Hacking NHS Pacemakers: A Feasibility Study

MARCHANG, Jims <http://orcid.org/0000-0002-3700-6671>, BEAVERS, Jake and FAULKS, Mike

Hacking NHS Pacemakers: A Feasibility Study

Jake L Beavers
Department of Computing
Sheffield Hallam University
Sheffield, UK
J.Beavers@shu.ac.uk

Michael Faulks
Department of Computing
Sheffield Hallam University
Sheffield, UK
M.Faulks@shu.ac.uk

Jims Marchang
Department of Computing
Sheffield Hallam University
Sheffield, UK
Jims.Marchang@shu.ac.uk

***Abstract*—Pacemakers are common types of implants, in recent years there have been growing concerns around the security within these devices. This paper was created with the assistance of the NHS staff at NGH, it attempts to answer the question of if it is feasible to hack current models of NHS pacemakers. The experiments performed were done so in the mindset of an average hacker, not a team of experts with access to the required knowledge and equipment.**

Keywords—Medical IoT, Pacemaker, Penetration Testing, NHS, Hacking

I. INTRODUCTION

Implanted Medical devices have been steadily on the rise since the conception of medical technology, however in turn so has the dependency on such devices by patients. Pacemakers [4], insulin pumps and even neural implants are commonplace in everyday life. Many of these devices, and other types of medical equipment, have been proven time and again to have had flaws in their security. With little sign of meaningful changes to correct this concerning issue, it has become a hot topic in the news and in media.

In recent years there has been an increasing amount of attention towards medical device hacking [11], though no meaningful changes have been made to existing laws and legislation. The issue is a disconnect between the medical manufacturing industry and the field of Cyber Security, at first glance you could almost assume that these devices are being developed with only basic security principles in mind.

Cyber Security vulnerabilities have the potential to exist in any computer, it is easily forgotten that everything ranging from our smart phones to an MRI scanner are basically computers. If a malicious attack is performed on a server it can bring down a website, on a pacemaker this has the potential to kill. Take into account that the FDA (US Food and Drug Administration) recently recalled half a million pacemakers, due to a security vulnerability within the devices that could have been fatal [5].

Interesting to note is that when a patient dies their device is not checked for any form of tampering, a coroner will check the device for a malfunction but only on the rare occasion that this is requested. Simply put, it could be possible to get away with murder if you attack the targets medical implant. Dick Cheney (former Vice President) had his pacemakers wireless functions disabled by his doctors over fears of hacking [8], clearly proving that medical practitioners know there could be a potential risk of this occurrence.

This research scopes the threat landscape specifically within pacemaker units. It attempts to answer the question of if it is feasible for a person with no prior knowledge of the technology to hack a pacemaker.

A. Background Information

When people discuss medical implants, the first thing that comes to mind are pacemakers. This is mostly likely because they help to regulate the functions of the most vital organ within the human anatomy, coupled with the fact they are so commonly fitted that they are now even used as preventative medicine. There are an estimated 25,000 people every year in the UK that have a pacemaker fitted [1], this does not even include those outside of the UK or those who have other medical implants fitted. This figure is set to rise further with the ease of access to advanced medicine in the UK, as well as the longer lives that humans are experiencing due to the advances in modern medicine.

Various governing bodies have discussed the idea that the internet should be a human right, providing all of humanity with information and tools that can be as helpful as they are dangerous. It has been proven on numerous occasions that a whole range of medical equipment can be hijacked by a third party, ranging from Insulin Pumps [16] to X-Ray systems, CT Scanners and even Blood Refrigeration Units [15]. Yet despite this knowledge, there has been little advancement towards even the regulation of security within such devices, thus attacks that were used in 2008 may still be viable in 2018. There are governing bodies who regulate the manufacturers of medical devices, however, there appears to be an oversight when it comes to the regulations to enforce adequate security.

B. User Concerns

Data protection is a serious concern, everything from financial data to personal information is considered to be private and therefore should be protected.

This growing concern can be attributed to the ease of access to information on the internet, as well as the increase in Internet of Things (IoT) devices; which also incorporates medical devices. Data is becoming more complex to increase functionality and usefulness, this increase in data flooding the airwaves has led to the ease of access a third party has to private information. In previous penetration tests on pacemakers it has been proven that data can be leaked, code can be injected or even replayed back to the device, potentially causing a fatal cardiac arrest.

