2017

Neurosecurity for brainware devices

Brian Cusack
Auckland University of Technology

Kaushik Sundararajan
Auckland University of Technology

Reza Khaleghparast
Auckland University of Technology

Recommended Citation

Cusack, B., Sundararajan, K., & Khaleghparast, R. (2017). Neurosecurity for brainware devices. DOI: https://doi.org/10.4225/75/5a84ee2895b45

DOI: 10.4225/75/5a84ee2895b45
Cusack, B., Sundararajan, K., & Khaleghparast, R. (2017). Neurosecurity for brainware devices. In Valli, C. (Ed.). (2017). The Proceedings of 15th Australian Information Security Management Conference, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia. (pp.49-56).

NEUROSECURITY FOR BRAINWARE DEVICES

Brian Cusack, Kaushik Sundararajan, Reza Khaleghparast
Cyber Forensic Research Centre, Auckland University of Technology, Auckland, New Zealand
brian.cusack@aut.ac.nz, kaushik.sundararajan@gmail.com, khaleghparast@live.com

Abstract

Brainware has a long history of development down into the present day where very simple and usable devices are available to train for the control of games and services. One of the big areas of application has been in the health sciences to provide compensatory control to humans who may lack the usual capabilities. Our concern has been the protection of information in brainware so that a human intention may have confidentiality, integrity, and accessibility to the required implementation mechanisms for services. The research question was: What are the consequences of security failure in brainware? Our research tested a brainware device and found vulnerabilities. The most significant vulnerability was the ability to capture and inject communication packets so that a human intention could be hijacked. The consequences of this communication failure are for psychological harm to the human and unplanned for actions in the material environment.

Keywords: Security, Failure, Brainware, Hijacking, Harm

INTRODUCTION

Electro activity in the human brain has been studied for over a century and various applications devised that enhance human capabilities in areas where capability may be deficient. In particular thinking ability and motor control have been beneficiaries of brainware devices (Allison, et al., 2007; da Silva, 1996). Significant progress has been made from the times when invasive surgical operations were required to insert brainware devices inside a human brain to gain the benefits. Today brainware has become nonintrusive and the latest advancements have dry electrodes that sit on the human head collecting the electro activity of the brain (Wyecoff, et al., 2015). These are significant technological advancements that provide ease of use and ready access for research and learning. Some are woven inside baseball caps and other socially integrated headgear, and the device acts as an inconspicuous aid for enhanced human capability (Bonaci, et al., 2014; Kroeker, 2011). The headsets are also relatively inexpensive and available for purchase online or in gaming and electronics shops. They can be trained to control a wide variety of applications including, model cars, wheelchairs and games (Wolpaw et al., 2002). The simplest ones have a single electrode and minimal control functions such as up, down, left, and right; which is sufficient for a toy or a computer game. Other headsets have 14 and more electrodes and a greatly increased capacity to harness a wider variety of emotions in the human brain and to create a more refined control interface. The use of brainware is relatively simple once it has been trained (Jeunet, et al., 2016; Donoghue, 2002). The training of brainware software is similar to the training of voice activation and transcription software. The user in each situation has to go through a series of standardised algorithms that link the human variability to the standardised software processes. In brainware that is used for playing a game or controlling a wheelchair, the user has to think and not to move or speak. So for example, if I was training my brainware application to steer a remote control car, I would have to continue to think the word “left” until the electro activity in my brain mapped onto the preprogramed software for turning the car left. Sometimes the matching takes longer than others but providing the user is prepared to concentrate and put in the time to train the software, the effects are created by thinking. In the radio controlled car situation, once the brain-ware is trained, then it is possible to put on the headset, look at the remote control car (power on in car) and control its movement up to approximately 3 meters by using the correct thoughts. Similarly, for the training of the control of a wheelchair and other medical applications the user has to spend time synchronising their electro brain activity with the application they wish to use, but once completed the communication is relatively effective (Millan, et al., 2004).

