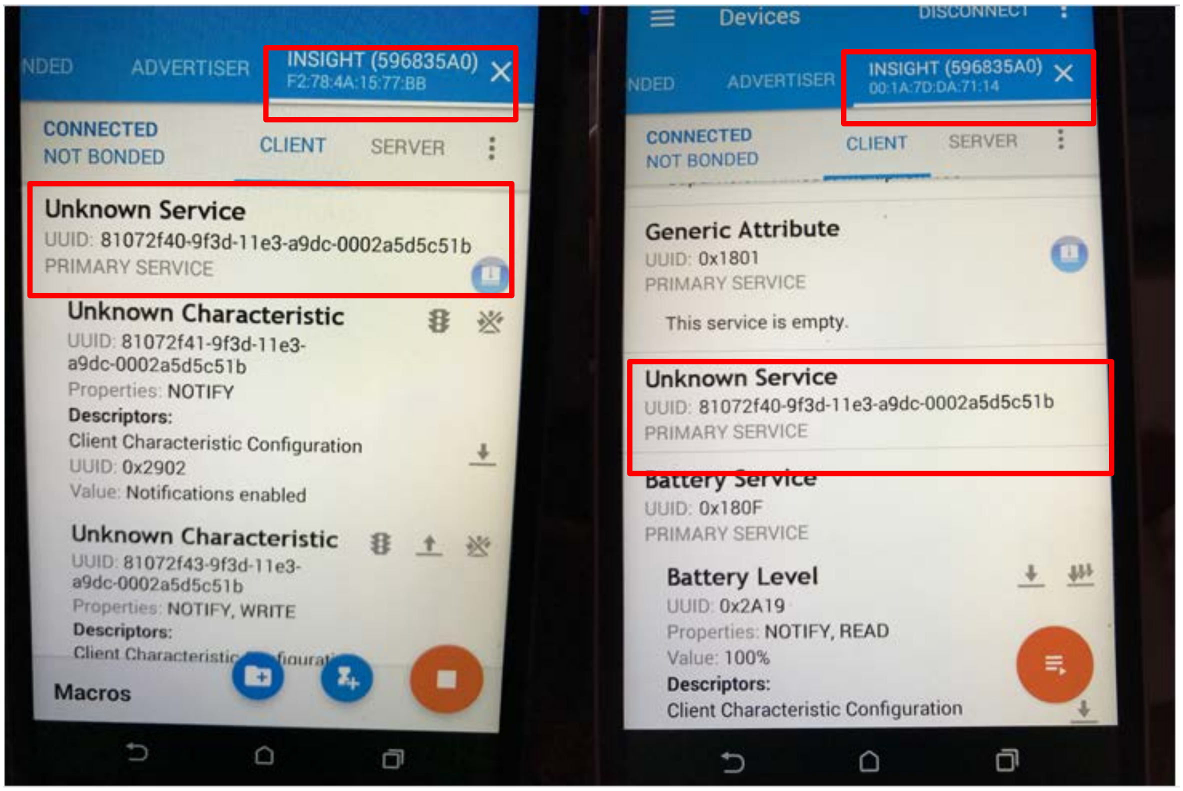
Device Name
UUID: 0x2A00
Properties: READ, WRITE

Appearance
UUID: 0x2A01
Properties: READ

Peripheral Preferred Connection Parameters
UUID: 0x2A04
Properties: READ

Generic Attribute
UUID: 0x1801
PRIMARY SERVICE

Figure 4.46 Real device on the left and fake device on the right



INSIGHT (596835A0)
F2:78:4A:15:77:BB

CONNECTED
NOT BONDED

Unknown Service
UUID: 81072f40-9f3d-11e3-a9dc-0002a5d5c51b
PRIMARY SERVICE

Unknown Characteristic
UUID: 81072f41-9f3d-11e3-a9dc-0002a5d5c51b
Properties: NOTIFY
Descriptors:
Client Characteristic Configuration
UUID: 0x2902
Value: Notifications enabled

Unknown Characteristic
UUID: 81072f43-9f3d-11e3-a9dc-0002a5d5c51b
Properties: NOTIFY, WRITE
Descriptors:
Client Characteristic Configuration

INSIGHT (596835A0)
00:1A:7D:DA:71:14

CONNECTED
NOT BONDED

Generic Attribute
UUID: 0x1801
PRIMARY SERVICE
This service is empty.

Unknown Service
UUID: 81072f40-9f3d-11e3-a9dc-0002a5d5c51b
PRIMARY SERVICE

Battery Service
UUID: 0x180F
PRIMARY SERVICE

Battery Level
UUID: 0x2A19
Properties: NOTIFY, READ
Value: 100%
Descriptors:
Client Characteristic Configuration

Figure 4.47 Real device on the left and fake device on the right

Figure 4.45 presents a screenshot of two Insight headsets with different mac address that look identical and have the serial number of the headset. Figures 4.46 and 4.47 present screenshots of the fake Insight headset which has a different mac address but does show the same characteristics and services such as the original. Both the images are placed side by side for comparison.