Only last year NHS systems were breached [10]. The attack was ransomware aimed at extorting money from the organisation, the question posed here however is how secure would patient data have been if the attack was directly aimed at stealing data?

C. Summary

Connecting devices to the internet has changed the way medicine works, now a patient can be monitored from home leading us into the realms of pre-emptive medicine. However like any other wireless capable device, if it can be accessed remotely then there will always be an unauthorised third party who will try it.

It is far too easy to give a device wireless capabilities, this used to be a key selling point for devices however it is now so commonplace that it could be mistaken for a mandatory requirement. The benefits of wireless connectivity should be weighed against the risks, specifically the reasons why this device is wireless and if it actually makes good use of the added function. In an operating theatre, wireless equipment can prevent the potential for accidental trips or falls during surgery. However, if it can be proven that the equipment within can be hijacked remotely, then adequate security should be implanted or alternative technology should be looked at.

A lack of security standards affects not only the end users but the companies as well. If a device can be hijacked and the data stolen, or the functions affected, then it can cause irreparable damage. The General Data Protection Regulation (GDPR) is now in effect and can fine companies who have their security breached, this may finally force companies who have previously been slack in their response to finally realise the importance of cybersecurity [3].

II. Considerations

To ensure that the findings would be delivered to the right parties, this work has been a collaborative effort between the researcher and the NHS trust.

A. Legal Considerations

The UK Data Protection Act and both the UK and American Human Rights Acts guarantee the right to privacy, specifically article 17 of the EU Data Protection Directive states that the companies must protect personal data against any unlawful or accidental loss, alteration or destruction and in particular during data transmission over a network [2]. In security terms, the confidentiality, integrity and availability of the data must be maintained.

For data protection purposes, the frequency of the device being tested in the figures provided in this paper has not stated in this work. This is because it was unknown at the time if this can lead back to a specific manufacturer, and since all manufacturers donated devices anonymously this cannot be disclosed.

B. Ethical Considerations

Research that could directly or indirectly cause harm should be classified in proportion to the potential damage, with respect to this paper the work performed only details attack methodology and what could feasibly be found by the general public. Furthermore this paper will not include any specifics that could cause harm, as that is not the intent of this research and has no impact on the direct findings. The instructions for the attacks performed have been excluded from this paper, only general details from the research has been disclosed.

III. Attack Vectors

When performing penetration tests on systems and networks it is important to scope out the incorporated technologies; this includes the hardware used, the software installed, any services that are running and how the data is transmitted.

All medical implants are required to operate on the MICS band [7], therefore it can be determined that the devices used in this experiment are guaranteed to operate on the 402MHz to 405MHz frequency range. There have been many successful hacking attempts on pacemakers by hijacking the RF module, thus the RF modules within the devices were deemed the most feasible attack vector for this research. Feasibly it is the most likely attack vector for an attacker as it is easily obtainable and cheap to purchase, the antenna used in this experiment cost ten GBP.

This section discusses the type of attacks that can be performed on medical implants, this section is a prerequisite to the experimentation.

A. Denial of Service (DoS)

DoS is a type of cyber-attack, the intended aim of which is to take the targeted source offline [17]. The methodology behind this attack is to overload the target by overpowering its resources, this is achieved by sending a multitude of spam data signals at the same time. This attack cannot work if the intended target has enough resources available to cope with the extra workload, in these instances more devices are required to perform the attack and succeed. DoS attacks can be combined with a code injection attack, the idea behind this is to execute spam code whilst flooding the connection to intensify the effect.

The primary defence methods for this type of attack are as follows:

- Disabling the wireless functions of the target to stop all communications
- Increase the resources available to the target so it can cope with the extra load
- Limit communication to only specific pre-authorised devices

In RF terms, the equivalent of a DoS attack is signal jamming. This is achieved by broadcasting on the same frequency but at a higher power than the target, effectively this is spamming the airwaves in the same way that a DoS attack spams wireless communications. This results is the device being unable to cope with the high levels of interference and in theory, may cause erratic behaviour in the

unit such as performing at a slower rate or even powering off entirely [18].