A significant problem for human behaviour and human psychological stability arises once the user has trained the brainware to perform particular functions. If the application does not behave in the ways that it has been trained and the user expectation satisfied, the relationship is destabilised and the effectiveness of the technology undermined. There are several ways that this may occur but our specific research interest was in the situation were the brainware is hacked and unexpected responses to thoughts are presented to the user (Denning, et al., 2004). In this situation many unintended human behaviours may be demonstrated and the purpose of the technological advantage lost. Consequently our research took a brainware device and tested it for security vulnerabilities

(Martinovic, et al., 2012; Li, et al,. 2015). The results show that the communication between the headset and the computer interface or the device has vulnerabilities that disclose information regarding the intended control function and the brain to device mapping. We also performed test attacks to disconnect the thought from its intended action. In this research our objective was to demonstrate the vulnerabilities in the use of brainware, but anecdotally it was obvious the intervention had a negative impact on the user. Our concern is that suitable consideration is given to the securing of the communication between the headset and the devices so that the user intention is conveyed through to the effect. The implication of disruption in the communication channel is for unplanned actions, frustration and potential harm to the user. The consequences may be insignificant when a remote control car is being used for fun, but it is a much more serious case when humans are controlling prosthetic arms, wheelchairs, and sufficing control effects (Wolpaw, et al., 2002; Kroeker, 2011; Lauer, et al., 2000).

Other writers have defined Neurosecurity as the protection of neural devices from adversaries trying to exploit, block, eavesdrop, or generally disrupt neural signals (da Silver, 1996; Darvis, et al., 2004; Nijholt, et al., 2009). Confidentiality is critical in maintaining the privacy of information and it is for the developers to assure that the properties of the device cannot be exploited to disclose signals or any other protected information (Lauer, et al., 2000; Golub, et al., 2016; Li, et al., 2015). Similarly, an attacker should not be able to change device settings or initiate unauthorised operations that compromise the integrity of the device and its information. The availability of the device for clear and intended communication requires strong security measures. Neuro security is consequently the protection of confidentiality, integrity, and availability of the neural devices for the intended user, in such a way that the safety of a person's neural mechanisms, neural computation, and free will, are protected (Millan, et al., 2004). Our laboratory tests on devices suggest that neural security is lagging in some readily available brainware headsets on the market today.

DEVICE TESTING

The brain computer interface (BCI) consists of four components and a connecting signal (see figure 1). BCI requires a human user who has a sensing device that collects the electro chemical energy transmissions from the brain. The sensing device communicates to a signal processing module that puts the sensor signals into a manageable format for transmission either through wired or wireless media. The forth component is an application that will drive an effect, such as movement, decisions, control, and so on.

