Ensuring Security of Human-Computer Integrated Devices in Insecure Environments

Author: Euan Brook

Abstract

This Paper will be focusing on the use of human-computer integrated devices within insecure environments, the paper will also look at how current and past attacks and methods could potentially damage these devices and how this affects acceptability. The investigation should provide an ample solution to prevent or slow down these types of attacks which will increase device safety within these insecure environments as well as the overall acceptability of them. The paper will investigate the acceptability and understanding of three types of human-computer integrated devices, Neural Implants, Pacemakers and RFID chips as well as the device safety and concerns. The population of this survey is made up from two groups within Staffordshire university. Convenience sampling has been used due to time constraints and the questionnaire only being placed in their subsequent group chats. There will be a visible divide between those who feel the devices are safe and those who do not. This information will show that the safety of this tech should be improved to provide a higher acceptability rating. The survey uses the acceptability of each device as its primary independent variable as thoses who undergo the survey will state their acceptability and concerns relating to each or all of these devices. The results from the survey show that the acceptability of these devices are high as 94.6% would use at least one. The data also states that 45.2% had knowledge of these devices and 32.3% stated the device not being secure alluding to the fact that there may not be enough security for these devices. The paper suggests that intrusion detection systems and data encryption should be used to provide a secure device and assist in preventing attacks repeatedly occurring. This is due to the lack of any cryptographic auditing with previous solutions.

Keywords: Medical Implanted Device, PaceMaker, RFID Implant, Neural Implant, Human Computer Integration

Introduction

This ability for computers and humans to symbiotically exist together has taken 10x longer than it was predicted to take by a paper reviewed within (Farooq and Grudin, 2016). This same paper also suggests that this prediction was made in 1960 before the digital revolution started and suggested that it would take 3x as long to use the technology than it took to make it. This prediction suggested that it could take up to 150 years to get human computer integration development working fully. This of course would give plenty of time to develop the integrity of these devices but this is where the problem lies, Pacemakers, Radio Frequency Identification implants and Neural Implants are already being used in insecure environments which doesn't leave 150 years to develop security for these devices. Alongside this (Neuralink 2020) a company designing a Brain-machine interface which will be implanted into the brain is rapidly being developed which will boost the usage and increase the amount of people using Human-Computer Integration in insecure environments.

This new advancement poses security concerns as accessibility of a device can hinder its security and integrity and using devices that are connected to vital organs being the brain, heart, and nervous system can lead to horrible outcomes. (Pycroft, et al, 2016) suggest that If unwanted access is gained it could lead to potential bodily harm and other malicious activities. The issue of these devices being susceptible isn't only related to the Neural implant and pacemaker it is also important for Radio Frequency Identification implants as well as they can store extremely confidential data like medical records or access codes for secure buildings. Pacemakers are extremely vulnerable as some models are susceptible to radio-based cyberattacks. This type of attack is suggested by (Tabasum, et al, 2018) to provide the attacking party with patient data and can send malicious commands back to the pacemaker jeopardising the device's integrity and the safety of its user. The threat of these devices being manipulated to cause harm to their users and even death has been a serious concern in the past as a vice president from the united states personally had his device disabled during his time in office from 2001 - 2009 to prevent a possible attack occurring (Pycroft, et al, 2016).

The solution is to develop a secure environment which will implement an Intrusion Prevention system working alongside an Intrusion Detection system as well as data encryption and cloud computing services to store vital data. Intrusion detection on neural implants and pacemakers will allow for counter measures to be deployed and to inform the user of the potential threat. RFID data can be secured via encryption and stored on the chip. It could also be implemented with an encrypted user ID and a secure database which is only accessible by verified users. To assist with the research a questionnaire has been developed to gather the knowledge using quota sampling (Brook, 2020). This information will provide a deeper understanding of how the public reacts to these types of devices.

The use of auditing connections made to these devices via intrusion detection have been previously recommended, logging any connection

that is made to the device. However this solution only allows for investigation after an attack instead of preventing one form taking place which is suggested by (Pycroft, and Aziz, 2018).