There are few ways to protect an RF device against signal jamming, the most efficient way is to attempt to mask the transmission so the attacker does not know which frequency to jam. Code Division Multiplexing (CDM) is an alternative method of combating signal jamming in UHF systems [19]. CDM works by spreading the spectrum of the signal into multiple channels, then each channel is encoded with its own unique code. Only the receiver of the signal knows the code generated, though the spreading effect does reduce the overall power of each channel.

In theory, a pacemaker or ICD should only be accessible by the corresponding manufactures programmer, however, as can be seen in the previous examples of attacks it has been possible to bypass the need for these devices. Fundamentally this is an unavoidable failing with all communication technologies. If you are going to allow wireless connectivity then you must account for unauthorised access attempts, so plan accordingly.

B. Replay Attacks

Home monitoring units send data to and from pacemakers and ICDs when the user is in the vicinity. This data can be captured mid-traffic by utilising the listening functions of a radio antenna, and then it can be replayed back to the device. Since the data or commands it is being sent came from the device originally it may be able to read them, whether the unit accepts this signal is down to the security employed by the receiver.

Since medical implants are commonplace in the UK it is expected that the MICS range could be flooded with signals. These signals clearly do not affect each other however as otherwise they would be subjected to constant replay attacks. Therefore, it can be surmised that some form of unique identifier must be used. If this is the case, then to successfully perform this attack a signal from the same device must be played back to it. If this is not the case then, theoretically any signal from a device of the same type and manufacturer could be used to attack any other.

C. Code Injection

Code injection is a generic term that refers to the unauthorised uploading of potentially malicious code [20]. The programming language used can alter however the fundamental techniques remain the same. When malicious code is packaged it is referred to as malware, this is a catch-all term given to computer viruses.

There are various cyber-security platforms and automated software that is specially designed to remove malware, however, if this code is not detected by such tools then it is left to the user to go through the system until it is found. Anti-virus providers and cyber-security agencies typically have in-house experts who specialise in searching for malicious code, once found their clients are notified and a patch to resolve the issue is pushed out. There are many skilled individuals who design malware to perform all sorts of functions such as stealing information, hijacking a device, blackmail purposes or just because they enjoy doing it. Due to the increase in IoT devices and expertise in computer skills, the amount of malware in circulation will exponentially increase.

Pacemakers and ICDs are re-programmable, they have to be to ensure that any issues with the software can be patched. This opens up a possible avenue for attack, if code is accepted from any source then malicious malware could be uploaded to the device instead. Code does not need to be long and complex, if simple commands are accepted then it would be possible to upload a command to download the data, wipe the device entirely or even switch the device off.

IV. EXPERIMENTATION

The materials used in the tests were ex vivo devices and sourced from deceased patients, all devices were decontaminated and wiped of confidential data before being transferred. Full approval was sourced from the companies that held the patent to the corresponding device(s) prior to testing. Four different ex vivo devices were sourced and used in the research and all four devices have been anonymised of their manufactures by being sealed into plastic biohazard tubs, labelled as devices one to four. All necessary precautions and actions have been taken in accordance with the agreement between all parties involved.

The MICS band frequency is typically flooded with signals, especially when in a busy location such as a University. Therefore to ensure the safety of those within the vicinity, suitable RF shielding was chosen and tested for signal leakage prior to performing the experiment. The most suitable commercially available product was the Titan RF shielding, which was then used to line a cardboard box. The antenna used in the testing was placed in the box alongside a testing device, the only signal that could be seen was from the testing device.

A. Equiptment and Setup

When implanted, a pacemaker or ICD unit sits under the collarbone, there is a short distance between an implant and the outside air. This may not sound like much however this can be enough to reduce signal strength, or shield it entirely. Therefore, manufacturers must take free space path loss into account when designing their devices. It was important to take this into consideration for the research. The units used were sealed in a thick plastic container with a three inch air gap, this may not quite simulate the same level of interference as dense bone and flesh but it will cause some level of interference.

The software used in this research is all open source, this means it is free to obtain and has a large online user basis that can assist you. Each piece of software was chosen for a specific function, also they are all commonly used in RF hijacking.