4.5 ANALYSIS

From the results obtained, an analysis leads to the determination that the information transmitted from the Emotiv Insight headset is not secure and can be captured and manipulated. With the most basic Bluetooth sniffer such as Adafruit BLE sniffer, the advertising data could be captured and also the pairing request sent by the Insight headset. Furthermore, with the Ubertooth-one, the data communication could be sniffed passively even after the pairing establishment between the Bluetooth devices which is achieved by using the Adafruit BLE sniffer. In addition, the Ubertooth-one could capture the pairing requests which is then decrypted by CrackLE. The Ubertooth-one was able to jam the connection by advertising bogus data packets preventing the smartphone from connecting with the Insight headset.

Finally, the Btlejuice framework could enable a MITM attack, an active interception replay attack, Denial of Service attack and a data modification attack. Active data sent for the brainware from the application could be actively captured which demonstrated that it is quite possible to cause damage to the individuals dependent on such devices for health and living.

4.6 CONCLUSION

Chapter 4 reported the results obtained from the experiment performed using the Insight headset. Some important findings are summarized below:

- The Adafruit BLE sniffer captured all advertising data transmitted from the Insight headset and the pairing information but ceased capturing upon pairing.
- The Ubertooth-one captures active communication between the Insight headset and the smartphone application. Furthermore, the captured data can then be decrypted by cracking the LTK.
- In addition, the Ubertooth-one jammed and interfered with the pairing request sent from the smartphone to the Insight headset.
- The Btlejuice enabled spoofing of the real device by creating a dummy device. The GATT data was intercepted. The intercepted data was then manipulated and forwarded to the headset.
- The Btlejuice also performed a replay attack and a hook attack wherein data was replayed again and sent back in the data stream. It could be looped to perform the same actions repeatedly.

Therefore, the results show that the information transmitted from a consumer grade Brain-Computer Interface device could be captured. In addition, the captured data could be sent back to the data stream and could be modified. The results obtained will be examined and discussed in Chapter 5. The results, research question and sub-questions will then be examined for final conclusions.

CHAPTER 5
DISCUSSION

5.0 INTRODUCTION

The intent of Chapter 5 is to develop and discuss the issues and problems in the use of Brain Computer Interfaces (BCIs) as summarized in Chapter 2 (Section 2.5). Furthermore, the empirical results obtained from Chapter 4 will be used to address the security and privacy issues described in Section 2.4.1 and Section 2.5. The review of similar studies aided in designing a methodology for data collection and analysis as presented in Section 3.3. Chapter 5 uses the evidence obtained through the implementation of the experimental design proposed in Chapter 4. The discussion will address the issues and challenges associated in the use of a BCI. Section 5.1 presents the findings relevant to testing the hypothesis. The findings obtained in Chapter 4 will be analyzed to test the hypothesis.

The hypothesis *That the data transmitted from a consumer grade Brain Computer Interface to the end user cannot be captured* is discussed in Section 5.1. Section 5.2 answers the sub questions SQ1 *What data can be captured from a communication session between the BCI and the user interface?* SQ2 *How can the pairing authentication information be interpreted?* SQ3 *How can the pairing between the BCI and the smartphone application be jammed?* SQ4 *How can captured information be substituted for a manipulated information exchange?* Section 5.3 answers the RQ *What are the security and privacy vulnerabilities for information in the use of Brain Computer Interface devices?* Section 5.4 evaluates the findings described in Chapter 4 with respect to the security and privacy issues discussed in Chapter 2. Section 5.5 concludes the discussion.

5.1 THE HYPOTHESIS

The hypothesis was generated through the appraisal of the research question and the sub questions as described in Section 3.2.2. The questions were generated by addressing the security and privacy issues in the use of BCIs summarized in Section 2.4.1. This section will evaluate the hypothesis in relation to the evidence for and against. Table 5.1 presents the results of the hypothesis test.

Table 5.1: Hypothesis testing

<table>
<tr><td colspan="2"><b>Hypothesis:</b> <i>That the data transmitted from a consumer grade Brain Computer Interface to the end user cannot be captured</i></td></tr>
<tr><td>FOR</td><td>AGAINST</td></tr>
<tr><td></td><td>Figure 4.11 presents a screenshot of the advertising data captured by the Adafruit BLE sniffer (Section 4.4.1)</td></tr>
<tr><td></td><td>Figure 4.12 and figure 4.13 present screenshots of the CONNECT_REQ parameter initiated from the smartphone (Section 4.4.1)</td></tr>
<tr><td></td><td>Figure 4.14 presents a screenshot of the pairing request received by the headset (Section 4.4.1).</td></tr>
<tr><td></td><td>Figure 4.16 presents a screenshot of an active ongoing communication between the smartphone application and the Insight headset captured by the Ubertooth-one (Section 4.4.2).</td></tr>
<tr><td></td><td>Figure 4.17 shows the CONNECT_REQ initiated by the smartphone (Section 4.4.2)</td></tr>
<tr><td></td><td>Figure 4.18 shows the transmitted data as LLU in the L2CAP layer that pushes the data to the ATT layer (Section 4.4.2)</td></tr>
<tr><td></td><td>Figure 4.23 displays the SCAN_REQ sent from the smartphone application to search the Insight headset (Section 4.4.2)</td></tr>
<tr><td></td><td>Figure 4.27 shows all the information regarding the pairing and exchange of credentials from the physical layer to the Low Energy Link Layer (LE_LL), L2CAP and then the SMP (Section 4.4.2)</td></tr>
<tr><td></td><td>Figure 4.39 shows the data sent from the smartphone application to the Insight Headset (Section 4.4.2)</td></tr>
</table>

Conclusion: The data transmitted from a consumer grade Brain Computer Interface to the end user can be captured.