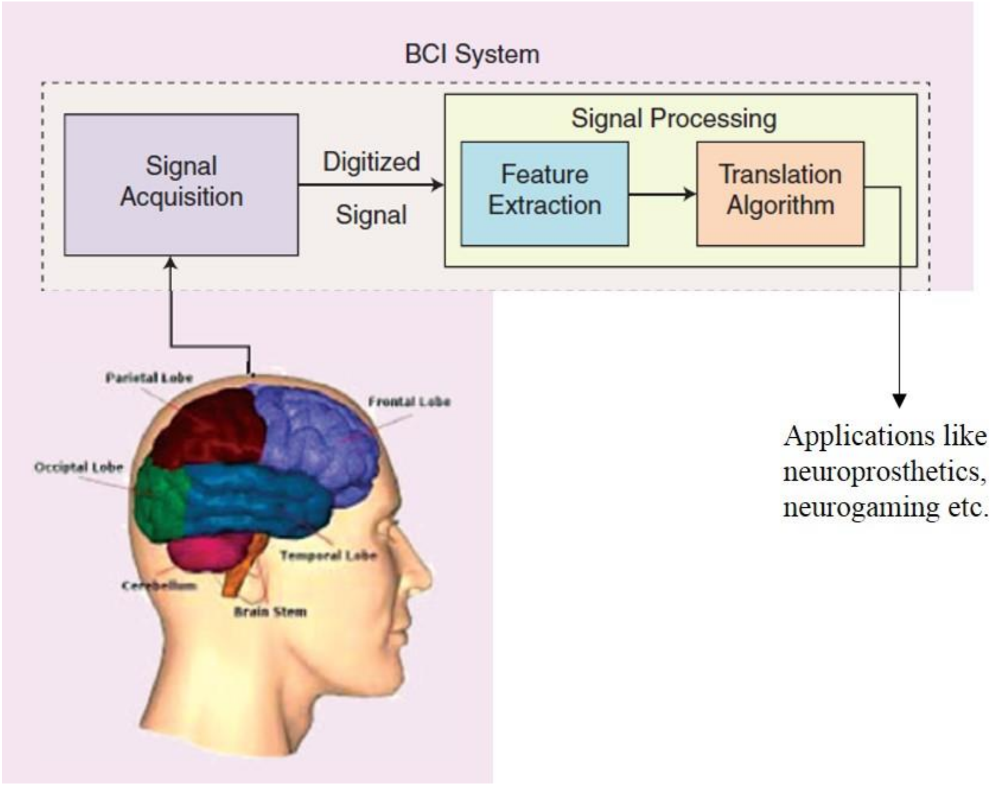


Figure 1. Brain Computer Interface Architecture

We chose the Emotiv Insight 5 channel EEG headset for testing. The Emotiv Insight is designed to detect performance levels of certain parameters that include the human 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 shows 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 for information conditioning. Once all the five channels are green then training can begin, and once trained the headset can be used many times by the same user.

Figure 2. Emotiv Insight 5 channel EEG headset (Emotiv, 2016)

Previous research has established the vulnerability of devices to disclose critical information when tethering in Bluetooth wireless networks (Li, Ding, Conti, 2015). We assumed the vulnerability and only briefly checked the matter to confirm the problem and potential violation of confidentiality. However, this research was concerned with intervention in the communication between the headset and the device. Could we hijack the headset control and substitute alternative commands, unknown to the user; and hence, violate the integrity of the system?

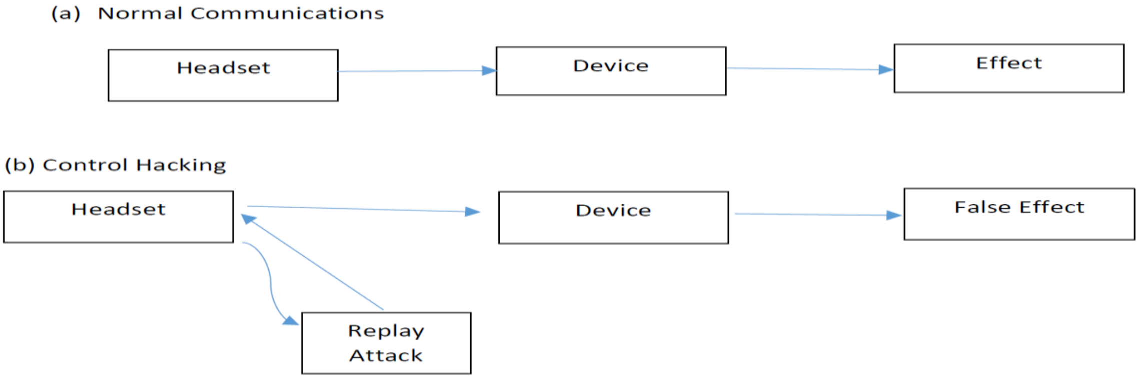
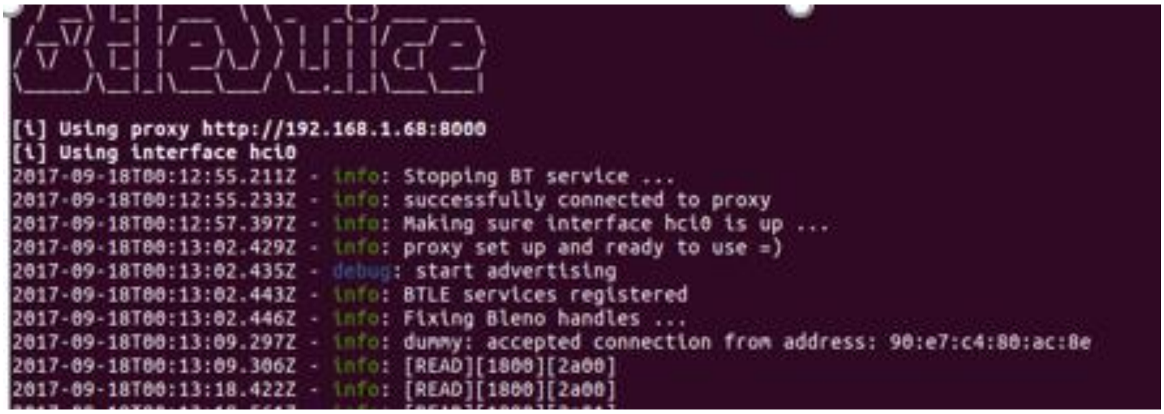