Hardware:

- Linux operating system installed on a standard desktop computer

- Software Defined Radio (SDR) antennae and USB dongle
- Four anonymised Pacemaker/ICD implants in sealed biohazard tubs
- “Yard Stick One”: Wireless transceiver

Software:

- GQRX: open source SDR receiver
- Audacity: open source, cross-platform audio editor and analyser
- RFCAT: RF transceiver software, capable of spectrum analysis

B. Analysing the Signal

GQRX was loaded and the SDR antenna was selected as the method of transmission. In fig. 1 GQRX is used to view the MICS range, this is 402MHz to 405MHz, as all medical implants run on this range.

The MICS band range is heavily populated, the research was performed in a densely populated urban area thus this makes sense. The devices in the range had a nice even spacing, this most likely was intentional as to prevent any signal issues caused by an overlap.

Note that during the experiment the signal was recorded, this was to be loaded into audacity to both analyse the signals further and to be used in the replay attack.

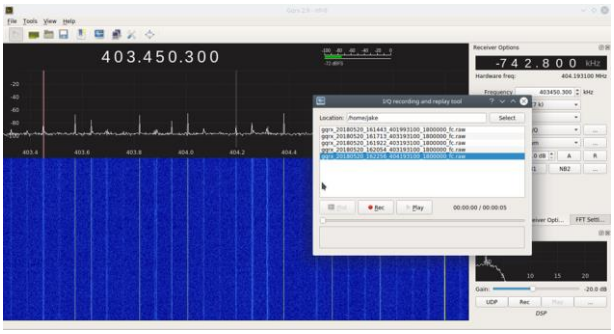

Fig. 1. *SDR antenna recording a signal through GQRX*

As can be seen in fig. 1 the wavelength was quite uniform, this is because this signal that was captured was the carrier signal. The units also appear to have multiple sidebands, though some of these may be false signals caused by interference from a cheap antenna, either way this leads to the conclusion that the devices employ Phase Shift Keying (PSK). This is further backed up as clear phase reversal patterns can be seen in fig. 3, the phase of the wave is shifting from the carrier to reflect binary values [21].

The carrier signal is used as a timing mechanism for the keying, when data is sent the waveform changes. The signal modulates to send data, the modulation can send multiple values, more than just a single 0 or 1. To simplify, there are many forms of PSK, these can even be combined with amplitude modulation to create new forms. These forms will not be discussed in this paper, as they are not conducive to the end results nor required for understanding the figures shown.

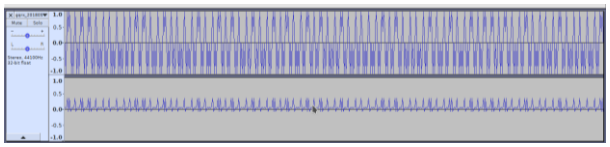

Fig. 2. *Wavelength of a captured signal (programmer)*

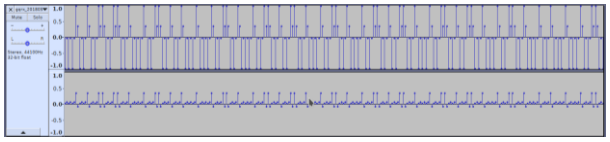

Fig. 3. *Wavelength with modulation mapped*

It could be possible to decode the signal by working out the value of the sifting phase, however, this proved to be difficult and the attempt was abandoned in favour of a conventional security analysis. This could lead to the conclusion that it is not feasible for an amateur to decode the signal.

Based on the reconnaissance results it can surmised that a hacker would need access to a hospital, or at least a home monitoring unit, to capture meaningful data to be used when hacking a pacemaker or ICD.

C. Radio Frequency Attacks

Once reconnaissance on the devices was performed, the threat landscape was mapped and attacks performed in the shielded testing environment.

1) Signal Jamming

Signal jamming was performed by setting the Yard Stick One to the same frequency as the device being tested, then the power of the signal was set to the maximum that the antenna could provide.

Devices 1 to 4 all succumbed to signal jamming, this came as expected. Though it is worth noting that no signs of erratic behaviour were present, only the communication module was affected. That is to say that communication to and from the device was blocked, the carrier signal remains visible however becomes distorted and unusable. If this was performed during an update of a device it may corrupt the data entirely, possibly affecting the defibrillation function, though this is a very specific scenario and would be detectable.