5.2 SUB QUESTIONS

The intent of the research question is to define the objective of this research. To answer the research question, four sub questions have been generated. The purpose of these 4 sub questions is to ensure that the research question is answered. These four sub questions are answered in the following sub sections:

5.2.1 Sub Question 1

(SQ1) What data can be captured from a communication session between the BCI and the user interface?

Table 5.2: Sub Question 1

Evidence
The Adafruit BLE sniffer captured the advertising data broadcasted by the Insight headset (see Section 4.4.1).
The sniffer also captured the connection request initiated by the smartphone to connect to the Insight headset (Figure 4.13, Figure 4.17, see Section 4.4.1)
The connection request, the temporary key and the Long-Term key (LTK) was also captured and decrypted (see Section 4.4.2, Figure 4.27).
The GATT data is the raw data presented to the API of the smartphone application (see section 4.4.3, Figure 4.37, Figure 4.38 and Figure 4.39).

Answer: Various types of connection information and application layer data can be captured from a communication session between the BCI and the user interface.

5.2.2 Sub Question 2

(SQ2) How can the pairing authentication information be interpreted?

Table 5.3: Sub Question 2

EVIDENCE
Figure 4.17 presents a screenshot of the Linux terminal showing the CONNECT_REQ that contains the pairing authentication information
In the figure 4.17 the pairing information was advertised on channel 37 (see Section 4.4.2).
Figure 4.25 presents a screenshot of the Wireshark window showing the exchange of pairing information which is the LTK
Figure 4.26 presents a screenshot of two test filestest2 and test7 with the TK and the LTK. This LTK was used to decrypt the captured communication.
Figure 4.27 shows the decrypted communication showing the raw data from the physical to the application layer.

Answer: The pairing authentication information can be captured by the Ubertooth-one and can be analyzed using the CrackLE tool.

5.2.3 Sub Question 3

(SQ3) *How can the pairing between the BCI and the smartphone application be jammed?*

Table 5.4: Sub Question 3

EVIDENCE
Figure 4.21 presents a screenshot of the terminal showing the interference command (see Section 4.4.2).
Figure 4.22 shows the error message; the Insight could not be paired because of an incorrect PIN or passkey (see Section 4.4.2).

Answer: The pairing request can be jammed using the Ubertooth-one.

5.2.4 Sub Question 4

(SQ4) How can captured information be substituted for a manipulated information exchange?

Answer: The captured information can be substituted for a manipulated information using the Btlejuice MITM framework.

This shows that any information which has been captured can be substituted with any other information causing the data to be modified resulting in the malfunction of the Insight headset. Table 5.5 answers sub-question 4.

Table 5.5: Sub Question 4

EVIDENCE
Figure 4.28 presents a screenshot of the Btlejuice framework showing the Bluetooth dongle connecting to the real device and presenting the dummy device to the smartphone application (see Section 4.4.3)
Figure 4.31 shows that the services and characteristics associated with the real device has been discovered and the dummy device is ready to perform the replay attack (section 4.4.3).
Figure 4.36 shows the terminal highlighting the dummy connection accepted by the smartphone (see Section 4.4.3).
Figure 4.37 presents a screenshot of the intercepted data sent from the smartphone application to the Insight headset (see Section 4.4.3).
Figure 4.39 shows a dialogue box which allows on the fly modification of active data intended to be sent to the Insight headset (see Section 4.4.3).

5.3 THE RESEARCH QUESTION

Section 5.2 summarized the issues with the use of Brain Computer Interfaces leading to the research question described in Section 3.2.2. These issues have been evaluated through an extensive literature review described in Chapter 2

Sections 5.2 answered all the sub questions proposed in Chapter 3 (Section 3.2.2). Answering the sub-questions has aided in answering the research question. Table 5.6 presents the security and privacy vulnerabilities for information in the use of Brain Computer Interface devices.

Table 5.6: Research Question

Research Question: (RQ) *What are the security and privacy vulnerabilities for information in the use of Brain Computer Interface devices*	
Security and Privacy Vulnerabilities	Reference/Evidence
Advertising Data	All advertising data broadcasted by the Insight headset was captured. These advertising packets contained information such as the mac address of the headset, the advertising data and the channel on which the device is broadcasting (see Figure 4.11, Section 4.4.1).
Connection Request	The Adafruit BLE sniffer captured the connection request initiated by the smartphone to connect to the Insight headset. This connection request contained information such as the mac address of the smartphone and the connection parameters (see Figure 4.12, Section 4.4.1). Additionally, the connection request is not encrypted, and it is being advertised on channel 39 (see Figure 4.13, Section 4.4.1).
Passive Eavesdropping	The data captured contained all possible information such as the mac address, the data in the host layer, the attribute layer and the generic attribute profile. All these data from eavesdropping relates to the physical layer and the application layer of the Bluetooth protocol stack (see Figures 4.13, 4.14, 4.15 and 4.16). Furthermore Figure 4.18 shows the capturing of an active ongoing communication between the Insight headset and the smartphone application by the Ubertooth-one (see Section 4.4.2).
Pairing Credentials	The TK is exchanged between the Insight headset and the application creating a temporary connection to transmit