The aim of the research is to review previous recommendations for securing these Human-Computer integrated devices and Medical implant devices while determining what security enhancements could be implemented to these devices that would improve acceptability and general security when operating these devices in insecure environments.

Literature Review

I. Data Theft

(Kamp, 2012) discusses a largely used service experiencing emails, passwords, bank info and other personal information being released after a malicious attack. One of the most recent data leaks that affected a large number of people, would have been Linked-In having their sha-1 hashed passwords stolen (Kamp, 2012). The age of the paper is justified as the attack on Linked-In occurred on June 5th, 2012 the same year this paper was published about the information. This paper is one of the few published about this specific incident.

This shows that even when a company attempts to have secure systems there will always be vulnerable assets which will be targeted and shows that even commonly used services such as Linked-In are vulnerable. This is worrying but most of this information like passwords and emails can be changed and damage caused by this can be prevented and stopped, but medical devices containing sensitive patient information like heart rithmic data and patients brain waves can cause concern for the rest of their life as this biological data can not be changed.

The data breaches that occurred on apple's ICloud service on August 31, 2014 resemble similar outcomes to that of a breach on an implanted device which stores such sensitive information.(Marwick, 2020) suggests that the data that was stolen in this case was explicit photography as well as other personal photos, the outcome of this incident left people exposed and vulnerable as it isn't as simple as changing a leaked password to resolve this issue.

Both of the previously mentioned data breaches surrounded non medical data from the early 2010's the most recent of the two attacks occurred just over 6 years ago. One of the more recent data breaches which was made public on December 17, 2019 involved customer information including passwords and Health card numbers that were stolen and held ransom against the canadian company LifeLabs. (Webster, 2020) suggests that this breach may be responsible for 15million patients' records being stolen. This paper also highlights that passwords and emails are not the only bits of data that a hacker may target. The attack is less than a year old showing that these breaches are still occurring to companies.

From these three types of data leaks it is clear that personal medical data is not changeable, this shows that data theft is a serious issue that needs to be mitigated against to ensure the devices are secure.

II. Targeted Attack

A targeted attack requires a high level of sophistication within the cyber sector as well as the medical sector this is suggested by (Pycroft

and Aziz, 2018). The information gathered from this research suggests that these types of attacks, even though they may pose a more deadly outcome to the user' are extremely scarce.

The following source implied that these cases were extremely scarce and that none had ever been recorded as happening, (Fu and Blume, 2014) supports the scarcity of these cases by suggesting that there are no cases of malicious attacks due to the lack of security auditing done by medical implant devices.

The sources state that there has never been an attack and that the devices do not have inbuilt security auditing abilities means that these devices are possibly much more insecure and vulnerable than they are made out to be. This level of false security and form of misinformation due to lack of data collection could lead to drastic events later on when human computer integration plays a much larger part within society as a whole.

III. Blind Attack

The risk of a blind attack taking place is far greater than that of a targeted attack. Blind attacks are not able to be carried out to the same extent as a targeted attack limiting the attacker to only certain types of vulnerabilities, in addition to this the ability to carry out a blind attack is excessively larger due to the level of skill required. Looking at figure I it is clear that there are only four major types of attacks that can be carried out

Table 1. Summary of Attack Types

Attack Category	Attack Type	Condition	Potential Harms
Blind	Switching off IPG	Any	Denial of stimulation; rebound effects
	Draining battery		Denial of stimulation; rebound effects; IPG damage
	Overcharge stimulation		Tissue damage
	Data theft		Violation of patient privacy; facilitation of further attacks
Targeted	~10 Hz STN stimulation	PD	Hypokinesia/akinesia
	GPi electrode contact change	PD	
	Increase voltage/decrease frequency ViM stimulation	ET	Exacerbated tremor
	Increased frequency PAG/PVG stimulation	Pain	Increased pain
	Increased frequency VPL/VPM stimulation	Pain	
	STN electrode contact change	PD	Impulse control disorders; alteration of affect
	NAcc electrode contact change	OCD	Alteration of affect
	NAcc stimulation control	OCD, depression	Alteration of reward processing; operant conditioning

ET, essential tremor; GPi, internal globus pallidus; IPG, implantable pulse generator; NAcc, nucleus accumbens; OCD, obsessive-compulsive disorder; PAG/PVG, periaqueductal/periventricular gray matter; PD, Parkinson disease; STN, subthalamic nucleus; ViM, ventral intermediate thalamic nucleus; VPL/VPM, ventroposterior lateral/medial thalamic nucleus.