Figure 3. Research Design

Consequently, the Ubertooth-one and Adafruit sniffers were not capable of manipulating and resending changed packets, and hence a framework called ‘Btlejuice’ was deployed. The framework makes use of external Bluetooth dongles CSR 4.0, creates a clone of the target device, and intercepts the Bluetooth General Attribute Profile (GATT) from the top most layer of the Bluetooth protocol stack. The support software requires setting the target device (the headset), and then double clicking the headset icon so that the Bluetooth dongle proxies the services and characteristics of the Insight headset and pairs with the headset. The packets are then captured on the proxy for manipulation and the system tricked into accepting the proxy communications in a replay attack. Figure 3a shows the normal information flow between the headset and the device and figure 3b how we hijack and replay fake messages to alter the device effect.

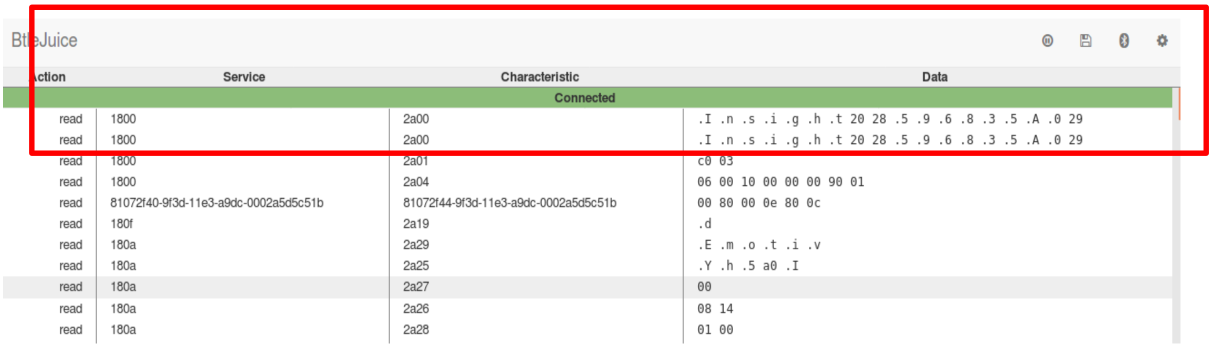
RESULTS

The implementation of the research design was challenging as we had to customise many of the tools used to fit the context. Similarly we had to access the Emotive code layer in order to audit the findings. Initially the standard Bluetooth sniffing tools functioned as expected and easily compromised the confidentiality of the