	the LTK for a successful encrypted connection (see Figure 4.25, and Figure 4.26, Section 4.4.2)
Communication Decrypted	The LTK derived using CrackLE was further used to decrypt the captured communication (Figure 4.26, Section 4.4.2).
Active Interception	The application layer data known as the Generic Attribute Profile (GATT) was intercepted using the Btlejuice MITM framework (see Figure 4.39, Section 4.4.3).
Denial of Service	The Ubertooth-one was used as a radio transmitter to jam or interfere with the connection. The pairing could be blocked rendering the device unusable (see Figure 4.21 and Figure 4.22, Section 4.4.2).
Replay Attack and Hook Data	The intercepted data could be selected and replayed again (see Figure 4.42 and Figure 4.43, Section 4.4.3).
Data modification attack	The intercepted data was modified and sent back into the data stream (see Figure 4.41, Figure 4.43 and Figure 4.44, Section 4.4.3).

5.4 DISCUSSION

Brain Computer Interfaces (BCIs) have emerged as a useful and accessible technological development. BCIs have had an impact for significant applications but the clinical applications have been most beneficial. Though the hardware setup for this experiment was difficult due to the complexity of the software and the hardware, once installed the attacks could be performed with ease. The attacks could be achieved with very cheap hardware and the exploitations also. The simplicity of the attacks provided a gateway for more sophisticated attacks. In this research, a wide range of security and privacy vulnerabilities have been determined. This Section 5.4 will discuss the important attacks that are possible to cause damage to the individual using a BCI for a medical dependency. Five types of attacks have been briefly highlighted with the possible repercussions for the Brain Computer Interface user. They are as follows:

5.4.1 Passive Eavesdropping

- Passive Eavesdropping: It was possible to intercept the ongoing communication between the BCI and the application (see Figures 4.13, 4.14, 4.16, 4.17, 4.18, 4.24, 4.25, 4.26, 4.27 and 4.37).

  Repercussion: Intricate details including the device name, the pairing information, the application layer data was revealed using the Ubertooth-one. Any individual using a BCI for motor movement could be at risk of confidential information being exposed. As passive eavesdropping leads to the determination of the LTK, the active ongoing communication could be decrypted to understand the data in a plaintext format.

5.4.2 Active Interception

- Active Interception: Using the Btlejuice framework, active application layer could be intercepted with an option either to forward the data packet to the headset or to drop the packet (see Figure 4.39 and 4.40). A dummy device was set up to match the services and characteristics associated with the Insight headset (see Figure 4.38). This dummy device was used to fool the application that it is the original Insight headset by spoofing the characteristics and services of the Insight headset. The nrf application was used to list both the devices which were identical as per the name and the model but differ in the mac address (see Figure 4.45, 4.46 and 4.47).

  Repercussion: Many of individuals are dependent on BCIs for clinical applications such as neuroprosthetic arms and controlling wheelchairs (see Section 2.3.4). Furthermore, individuals suffering from Amyotrophic lateral sclerosis (ALS) depend on BCIs to regain muscular movements. An attacker could simply step into the vicinity of the individual and snoop on every single data transmitted by the BCI and causing them to malfunction using simple commands. For example, the individual using the Insight headset is thinking to push the chair forward, the command is sent from the application using the training data but if the push data is intercepted and not forwarded, then the headset will never perform the intended function and the individual would not be able to drive the wheelchair.

5.4.3 Denial of Service

- Denial of Service: The pairing request initiated from the smartphone to connect to the BCI could be blocked using the Ubertooth-one (see Figure 4.22).
  Repercussion: This attack is a very simple form of attack but has a serious effect on the individual. There are individuals using the BCI for neurorehabilitation. This essential for individuals who have had weak muscular movements. Preventing the device from pairing with the smartphone can render the device functionless thereby causing damage to the individual.

5.4.4. Replay Attack

- Replay Attack: A specific data for a command or a thought in the form of data could be replayed back in the data stream.
  Repercussion: Individuals with neuroprosthetic arms don't have motor neurons to control muscular movements. Instead, BCIs have been designed to translate the electrophysiological signals to machine language which will control the movement of the prosthetic arms. If the individual is trying to lift an object, replaying a specific action will restrict the individual from completing a specific action.

5.4.5 Data Modification

- Data Modification: The intercepted data could be modified and forwarded to the headset (see Figure 4.43 and 4.44).
  Repercussion: This attack would trick the device into performing a different function rather than what it is designed to execute. For example, an individual using the BCI is using to spell the words using a P300 speller, every character or neural signal for the specific letter can be modified and forwarded to the BCI. On the other hand, the movements of prosthetic arms can also be controlled and modified using the Btlejuice framework (see Figure 4.41).

The vulnerabilities determined from various tests shows that the information transmitted from a consumer grade Brain Computer Interface (BCI) is not secure and can be tampered. The privacy and the security issues described in Chapter 2 (Section 2.4.1) have given a base to determine additional vulnerabilities and issues with the information transfer associated in the use of the BCI. The issues summarized in Section 2.5 and the similarity studies analyzed in Chapter 3 have aided in the designing of the research methodology for this thesis and have flagged added weaknesses in the use of BCIs.