Figure I - Types of attacks (Pycroft, et al, 2016)

IV. Acceptability

Acceptability plays a key role in knowing if people feel safe using this device or being around them. The acceptability in Human computer integration and Medical Implant Devices can be quite substantial in many different areas.

An area of previous concern was surrounding the Affordable Care Act also known as Obamacare, which was being presented as an alternative for previous health care within the United States government. The act has positives and negatives that can be seen in (Manchikanti, et al, 2017). However one of the biggest downfalls which nearly completely stalled the bill from becoming a legal legislative was the belief that RFID implants would be mandatory. This was an entirely false belief which is proven by reading through (H.R.3590, 2009). This event allowed the world to see how acceptable this human integration was when it came to connecting people to the internet of things via tracking and mass data collection. The website debunking this myth states that it is a simple mis-interpretation of the original draft of the affordable care act (H.R.3200, 2009). However the bill was severely challenged by the public fear that it would allow for mass chipping and data gathering. This shows an extremely negative view towards having these types of devices that could potentially store and send private information to governments as well as

companies in an extremely intrusive method. Although the Health Care Act was made public in 2009, these fears still exist. The Debate continues about governments, companies and malicious groups having access to personal data. There is a lack of research on acceptability of intrusive medical devices. Conversely, recent research shows that there is a high acceptability amongst the public of devices that store personal health information. (Willius, 2019)

Due to the lack of research, An understanding of current acceptability of devices can also be found in the results of research done by a questionnaire which was given to staffordshire University students which can be seen later in this paper.

V. Intrusion Detection & Prevention

Most pacemakers have no ability to log potential attacks (Pycroft and Aziz, 2018). This poses a serious problem as device failure will never be put down to a malicious attack. (Halperin, 2008) also suggests the fact that these devices with logs have no method of cryptographic auditing which provides hackers the ability to spoof the connection Identification.

Implementing an Intrusion detection system within these devices may not directly prevent threats to those with these devices implanted in them but it would provide information into what attack happened and how it was carried out. The use of intrusion detection systems could provide companies with the ability to mitigate against these risks with the rest of their devices.

There is of course a large ethical issue that arises when it comes to the fact that some patients may be at risk of an attack whilst others are not, which could put them in serious risk and could lead to death to then allow for the rest of the users to not have this attack possible on their implanted devices. This is where Intrusion prevention can be used.

(Yaacoyb, 2020) suggests that intrusion prevention systems should be used to delay the possibility of a threat or medical information being stolen. The amount of intrusion prevention systems within these devices are minimal however a firewall can be used as a sufficient intrusion prevention system. (Kintzlinger, et al, 2020) suggests that a curated firewall could be used to prevent malicious programing by setting base variables for the device like the minimum amount of beats per minute.

VI. Encryption

The use of encryption within medical implant devices and human computer integration tends to be the main form of security for these devices as it is capable of providing a reasonably secure environment.(Thamilarasu, 2020) suggests that this method of security comes at a high computational cost and the small devices cause significant challenges when it comes to the implementation of this security system. The paper (Belkouja, 2018) suggests that even with this encryption these devices are still susceptible to man in the middle attacks.

The use of encryption within medical implants is a useful method of security as research done by (Davis, 2019) suggests methods for reducing the power usage of encryption standards. The need for this lower power encryption is due certain human computer integrated devices being fully implanted within the body with no physical connection unlike (neuralink, 2020) which will implement wireless charging for the implanted chip. The need for this optimization of encryption within these types of devices is due to the current lifespan of a pacemaker battery which is suggested to be around 5-15 years by (Davis, 2019).