The most likely reason for this attack not affecting the device would be due to Bandpass filtering, which is employed in modern implants and so would have protected against a lower power signal jamming attempt; a higher power attack however is harder to defend against though would not be feasible to perform without more expensive equipment.

2) Code Injection

In a previous attack in 2008 it was possible to replace the patient’s name in the device, if this is possible then it is also

possible to upload any code to a device. The Yard Stick One was set to attempt to upload the word "Hello" to see if the test devices would accept code. Once uploaded the Yard Stick One awaiting a returning signal, similar in concept to the TCP handshake, a response was received though the results implied that all four devices had not accepted the code.

From this it can be determined that the devices use a form of checksum, most likely it employs Cyclic Redundancy Check (CRC) as it is a commonly used in the transmission of data packets [6]. To decode this, someone would need to look through possibly thousands of packets as to work out the pattern in the CRC. The checksum would prevent code from being injected, as the malicious packets would not be sequential to those in the pacemaker, thus the device would ignore the incoming data.

Depending on the encryption methods used it may be possible to reverse engineer these packets, if this is done then data can be uploaded and the security in place bypassed. It is unlikely that this could be done using commercially available equipment, or at least not without expert knowledge on the matter.

3) Replay Attack

A data packet from a pacemaker could potentially be accepted by another, as the packet would be formatted for use with the internal equipment and method of data transfer. If a signal that induces defibrillation could be captured then it could be replayed back to any implant.

This test was performed by using GQRX to capture a signal, and then using the Yard Stick One it was possible to replay this signal directly at a device. Devices 1 to 4 all rejected the replayed signal, the reason is most likely the combination of why the devices rejected the code injection and why there was no erratic behaviour during the signal jamming.

The rejection of the code was expected, though not for the same reasons as the other attacks. The code used was quite basic, furthermore it took longer than it would have done with an actual implanted device to collect data relevant enough for this attack to be performed.

Simply put, it is easier to perform this attack in the real world. For this attack to be reattempted a live setup must be used, to do this patient consent must be signed which can take time. This attack vector could be revisited in future research at a higher level.

D. Summary

Radio Frequency has been previously stated as being easily breakable, however, the results from this line of testing could argue that they are shielded enough to alleviate users concerns. It could be a legal consideration as to why documentation states potential risks of EMI interference, that device manufacturers who implement RF technology must inform the user of potential risk.

The devices used in the tests were provided by the NHS, they are standard modern units and as such it is expected that they should have a reasonable defence against hacking. To answer the question posed in this paper, it may be feasible for someone to scope out the landscape and attempt the attacks. However for the attacks to work, the individual must have expertise and knowledge of both RF and the inner workings of the devices. Attempts using more high-tech equipment could potentially reveal weakness, though that is something to return to in future research.

To answer all the questions posed in this paper it would require access to a working setup, this setup would require a live pacemaker or ICD connected to a home monitoring unit.

V. Side Experiments

This section briefly explains other tests that were performed, which use alternative methods and equipment from the main body of the work. When discovering vulnerabilities it is important to test multiple methods, these tests were performed to see if these were other areas worth exploring

A. RFID Scanner

An attempt was made to scan the devices using a standard RFID scanner used in cloning cards, a report in 2010 [9] stated some RFID scanners can interfere in pacemakers, therefore this test was to see if implants could be vulnerable in 2018. In theory if this was possible then the code could be uploaded to the device and some operational functions could be accessible, the device could be turned off for example.

It is fortunate that this is not the case as this method is very simple to attempt. It is worth noting however that there are many other more powerful RFID readers out there which may, with the right programming, possibly be able to do this.

B. Oscilloscope

A setup involving an oscilloscope was attempted. This was an attempt to mimic a setup used in a 2008 test performed on magnetic induction based devices [14]. Due to the primary aim of this work it was deemed unnecessary to further this specific method of testing.

This was mostly due to that an oscilloscope setup requires the implant to be directly connected to the unit. The devices used in this test were sealed in a container for anonymity, so this test was not possible on any of the devices (aside from a standalone test implant that was obtained and excluded from the primary experimentation).