5.5 CONCLUSION

Chapter 5 discussed the findings presented in Chapter 4. This discussion has rendered the hypothesis *That the data transmitted from a consumer grade Brain Computer Interface to the end user cannot be captured* to be falsified as the information could be captured. Furthermore, the hypothesis was tested by answering the sub-questions and then eventually the research question. Chapter 6 will conclude the research by investigating possible limitations to the research, identify areas for further research and end with my critical reflection as a personal journey of learning through the research.

CHAPTER 6
CONCLUSION

6.0 INTRODUCTION

The research had a strong literature that aided in determining the possible security flaws for exchange of information between the Brain Computer Interface and the smartphone application. Chapter 2 described the existing security and privacy issues in the use of BCIs (Section 2.4.1). The issues summarized in Section 2.5 lead to the research question (Section 3.2.3) and the results obtained in Chapter 4. A review of similar studies (Sections 3.1.1 to 3.1.5) aided the design of the research methodology. The results were used to test the hypotheses and also answer the research question and sub questions. The findings show that the hypotheses failed. Answers to the research question have been briefly discussed in Section 5.3. Chapter 6 presents the conclusion of this research. Section 6.1 presents the limitations associated with this thesis in terms of scope, perception and generalization. Section 6.2 suggests areas that would benefit from future research. Section 6.3 discusses my personal journey in this thesis and finally Section 6.4 gives the final conclusion to this research.

6.1 LIMITATIONS

This section addresses the limitations associated with the research and pin points specific limitations which have impacted the transfer of this research. Sub sections 6.1.1 to 6.1.3 describe the limitations in terms of scope, perception and generalization

6.1.1 Scope

To determine the scope of this research, limitations needed to be assessed with respect to the software and the hardware requirements. Though, several Bluetooth sniffers were available to test the Brain Computer Interface, the research was designed with minimalistic requirements to maximize the output of the testing. Emotiv designs two variants of BCI, the Insight and the EPOC. Emotiv Insight is a consumer grade BCI which has an in-built processesor responsible for capturing the electrophysiological signals and forwarding them to the end user. Emotiv Insight only has 5 channels whereas the EPOC is 14 channel BCI for research. With the research budget, the device had to be limited to the Emotiv Insight. In addition, the motive was to test this headset with a basic hardware configuration for a laptop. The test bench was designed with readily available hardware. The attack model was divided into segments of attack types which gave feasibility for a potential MITM attack and a data modification attack. The scope of this research was limited to vulnerability testing on the Emotiv Insight with simple sniffing hardware and tests for the security in the transfer of information.

6.1.2 Perception

During the research phase, it was observed that there were few frameworks designed to perform vulnerability testing for BCI technologies. There are a limited number of vulnerability testing frameworks for Bluetooth 4.0 available but the results derived using the Btlejuice framework showed effective interception of active application layer data and export all the application layer data (Section 4.3.1, Section 4.4.1 and Section 4.4.3). The. pcap files and log files obtained using the sniffers are results which were used to test the hypothesis to determine the fail/not fail result. The research can therefore be extended to investigate the perception of limited available resources.

6.1.3 Generalization

The generalization of the choice of the sniffing hardware and the threat model was described in Section 3.1.2 and Section 3.1.4. The approach defined in the similar studies discusses the feasibility of passive eavesdropping and intercepting data transferred to and from the Brain Computer Interface. The Adafruit BLE sniffer and the Ubertooth-one can record and export data into Wireshark and also run live capturing featuring all significant information being exchanged between Emotiv Insight and the smartphone. The sniffing hardware has the ability of continuously monitoring the security associated with various modem wearables including the Emotiv Insight, smart watches, and so on. Also the sniffers, including Btlejuice were therefore tested to check the vulnerabilities in relation to information exchange. Furthermore, the framework enabled the extraction of data from the application layer presented to the Application Programming Interface (API) on the smartphone. This framework can be deployed to perform vulnerability assessment for most devices using Bluetooth 4.0.

6.2 FUTURE RESEARCH

The limitations addressed in Section 6.1 may be mitigated through future research. The sub-sections below discuss various directions for future research, such as framework testing, tools development and BCI standards.

6.2.1 Framework Testing

The development of a testing framework will enable the testing of Brain Computer Interfaces (BCIs) for privacy and security issues in the transfer of information. The Btlejuice framework developed for the Linux platform is a Man In The Middle (MITM) framework designed for man in the middle attacks in Bluetooth 4.0/Bluetooth Low Energy/Bluetooth Smart. This framework will aid in determining flaws associated with the security and privacy for information. Most of the devices programmed to function on Bluetooth 4.0 include wearable technology, smart locks for houses, insulin pumps, smartwatches and fitness trackers. All these devices can be tested with this framework, and security vulnerabilities may be evaluated and mitigated.