Methodology

The survey will capture qualitative data to provide a deeper understanding of the respondent's quantitative responses.

The primary data will be obtained using convenience sampling, this method will be used as it assists with the time constraint surrounding the project and does not require everyone within the two groups to fill out the questionnaire. The questions that will be asked and the expected responses can be seen within the data tool located within the appendix. The data will be from two sub groups; L6 Cyber security students and team members from lacrosse that are both from staffordshire university. The use of these two subgroups is to help lessen any possible research bias that could be caused due to only sampling cyber security students.

A questionnaire will be used as a mono-method it provides a suitable method of collecting multiple pieces of information form a large sample audience and helps with developing statistics from the data. The questionnaire will be sent to two active facebook group chats and will be designed using google forms. The use of google forms within research and data collection is suggested to be extremely useful by (Mondal, 2018)(Hsu, 2017).

On Top of this, the information gathered will comply with current GDPR legislation as the information will only be stored anonymously. The data that will be gathered will also apply with the Research Ethics Proportionate Review Form.

Journal Name	Q-Value	Frequency
Interactions	2	1
2018 international conference on computer application (ICCA)	PR	1
World Neurosurgery	2	1
Expert Review of Medical Devices	2	1
acmqueu	2	1
Ethics and information Technology	1	1
Biomedical Instrumentation & Technology	3	1
Open Access	1	1
Pain Physician	1	1
US Government Legislation	PR	2
Patient Prefer Adherence	1	1
IEEE Pervasive Computing	2	1
Future Generation Computer Systems	1	1
IEEE Access	1	2
Journal of Sensor and Actuator Networks	2	1
2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS)	PR	1
International Journal of clinical and experimental Physiology	2	1
Science Scope	PR	1
Proceedings of the 2016 7th International Conference on Education, Management, Computer and Medicine (EMCM 2016)	PR	1

figure II - q-values of reviewed papers

Results

The results from the survey (Brook, 2020) provide information that supports both a change in public acceptability and provides awareness to potential threats as well as previous issues with these devices.

The Overall acceptability ratings from (Brook, 2020) suggest that there is a general change of attitude towards this tech when compared to previously viewed papers. Which can be seen from the data presented in Figure III. Around 94% of participants stated that they would use at least one of these devices.

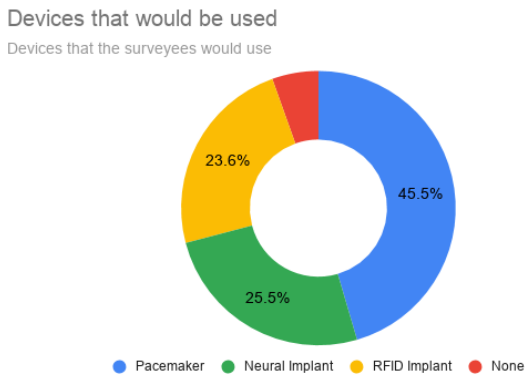

Figure III - Devices that would be used

The data from Figure IV suggests that around 26% of those surveyed have family members with one of these implantable devices.

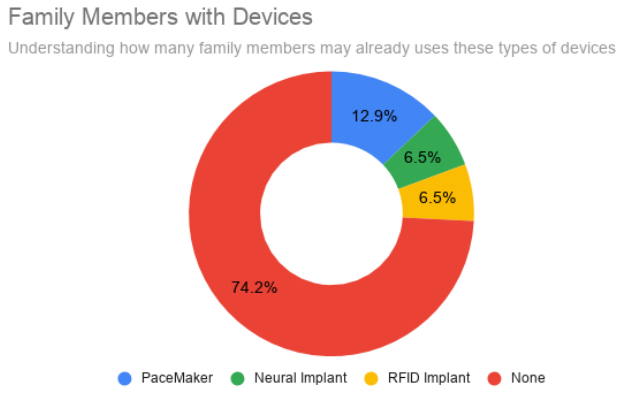

Figure IV - Devices Used By family members

Data from (Brook, 2020) suggests that the sampled population believe that the devices are safe as around 68% stated they believed these devices to be safe which can be seen in figure V, but some have concerns that the implanted devices may be attacked and therefore cause bodily damage as well as provide means for tracking personal information like location.