communication between the headset and the device. However, the violation of communication integrity required the implementation of the Btlejuice system of hardware and software in order to create replay attacks that changed the intended device effects. The headset communication was connected to a proxy client which had the same characteristics and services as the Insight headset. On launching the application called Mental Commands, a dummy headset is displayed on the proxy, and can be manipulated to recreate any of the headset commands. The compromised commands were then sent back to the headset to broadcast to the device. As soon as the proxy application connects to the headset, the Btlejuice suite starts to capture all the data sent. The following set of screen shots (figures 4 to 9) show the results.



```
[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 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. Screenshot of Btlejuice intercepting communication

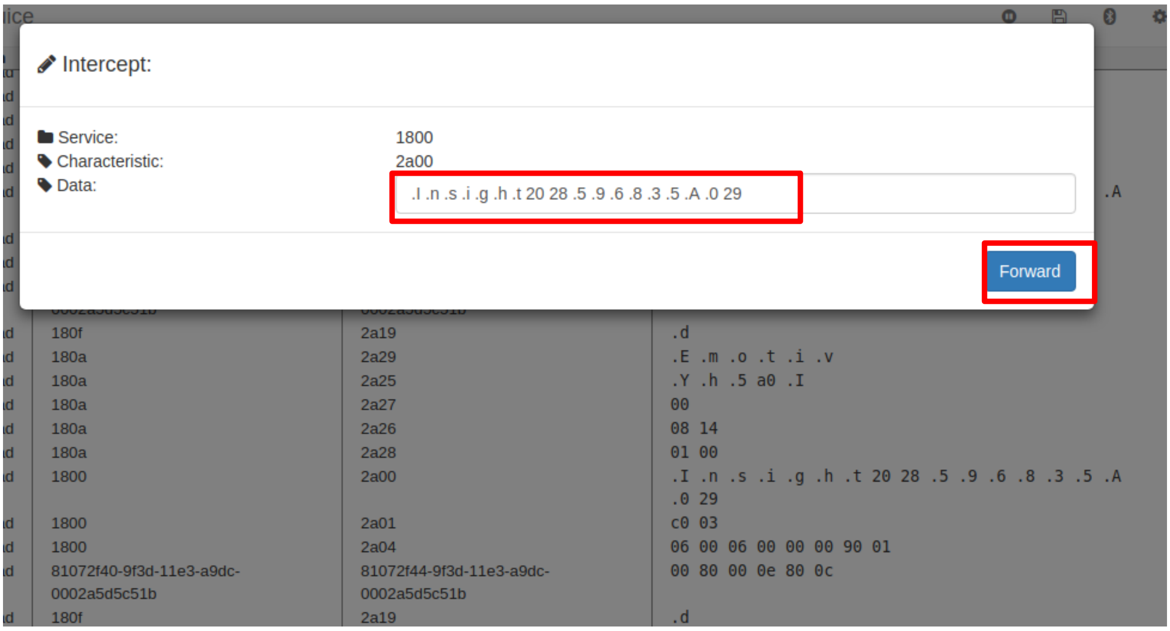


BtleJuice

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 5. Screenshot of the application Mental Commands sending commands to the headset