6.2.2 Tools

The investigation of data captured using the sniffers was analyzed using Wireshark. The sniffers designed to capture Bluetooth data or Wireless data are mostly designed to dump files into Wireshark. The Adafruit BLE sniffer and the Ubertooth-one are cheap and affordable tools that disclose information vulnerabilities. The Emotiv Insight is a consumer grade BCI which has an in-built motherboard converting neural signals to digital signals and the information can be easily captured. The Emotiv EPOC has 14 channels with an open end transmitting raw signals as well. The capturing of data will be easier as compared to the Insight. Furthermore, BCIs should be tested with complex sniffing hardware to eliminate possible security vulnerabilities and ensure safety, security and privacy to the individual is fully tested.

6.2.3 BCI Standards

Brain Computer Interface technology is starting to gain regular use for medical purposes especially for individuals with motor disability. Furthermore, it is enabling people with speaking disability to control external spelling software translating their neural signals enabling them to spell words with their thoughts. BCIs have also been employed for neurorehabilitation and have shown promising effects on individuals recovering from brain strokes. This technology is has proven to be beneficial and expected to expand in use over the next decade. There is a need for certain protocols or standards that all BCIs must meet before being approved for consumer use. The test bench proposed in this thesis will help gauge the shortcomings in the use of BCIs which can be set as pre-requirement testing to ensure the information is safe and secure, so the individual is not exposed to dangerous risks.

6.3 PERSONAL JOURNEY

My personal journey began with doubts that Brain Computer Interface (BCI) technology is secure. Hence, I wanted to determine the flaws associated with use. I began reviewing different types of consumer grade BCIs such as Neurosky, Muse and Emotiv. I decided to use the Emotiv Insight as it had 5 channels and had better functionality as compared to its competitors. In addition, it is a consumer grade BCI which is aimed for consumer use. After acquiring the Emotiv Insight, I started understanding the working of the device and the training sets required for functionality improvement. This headset could be used to control external devices such as wheelchairs and prosthetic arms. After gathering sufficient information about the headset, I started developing my literature review. On reviewing literature, I started to understand the working of information transfer from the BCI to the end user and analyzed similar studies which helped me develop my methodology. I learnt that the simple headsets were difficult to be tested as compared to the expensive ones such as the Emotiv EPOC.

After training the headset, I had to find a Bluetooth sniffer which could potentially capture information transmitted by the headset. On researching about Bluetooth sniffers, the Adafruit BLE sniffer was the cheapest hardware available. Then experimenting with the hardware, I found only a specific version of Wireshark was supported, version 1.12. The Adafruit BLE sniffer worked effortlessly on the Windows platform. After capturing data from the headset, I came across a limitation that the data capture would come to a halt as soon as the headset was connected to the application of the smartphone. This proved that this sniffing hardware could only capture advertising data and services associated with the headset but not the actual data that is transmitted between the BCI and the application. My search for an advanced Bluetooth sniffer found a sniffer which could capture data after the Insight connecting to the smartphone. I learned that cheap hardware has limitations and requires innovation and technical support .

All thanks to Michael Ossman who developed the Ubertooth-one. The Ubertooth-one is one of the most affordable Bluetooth sniffer capable of multiple functions including passive eavesdropping, faking a bogus device with continuously changing the Bluetooth mac address consistently. Furthermore, the Ubertooth-one was also capable of capturing the Long term key and all kind of pairing information that was later used to decrypt the entire communication it captured. On acquiring the Ubertooth-one, I had to test different distributions of Linux including Kali Linux and Ubuntu. Updating the firmware on the

Ubertooth-one was easy. I had to jumper a couple of PINs which finally enabled the firmware to update. After the firmware updated, the Ubertooth-one worked well. By this time, I started documenting my research findings and followed the research design proposed through the methodology in Chapter 3. The Ubertooth-one could passively capture an ongoing communication between the BCI and the smartphone, but data injection was not possible. Injecting and modifying the captured data was the missing puzzle. At the initial stages of setting up the Ubertooth-one the firmware could not be flashed on the device. I began researching numerous forums and the GitHub Forum for the Ubertooth-one. It was great to have the developer of the tool to reply back with the answers which eventually helped me to configure the Ubertooth-one.

I started to explore all applications which could enable a much more complex attack vector. That is when, I came across the Btlejuice framework developed by Damien Cauqill. The Btlejuice installation was the most tedious part of the entire thesis. The pre-requisites for the Btlejuice framework had to be individually installed and some of them were not even available. I had to email the developer to check for those plugins. After getting access to the required plugins, the Btlejuice framework was installed. It had to be installed on two different machines and required careful attention to the most minor plugin because as the framework would not launch properly and would give errors. After installing the dependencies, the framework enabled various types of attacks and aided in answering the research question and testing of the hypothesis. The hardest phase that I experienced throughout the installation of the framework was the requirement of specific version of the plugins required for the Btlejuice to function correctly. I learnt that the plugins required needed to be installed in an order and only with compatible versions for the software to work correctly in Linux.

The results were further discussed in Chapter 5 highlighting the privacy and security vulnerabilities associated in the information transmitted from the Emotiv Insight to the smartphone. These results helped me in understanding the security vulnerabilities and issues involved in the information transfer. Furthermore, the MITM attack proved that a simple attack can have major repercussions. I also learnt that the security protection is not 100% but can be thwarted by simple and cheap tools.

In conclusion, my personal journey involved change and adaptation, and learning of underlying layers associated with the Bluetooth Low Energy protocol stack. In addition, I focused on my similar studies review, specifically Section 3.1.4, as the study involved a similar testing set up with an implantable medical device. These findings are significant in understanding the security involved in data transfer and addresses the vulnerabilities which may be mitigated with future research, and manufacturing standardization.