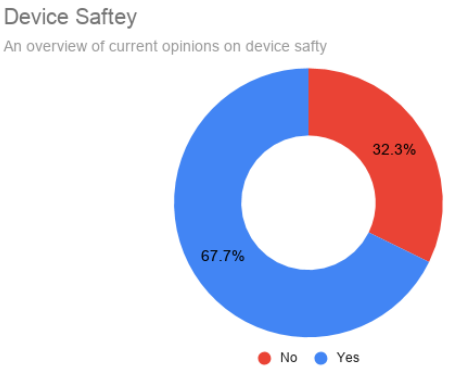

figure V - Overview of Device Safety

Discussion

Reviewing the information that was mentioned previously, it is clear that blind attacks and targeted attacks are serious concerns. As stated previously these implanted devices don't have much or any security to help mitigate against these attacks even though the sampled group believed them to be safe.

Using a simple risk assessment figure VI it can be seen that blind attacks score in the area of 8 and 12 as the difficulty rating is 4 and the consequence is 2-3 whereas a targeted attack only scores 5 due to the level of skill required to carry one out. This means that out of the two security issues there should be a larger focus on mitigating against blind attacks due to their score. This however does not necessarily mean that targeted attacks should not be mitigated against at all.

Risk Assesment		Dificulty				
		1 challengeing	2	3 Complicated	4	5 Simple
Concequence	5 Catastrophic	5	10	15	20	25
	4	4	8	12	16	20
	3 Moderate	3	6	9	12	15
	2	2	2	6	8	10
	1 Negligible	1	2	3	4	5

figure VI - Difficulty x Consequence Risk assessment.

Looking at the information from above there are three main types of solutions available to use. The biggest issue with implementation is the size of the device as well as the device's battery. Implementation of these solutions could potentially require more operations for the patient as the devices will need to be replaced. Even though this would not be classified as a risk related to the device being attacked in an insecure environment it does still pose a threat. One of the best solutions to implement would be data encryption for information stored on the devices as well as the data being transmitted to and from the device.

The solution that would help alert users to attacks as well as assist in development against targeted attacks would be an intrusion detection system. This system has previously been stated to have a low impact on battery life when compared to an intrusion prevention system which would constantly be checking every packet of data that is sent and received by the device instead of just a unique connection address. Perhaps in the near future with enhancements in the cloud computing sector, such intrusion prevention systems could be entirely within this domain. Advanced artificial intelligence for detecting possible threats could be hosted on these servers instead of on the physical device.

Conclusion

Reviewing both primary and secondary data it has been made clear that the knowledge of these devices is still growing as figure VII shows that 45% of people that took part in primary research stated they already knew what Human-computer integration was.

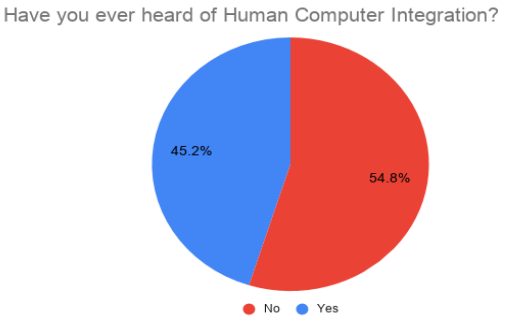

figure VII - Knowledge of Human Computer Integration

This information when combined with the percentage of people who would use these devices and the previously gathered information around acceptability with devices such as RFID chips in american medical politics proves that the devices still need vast improvements to ensure security and privacy from unauthorised users of the devices. To conclude the use of Intrusion Detection systems should be implemented to both ensure device integrity and provide secure logs of previously connected devices. This system can then be used to alert the device that an unauthorised device has connected allowing for device features that could pose harmful outcomes to the user if manipulated to be deactivated temporarily. The use of encryption within the device will assist in improving acceptability to the general public as it has within online transactions and virtual banking (Wang, 2017). Overall this solution will solve the security concerns surrounding these devices and provide security in insecure environments.