All the data transmitted by the application on the proxy destined for the Insight headset could be intercepted and also had the option to modify the data. This feature known as ‘on the fly modification’ could be performed. Initially, any command sent by the headset will be sent to the proxy to confirm whether the data should be forwarded to the headset for sending to the device or not. Figure 6 presents a screenshot 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 with a different command to the headset for a different or unintended function to perform.



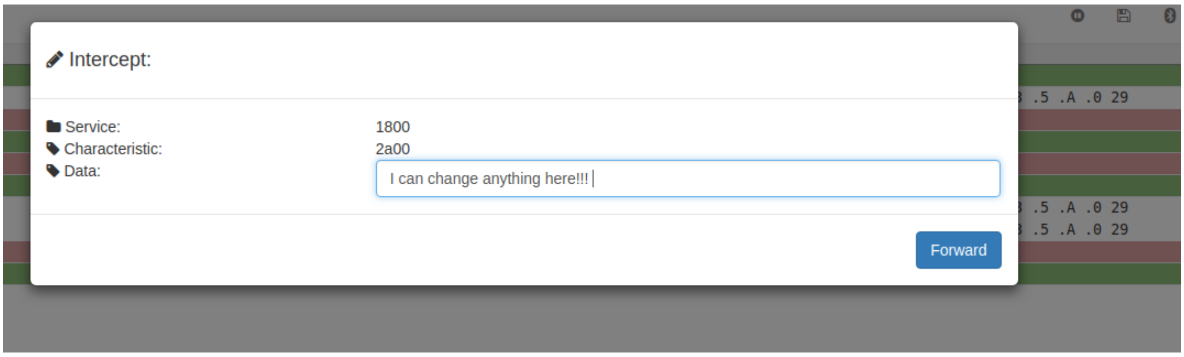
Intercept:

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

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

Figure 6. Screenshot of the active data sent from the proxy application to the headset

Figure 7 shows specific data captured for command 1800, and the way it may be modified to any other command. In this situation 1800 was associated with the device turning left effect. On this screen the turn right command 180f can be inserted to replace 1800, and the device effect subsequently changed. The lexicon of commands can be obtained from the headset or from the support literature.

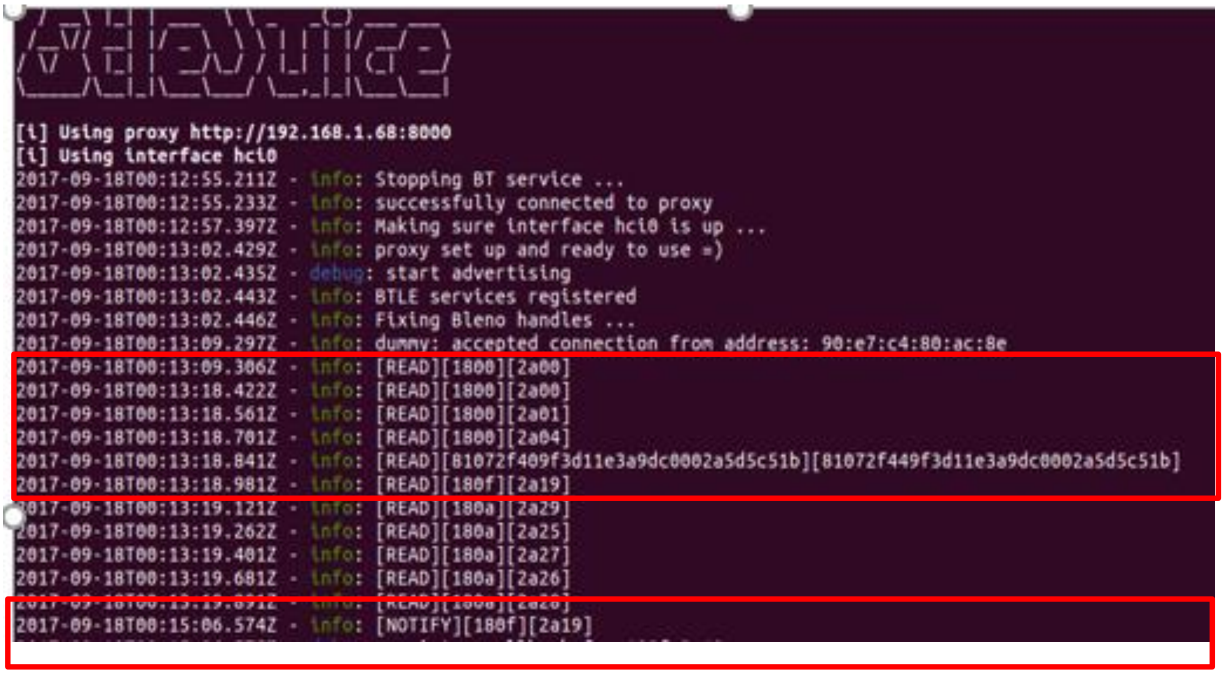


Intercept:

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

Figure 7. Screenshot of the modification of commands

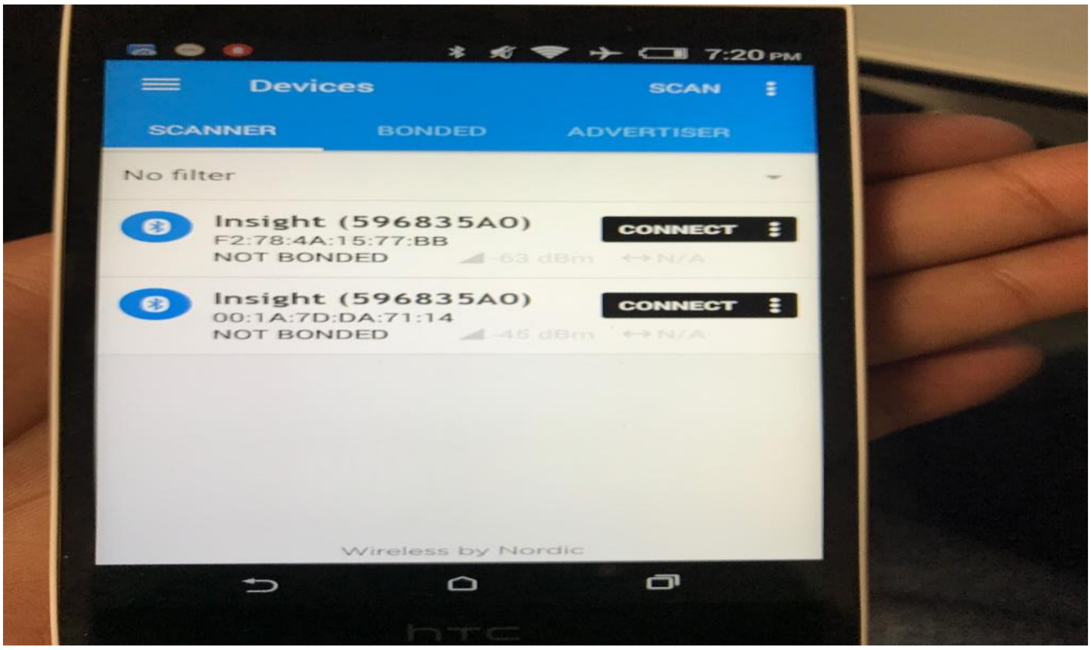
The command change can also be seen in the Btlejuice terminal window in figure 8.