6.4 CONCLUSION

Brain Computer Interfaces (BCI) have been an emerging technology which has aided individuals to manage their disabilities and abilities. Many of the modern day wearables are being used widely by people to monitor their stress levels, interest levels, heart rates and personal social networks. This thesis reported potential vulnerabilities and the feasibility for an attacker to cause harm to an individual. Security cannot be improved instantly. It is a slow and steady process. The significance of this research is to emphasize security and privacy in the design and the use of the BCI. With recent malware such blueborne, attacking Bluetooth low energy devices, it is easier to successfully attack and use minimal hardware. Researchers from the BCI community should develop frameworks and standards so that all the companies manufacturing such technologies must meet specified requirements. The information protection requires extensive black box and white box testing, vulnerability assessment and a full risk assessment, prior to release.

REFERENCES

Allison, B., Graimann, B., & Gräser, A. (2007). Why use a BCI if you are healthy Symposium conducted at the meeting of the ACE Workshop-Brain-Computer Interfaces and Games, Germany.

Ang, K. K., Guan, C., Chua, K. S. G., Ang, B. T., Kuah, C., Wang, C., Zhang, H. (2010). Clinical study of neurorehabilitation in stroke using EEG-based motor imagery brain-computer interface with robotic feedback*IEEE.* Symposium conducted at the meeting of the Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE, France.

Blinowska, K., & Durka, P. (2006). Electroencephalography (eeg). *Wiley Encyclopedia of Biomedical Engineering,Warszawa, Poland*.

Bonaci, T., Calo, R., & Chizeck, H. J. (2014). App stores for the brain: Privacy & security in Brain-Computer Interfaces*IEEE.* Symposium conducted at the meeting of the Ethics in Science, Technology and Engineering, 2014 IEEE International Symposium Chicago, IL, USA.

Bright, D., Nair, A., Salvekar, D., & Bhisikar, S. (2016). EEG-based brain controlled prosthetic arm. *IEEE.* Symposium conducted at the meeting of the Conference on Advances in Signal Processing (CASP), Pune, India.

Chang, K.-H. (2014). Bluetooth: a viable solution for IoT?. *IEEE Wireless Communications, 21*(6), 6-7.

Conti, M., Mancini, L. V., Spolaor, R., & Verde, N. V. (2015). Can't you hear me knocking: Identification of user actions on android apps via traffic analysis*ACM.* Symposium conducted at the meeting of the Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, Shanghai, China.

Da Silva, F. L. (1996). The generation of electric and magnetic signals of the brain by local networks. In *Comprehensive human physiology* (pp. 509-531): Springer.

Darvas, F., Pantazis, D., Kucukaltun-Yildirim, E., & Leahy, R. (2004). Mapping human brain function with MEG and EEG: methods and validation. *NeuroImage, 23*, S289-S299.

Denning, T., Matsuoka, Y., & Kohno, T. (2009). Neurosecurity: security and privacy for neural devices. *Neurosurgical Focus, 27*(1), E7.

Donoghue, J. P. (2002). Connecting cortex to machines: recent advances in brain interfaces. *Nature neuroscience, 5*, 1085-1088.

Fazel-Rezai, R., Allison, B. Z., Guger, C., Sellers, E. W., Kleih, S. C., & Kübler, A. (2012). P300 brain computer interface: current challenges and emerging trends. *Frontiers in neuroengineering, 5*, 14.

Finke, A., Lenhardt, A., & Ritter, H. (2009). The MindGame: a P300-based brain–computer interface game. *Neural Networks, 22*(9), 1329-1333.

Forstmann, B. U., & Wagenmakers, E.-J. (2015). Model-based cognitive neuroscience: A conceptual introduction. In *An introduction to model-based cognitive neuroscience* (pp. 139-156): Springer.

Frank, M., Hwu, T., Jain, S., Knight, R., Martinovic, I., Mittal, P., Song, D. (2013). Subliminal probing for private information via EEG-based BCI devices. *arXiv preprint arXiv:1312.6052*.

Golub, M. D., Chase, S. M., Batista, A. P., & Byron, M. Y. (2016). Brain–computer interfaces for dissecting cognitive processes underlying sensorimotor control. *Current opinion in neurobiology, 37*, 53-58.

Hjelm, S. I., & Browall, C. (2000). Brainball-using brain activity for cool competition Symposium conducted at the meeting of the Proceedings of NordiCHI.

Huettel, S. A., & McCarthy, G. (2004). What is odd in the oddball task?: Prefrontal cortex is activated by dynamic changes in response strategy. *Neuropsychologia, 42*(3), 379-386.

Jeunet, C., Jahanpour, E., & Lotte, F. (2016). Why standard brain-computer interface (BCI) training protocols should be changed: an experimental study. *Journal of neural engineering, 13*(3), 036024.

Johnson, B., Maillart, T., & Chuang, J. (2014). My thoughts are not your thoughts*ACM.* Symposium conducted at the meeting of the Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication.

Kroeker, K. L. (2011). improving Brain-computer interfaces. *Communications of the ACM, 54*(10), 11-14.