7 References

1. Farooq, U and Grudin, J., 2016. Human-Computer integration. Interactions, [online] 23(6), pp.26-32. Available at: <https://dl.acm.org/doi/fullHtml/10.1145/3001896> [Accessed 10 December 2020].
2. Neuralink. 2020. Neuralink. [online] Available at: <https://neuralink.com/> [Accessed 24 November 2020].
3. Tabasum, A., Safi, Z., Alkhater, W. and Shikfa, A., 2018. Cybersecurity Issues in Implanted Medical Devices. 2018 International Conference on Computer and Applications (ICCA), [online] Available at: <https://ieeexplore.ieee.org/abstract/document/8460454> [Accessed 10 December 2020].
4. Pycroft, L., Boccard, S., Owen, S., Stein, J. and Fitzgerald, J., 2016. Brainjacking: Implant Security Issues in Invasive Neuromodulation. World Neurosurgery, [online] 92. Available at: <https://pubmed.ncbi.nlm.nih.gov/27184896/> [Accessed 24 November 2020].
5. Pycroft, L. and Aziz, T., 2018. Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. Expert Review of Medical Devices, [online] 15(6). Available at: <https://www.tandfonline.com/doi/ref/10.1080/17434440.2018.1483235?scroll=top> [Accessed 24 November 2020].
6. Kamp, P., 2012. LinkedIn Password Leak: Salt Their Hide. Aacmqueue, [online] 10(6). Available at: <https://queue.acm.org/detail.cfm?id=2254400&ref=fullrss> [Accessed 24 November 2020].
7. Marwick, A., 2020. Scandal or sex crime? Gendered privacy and the celebrity nude photo leaks. Ethics and Information Technology, [online] 19. Available at: <https://link.springer.com/article/10.1007/s10676-017-9431-7#citeas> [Accessed 24 November 2020].
8. Fu, K. and Blum, J., 2014. Controlling for Cybersecurity Risks of Medical Device Software. Biomedical Instrumentation & Technology, suppl. Horizons, [online] 48, pp.38-41. Available at: <https://pubmed.ncbi.nlm.nih.gov/24848148/> [Accessed 10 December 2020].
9. Webster, P., 2020. Canadian digital health data breaches: time for reform. Open Access, [online] 2(3), pp.e113-e114. Available at: <https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30030-3/fulltext> [Accessed 11 December 2020].
10. Manchikanti MD, L., Helm II MD, S., Benyamin MD, R. and Hirsch MD, J., 2017. A Critical Analysis of Obamacare: Affordable Care or Insurance for Many and Coverage for Few?. Pain Physician, [online] 20(3), pp.111-138. Available at: <https://www.painphysicianjournal.com/current/pdf?article=NDMwMg%3D%3D&journal=104> [Accessed 10 December 2020].
11. H.R.3590, 2009. H.R.3590 - Patient Protection And Affordable Care Act. [online] Available at: <https://www.congress.gov/bill/111th-congress/house-bill/3590/> [Accessed 10 December 2020].
12. H. R. 3200. 2009, [online] Available at: <https://www.govinfo.gov/content/pkg/BILLS-111hr3200ih/pdf/BILLS-111hr3200ih.pdf> [Accessed 10 December 2020].
13. Willius, A., Hidalgo, M., Zuñiga, P., Vengas, M., Díaz, C., Abarca, E., Gutierrez, E. and Bedregal, P., 2019. An Acceptability Study Of A Personal Portable Device Storing Critical Health Information To Ensure Treatment Continuity Of Home-Dwelling Older Adults In Case Of A Disaster. Patient Prefer Adherence, [online] 13, pp.1941-1949. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6850675/> [Accessed 11 December 2020].
14. Halperin, D., Heydt-Benjamin, T., Fu, K., Kohno, T. and Maisel, W., 2008. Security and Privacy for Implantable Medical Devices. PERVASIVE computing, [online] 7(1), pp.30-39. Available at: <https://ieeexplore.ieee.org/document/4431854> [Accessed 10 December 2020].
15. Yaacoyb, J., Noura, M., Noura, H., Salaman, O., Yaacoub, E., Couturier, R. and Chehab, A., 2020. Securing internet of medical things systems: Limitations, issues and recommendations. Future Generation Computer Systems, [online] 105, pp.591-606. Available at: <https://www.sciencedirect.com/science/article/abs/pii/S0167739X19305680> [Accessed 10 December 2020].
16. Kintzlinger, M., Cohen, A., Nissim, N., Rav-Acha, M. and Khalameizer, V., 2020. CardiWall: A Trusted Firewall for the Detection of Malicious Clinical Programming of Cardiac Implantable Electronic Devices. IEEE Access, [online] 8, pp.48123-48140. Available at: <https://ieeexplore.ieee.org/document/9025056> [Accessed 12 December 2020].