Feasibly the RF antenna used in this research would be the most likely tool used to exploit these devices as it is cheaper, easier to obtain and gave the same results as the oscilloscope. There is also far more information on hacking RF technology than there is in decoding signals using an oscilloscope, overall the RF antenna provides a more accurate answer to the question posed.

VI. Conclusion

The results from the experimentation were promising, the fact they were not vulnerable to basic attacks shows a commitment to security from the manufacturer's involved.

Do not let this make you complaisant and ignore the broader issues however, the legal aspects and manufacturing regulations are still lacking across the industry. Furthermore these experiments were performed on current NHS models that have been put through rigorous testing, devices from other companies or countries may not be as secure as those involved in this test.

Consider that in some cases patients have pacemakers or ICDs fitted pre-emptively, even if they are not active at the time if the device is vulnerable it could still trigger fibrillation. It is not only those who rely on the units that are at risk, those who have them fitted and do not rely on them have equal risk.

Also consider that there is still potential to cause a fatal heart attack in some devices almost 10 years after the flaws were reported [13], this can only lead to the conclusion that meaningful research and the development of new security methods is vital. In an ideal scenario independent security officers should have the ability to test the devices for such flaws as is the case in some other industries, new laws are clearly required to prevent this in the future. The industry is catching up to the necessary standards however progress has been far too slow.

Barnaby Jack [12], the most renowned medical hacker, was quoted stating that hacking into a pacemaker was easy. It is important to remember however that quote was from an expert in the field, there is reasonable difficulty in performing this feat without access to high-grade equipment and expertise.

Home monitoring units should be considered as vital pieces of equipment. The idea that a patient could have their condition monitored constantly is life-changing, potentially reducing the drain on healthcare resources and improving the general health of patients across the globe. The units also contain private and personal information, on both the patient and their implanted device, these devices have been proven to be vulnerable to man-in-the-middle exploits yet this is overshadowed in the media.

Pacemakers and ICDs clearly have the potential to be vulnerable in the same way as any other device, the issue here is the same one that is affecting the security of all IoT devices. The problem is that people only think of desktops, laptops and some mobile devices when they think of computers. In the age of IoT, every device can have a computer embedded within it. Therefore all devices comes with the same risks of potential vulnerabilities in the software, hardware or general function that could be exploited.

Bluetooth is due to become the next standard of wireless communication modules for medical implants, if the lapse in cybersecurity knowledge in the medical industry carries over then users may be just as vulnerable, if not more. Bluetooth technology is commonplace and has had some serious vulnerability over the years, there are even tutorials online that demonstrate how to exploit these issues.

RF has many faults as well, though if Bluetooth turns out to be more vulnerable then RF may be more viable, at least for the time being. Protective methods such as BPF may exist in RF however that does not mean it is enforced. If BPF is standard practice then the possible effects of EMI on implants may be exaggerated, though if this is not the case then EMI may be more harmful than users realise.

Old laws and legislations are commonly applied to new technologies and practices, it does not mean that they work however. This is commonly the case for copyright law, the law does not adequately cater for the IoT age yet it shows little sign of being revised. The CVD for example has been standardised yet it is not an enforced standard practice, yet some companies have adopted the principle of it. This clearly shows that the market is ready to accept such ideas, as they can benefit everyone involved.

The issue here could be resolved by a threat to enforce these legislations with a set deadline, the industry would then have to sit up and take notice or face the possibility of legal reprisal if they fail to comply. GDPR may be the turning point that enforces security across all industries, the only problem here would be if the companies then only implement the bare minimum security required, treating this recent law an annoyance rather than enforcement.

Fundamentally, the main issue cyber security faces across all industries is that it has no financial return. It can be argued that by increasing security, you are reducing the risk of financial loss from lawsuits. However, the bottom line is that no money is directly made from it, but rather money is spent to prevent a greater loss. This kind of thinking is implemented by companies to make a profit, which is understandable as people are not paid to think outside of their own area. They should instead see such a cost as an insurance policy, a way of minimising damage with a financial safety net. Therefore in the same way that one would take an insurance policy out before they can drive a vehicle, these manufacturers should have to ensure a minimum level of security within their own devices before they can be used.