Lauer, R. T., Peckham, P. H., Kilgore, K. L., & Heetderks, W. J. (2000). Applications of cortical signals to neuroprosthetic control: a critical review. *IEEE transactions on rehabilitation engineering, 8*(2), 205-208.

Li, Q., Ding, D., & Conti, M. (2015). Brain-computer interface applications: Security and privacy challenges*IEEE.* Symposium conducted at the meeting of the Communications and Network Security (CNS).

Mak, J. N., & Wolpaw, J. R. (2009). Clinical applications of brain-computer interfaces: current state and future prospects. *IEEE reviews in biomedical engineering, 2*, 187-199.

Martinovic, I., Davies, D., Frank, M., Perito, D., Ros, T., & Song, D. (2012). On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces Symposium conducted at the meeting of the USENIX security symposium.

Millan, J. R., Renkens, F., Mourino, J., & Gerstner, W. (2004). Noninvasive brain-actuated control of a mobile robot by human EEG. *IEEE Transactions on biomedical engineering, 51*(6), 1026-1033.

Miranda, R. A., Casebeer, W. D., Hein, A. M., Judy, J. W., Krotkov, E. P., Laabs, T. L., Sanchez, J. C. (2015). DARPA-funded efforts in the development of novel brain–computer interface technologies. *Journal of neuroscience methods, 244*, 52-67.

Moore, M. M. (2003). Real-world applications for brain-computer interface technology. *IEEE Transactions on neural systems and rehabilitation engineering, 11*(2), 162-165.

Nijholt, A., Bos, D. P.-O., & Reuderink, B. (2009). Turning shortcomings into challenges: Brain–computer interfaces for games. *Entertainment computing, 1*(2), 85-94.

Nunez, P. (1981). Electric® elds of the brain: New York: Oxford University Press.

Pasqualotto, E., Federici, S., & Belardinelli, M. O. (2012). Toward functioning and usable brain–computer interfaces (BCIs): a literature review. *Disability and Rehabilitation: Assistive Technology, 7*(2), 89-103.

Pattnaik, P. K., & Sarraf, J. (2016). Brain Computer Interface issues on hand movement. *Journal of King Saud University-Computer and Information Sciences*.

Rains, G. D. (2001). *Principles of human neuropsychology* (First ed.): McGraw-Hill. Retrieved from https://books.google.co.nz/books?id=rZruAAAAMAAJ

Ramadan, R. A., & Vasilakos, A. V. (2017). Brain computer interface: control signals review. *Neurocomputing, 223*, 26-44.

Rushanan, M., Rubin, A. D., Kune, D. F., & Swanson, C. M. (2014). SoK: Security and privacy in implantable medical devices and body area networks*IEEE.* Symposium conducted at the meeting of the Security and Privacy (SP), 2014, San Jose, California.

Salhi, J., MacLaurin, J., & Toumi, S. (2016). Mean Field Dynamics of a Network of Wilson-Cowan Neurons with Electrical Synapses. *arXiv preprint arXiv:1601.05572*.

Schalk, G., McFarland, D. J., Hinterberger, T., Birbaumer, N., & Wolpaw, J. R. (2004). BCI2000: a general-purpose brain-computer interface (BCI) system. *IEEE Transactions on biomedical engineering, 51*(6), 1034-1043.

Scherer, R., Moitzi, G., Daly, I., & Müller-Putz, G. R. (2013). On the use of games for noninvasive eeg-based functional brain mapping. *IEEE Transactions on Computational Intelligence and AI in Games, 5*(2), 155-163.

Sutton, S., Tueting, P., Zubin, J., & John, E. R. (1967). Information delivery and the sensory evoked potential. *Science, 155*(3768), 1436-1439.

Thomas, K. P., & Vinod, A. (2016). Utilizing individual alpha frequency and delta band power in EEG based biometric recognition*IEEE.* Symposium conducted at the meeting of the Systems, Man, and Cybernetics (SMC), 2016 IEEE International Conference, Taiwan.

Verschuere, B., Crombez, G., Koster, E. H., & De Clercq, A. (2007). Antisociality, underarousal and the validity of the Concealed Information Polygraph Test. *Biological Psychology, 74*(3), 309-318.

Wang, H., Chang, W., & Zhang, C. (2016). Functional brain network and multichannel analysis for the P300-based brain computer interface system of lying detection. *Expert Systems with Applications, 53*, 117-128.

Wang, Q., Sourina, O., & Nguyen, M. K. (2010). Eeg-based" serious" games design for medical applications*IEEE.* Symposium conducted at the meeting of the Cyberworlds (cw), 2010 international conference, Hong Kong.

Wolpaw, J. R., Birbaumer, N., McFarland, D. J., Pfurtscheller, G., & Vaughan, T. M. (2002). Brain–computer interfaces for communication and control. *Clinical neurophysiology, 113*(6), 767-791.

Wolpe, P. R., Foster, K. R., & Langleben, D. D. (2005). Emerging neurotechnologies for lie-detection: promises and perils. *The American Journal of Bioethics, 5*(2), 39-49.

Wyckoff, S. N., Sherlin, L. H., Ford, N. L., & Dalke, D. (2015). Validation of a wireless dry electrode system for electroencephalography. *Journal of neuroengineering and rehabilitation, 12*(1), 95.