17. Thamilarasu, G., Odesile, A. and Hoang, A., 2020. An Intrusion Detection System for Internet of Medical Things. IEEE Access, [online] 9, pp.181560 - 181576. Available at: <2929> [Accessed 10 December 2020].
18. Belkouja, T., Du, X., Mohamed, A. and Al-Ali, A., 2018. Symmetric Encryption Relying on Chaotic Henon System for Secure Hardware-Friendly Wireless Communication of Implantable Medical Systems. Journal of Sensor and Actuator Networks, [online] 7(2). Available at: <https://www.mdpi.com/2224-2708/7/2/21> [Accessed 10 December 2020].
19. Davis, C., Muthineni, A. and John, E., 2019. Low-Power Advanced Encryption Standard for Implantable Cardiac Devices. *2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS)*, [online] pp.41-44. Available at: <https://ieeexplore.ieee.org/abstract/document/8884946> [Accessed 10 December 2020].
20. Mondal, H., Mondal, S., Mondal, S. and Ghosal, T., 2018. Using Google Forms for Medical Survey: A Technical Note. Journal of Clinical and Experimental Physiology, [online] 5(4), pp.216-218. Available at: <https://www.researchgate.net/publication/338260253_Using_Google_Forms_for_Medical_Survey_A_Technical_Note> [Accessed 10 December 2020].
21. Hsu, H. and Wang, S., 2017. Using Google Forms to Collect and Analyze Data. Science Scope, [online] 40(9). Available at: <https://www.questia.com/library/journal/1G1-490937186/using-google-forms-to-collect-and-analyze-data> [Accessed 10 December 2020].
22. Wang, J., 2017. Analysis of Data Encryption Technology and Secure Electronic Transaction. 2016 7th International Conference on Education, Management, Computer and Medicine (EMCM 2016), [online] Available at: <https://www.atlantis-press.com/proceedings/emcm-16/25870615> [Accessed 10 December 2020].
23. Brook, E, 2020. Analysis of general Knowledge, Understanding and acceptability of Human-Computer Integration [online] available at: <https://docs.google.com/spreadsheets/d/1Vi7h_QowJ4XGQoQTci1lhseMa1n4P7bjk-j54HDx9VU/edit?usp=sharing>[Accessed 16 December 2020].

Appendix

I. Data Collection Tool

This data will be collected in the form of a google forms questionnaire and stored with an excel file as well as graphical representation, Google forms allows for the risk of a human data entry error to be avoided as the system automatically stores data in an excel format.