This work attempted to answer if someone with no prior knowledge of the technology could attack it, just because it appears that the devices are safe against amateurs does not mean they are safe against expert hackers. The security of medical devices must be investigated now in its infancy, before this becomes the next form of cyber terrorism. With the increase in availability of information, and the rise in the numbers of malicious hackers, the security of medical devices as a whole should be paramount.

ACKNOWLEDGMENT

I would like to give special thanks to the staff of Sheffield NGH who were involved in this project. In particular, Dr Paul Morris, who organised obtaining the ex vivo implants.

I would also like to acknowledge my mentor, Michael Faulks, for his guidance and assistance during my research and masters dissertation.

REFERENCES

[1] Focus on: Pacemakers. (n.d.). Retrieved from https://www.bhf.org.uk/heart-matters-magazine/medical/pacemakers

[2] EU Directive 95/46/EC - The Data Protection Directive. (n.d.). Retrieved from https://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-2/93.html

[3] Burgess, M. (2018). What is GDPR? The summary guide to GDPR compliance in the UK. Retrieved from http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

[4] Pacemakers. (n.d.). Retrieved from https://www.bhf.org.uk/heart-health/treatments/pacemakers

[5] Seals, T. (2018). Abbott Addresses Life-Threatening Flaw in a Half-Million Pacemakers. Retrieved May 19, 2018, from https://threatpost.com/abbott-addresses-life-threatening-flaw-in-a-half-million-pacemakers/131709/

[6] Cyclic Redundancy Check (CRC). (n.d.). Retrieved from https://www.techopedia.com/definition/1793/cyclic-redundancy-check-crc

[7] Yuce, M. R., & Islam, M. N. (2016). Review of Medical Implant Communication System (MICS) band and network. ICT Express,2(4), 188-194. doi:10.1016/j.icte.2016.08.010

[8] BBC. (2013) Dick Cheney: Heart implant attack was credible. Retrieved from http://www.bbc.co.uk/news/technology-24608435

[9] O'Connor, M. C. (2010). Study Finds RFID Readers May Affect Pacemakers, But Pose No Urgent Risk. Retrieved from http://www.rfidjournal.com/articles/view?7307

[10] Lam, B. (2017). NHS cyber attack: Views from the front line. Pharmaceutical Journal. Retrieved from https://www.pharmcaceutical-journal.com/opinion/qa/nhs-cyber-attack-views-from-the-front-line/20202794.article

[11] New York Post. (2016). Yes, pacemakers can get hacked. Retrieved from http://nypost.com/2016/12/29/yes-pacemakers-can-get-hacked

[12] Barnaby Jack. (2017). Retrieved from https://en.wikipedia.org/wiki/Barnaby_Jack

[13] Fatal flaws in ten pacemakers make for Denial of Life attacks. (2016). Retrieved from https://www.theregister.co.uk/2016/12/01/denial_of_life_attacks_on_pacemakers/

[14] Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T., Maisel, W. H. (2008). Pacemakers and Implantable Cardiac Defibrillators:Software Radio Attacks and Zero-Power Defenses. IEEE Symposium on Security and Privacy.

[15] Zetter, K. (2015). Medical Devices that are Vulnerable to Life-Threatening Hacks. Retrieved from https://www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks/

[16] Finkle, J. (2016). J&J warns diabetic patients: Insulin pump vulnerable to hacking. Reuters. Retrieved from https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e/jj-warns-diabetic-patients-insulin-pump-vulnerable-to-hacking-idUSKCN12411L

[17] Denial of Service. (2015). Retrieved from https://www.owasp.org/index.php/Denial_of_Service

[18] Jamming & Radio Interference: Understanding the impact. (n.d.). The Institute of Engineering and Technology. doi:10.1049/etr.2012.9002

[19] Thakur, D. (n.d.). Code Division Multiplexing. Retrieved from http://ecomputernotes.com/computernetworkingnotes/multiple-access/code-division-multiplexing

[20] Code Injection. (2013). Retrieved from https://www.owasp.org/index.php/Code_Injection

[21] Poole, I. (n.d.). What is PSK, Phase Shift Keying. Retrieved from http://www.radio-electronics.com/info/rf-technology-design/pm-phase-modulation/what-is-psk-phase-shift-keying-tutorial.php