```
[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 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]
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 8. Screenshot of the modified data sent back to the headset

The images report the feasibility of a data modification attack and a replay attack; to violate the integrity of Brianware communication to a device. On further analysis, the nrf Bluetooth application could list both the devices, the real Insight headset with the mac address **f2:78:4a:15:77:bb** along with the fake Insight headset on the proxy with the mac address **00:1a:7d:da:71:14.**



7:20 PM

Devices SCAN

SCANNER BONDED ADVERTISER

No filter

Insight (596835A0)
F2:78:4A:15:77:BB
NOT BONDED -63 dBm N/A
CONNECT

Insight (596835A0)
00:1A:7D:DA:71:14
NOT BONDED -45 dBm N/A
CONNECT

Wireless by Nordic

Figure 9. Screenshot of the nrf Bluetooth application showing the real and the fake control

The headset is connected to the proxy and the fake 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. Figure 9 presents a screenshot of two Insight headsets with different mac address that look identical, including the serial number of the headset.

CONCLUSION

The confidentiality of the headset was easily compromised but the violation of integrity was more difficult. We fundamentally structured a man in the middle attack where fake packets were substituted for the real ones. The attack progressed in two phases. In the first phase, the primary channel of communication sent the packets correctly but then the control was switched to a fake proxy. The proxy took the correct packets and substituted alternative ones back to the headset, and subsequently the communication stream to the device. This meant that the radio controlled car would get one signal that would tell it to turn right and then almost immediately another signal to turn left. The consequence was that the car would buzz but turn neither left nor right and remained frozen in the current state. The second phase of attack was to divert the primary communication channel and to substitute new control commands. This meant that if the primary channel had told the car to turn right then we removed the control packets and substituted a fake command to turn left. These attacks were successful and the remote control car became in control of the secondary information source. The effect demonstrated that it is possible to shift the primary control to a secondary source but there is still more research to design a sandbox that would quickly process the incoming raw signals and to substitute the fake commands. These findings are disturbing and indicate that the accessibility to the communication channel between the headset and the device or game, can also be disrupted. A simple denial of service attack can be hosted by multiple secondary sources substituting packets into the communication stream. These packets could be both meaningless and meaningful in the command and control structures, but either disposition would bring disruption to channel access. The implications are for disruption of human intentions and unintended actions.

The consequences of security failure in brainware devices are yet to be documented in sufficient numbers and scope, that regulatory requirements are implemented for device performance specifications. We also observed that with different brainware headsets that there were no standardised ways of doing a smile for example. This is something that the industry might look at in the future so that when a user is training a headset then a human characteristic is consistent between the different brands and different algorithms. The headsets are also sensitive to underlying emotions and can be used for feedback to the user and not just to an external control situation. For example the five electrode headset also reported to the user other parameters that included the user attention level, the user focus level, the user engagement level, the user interest level, the user relaxation level, and the user stress level. These emotional contexts are part of the feature extraction the brainware computes and provides as output. Our concern here is that not only is there information with an external control capability, but these headsets are also linked into an information feedback loop to the user. If either of these two information streams is compromised, then there are unplanned for consequences arising from the use of the technology.

REFERENCES

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

Bonaci, T., Calo, R., & Chizeck, H. J. (2014). App stores for the brain: Privacy & security in Brain-Computer Interfaces. Paper presented at the International Symposium on Ethics in Science, Technology and Engineering, 2014 IEEE.

Da Silva, F. L. (1996). The generation of electric and magnetic signals of the brain by local networks. 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.

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.

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.

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. Paper presented at the IEEE Conference on Communications and Network Security (CNS).

Martinovic, I., Davies, D., Frank, M., Perito, D., Ros, T., & Song, D. (2012). On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces. Paper presented at 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.

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

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

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.

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.