Topic	Aim	How Will I Know	Question Type	Question
Knowledge of Human-Computer Integration	This questionnair will allow for a greater insight of the understandin of Human-Computer intergation capabilites, security aswell as how accepting university students within Staffordshire University are towards the newadvances in this tech	The surveyee will state whether or not they have heard of HCI	Closed	Have you ever heard of Human Computer Integration?
		The surveyee will state whether or not they know if any device is used by them or a family member	Closed	Do you or anyone in your family use any of the following human computer intergrated devices?
		The surveyee will state if they have heard of any security breaks within HCI, and give an example	Closed/Open	Are you aware of any recent Human-Computer integration security breaches?
		The surveyee will state if they think the device are safe	Closed	Do you belive these devices are safe?
		The surveyee will state if they have any worrys aswell as expressing them	Closed/Open	Do you have any worries about this type of tech? If so what are they?
		The surveyee will state which device they would use	Closed	What Device would you be open to using?
		The surveyee will state if they would use a pacemaker the extend their natural life	Closed	Would you use a pacemake to extend your natural life?
		The surveyee will state if they would use a Neural implant to extend their natural life	Closed	Would you use a neural implant to extend your natural life?
		The surveyee will state if they would connect their brain to a machine	Closed	If you had a Pace Maker or Neural Implant would you connected it to a 3rd party device (eg. Mobile phone)
		The surveyee will state if they would connect their RFID implant or pacemaker to a machine	Closed	If you had one of the following would you connect your RFID implant or pacemaker to a machine?
		The surveyee will state how they think an implant could effect their life	Open	What could a Neural implant or RFID implant do for you?

Respones Type	Validation Method	Data Type	Graph Type	Link to Research
Unselected radio button (Yes / No)	grouped radio buttons (one response)	discrete	BarChart	Understanding of Human Computer Integration
Unselected CheckBoxes (PaceMaker, Neural Implant, RFID Implant)	(PaceMaker, Neural Implant, RFID Implant) can all be selected independly or none selected	discrete	BarChart	Capabilities and Understanding of Human Computer Integration
unselected radio button(Yes / No) TextBox	grouped radio buttons (one response) Textbox only allows input if the yes radio button has been selected Max char 280 Text will need to be entered into the text box to validate that they actualy know about a breach	discrete/continuous	BarChart	Knowledge of security issues within the area
unselected radio button(Yes / No)	grouped radio buttons (one response)	discrete	BarChart	
unselected radio button(Yes / No) TextBox	grouped radio buttons (one response) Textbox only allows input if the yes radio button has been selected Max char 280	discrete/continuous	BarChart	
unselected radio button (paceMaker, Neural Implant, RFID Implant, All Devices, None)	grouped radio buttons (one response)	discrete	BarChart	Acceptance of The technology
Unselected radio button (Yes / No)	grouped radio buttons (one response)	discrete	BarChart	
Unselected radio button (Yes / No)	grouped radio buttons (one response)	discrete	BarChart	
Unselected radio button (Yes / No)	grouped radio buttons (one response)	discrete	BarChart	
Unselected radio button (Yes / No)	grouped radio buttons (one response)	discrete	BarChart	
TextBox	Max char 280	continuous	Similar Ideas may be used in a BarChart	Understanding of Human Computer Integration

III. Results from (Brook, 2020)

Timestamp	Have you ever heard of Human Computer Integration?	Do you or anyone in your family use any of the following human Computer integrated devices	Are you aware of any recent Human-Computer integration security breaches?	If you answered Yes above please state the security breach	Do you believe these devices are safe?	Do you have any worries about this type of tech? If so what are they?	What devices would you be open to using?	Would you use a neural implant to extend your life?	If you had a Pace Maker or Neural Implant would you connected it to a 3rd party device (eg. Mobile phone)	What would you like a Neural implant or RFID implant do for you?
11/30/2020 17:07:09	No		No		No	Potential murders from hacking components	PaceMaker	Yes	Yes	Help with a disability, Extend your natural life, Increase accessibility (eg. Understanding Languages, or controlling a robot)
11/30/2020 17:21:02	No		No		Yes	I don't know what this is	Neural Implant	Yes	Yes	Increase accessibility (eg. Understanding Languages, or controlling a robot)
11/30/2020 17:23:50	No		No		No	N/A	PaceMaker	Yes	No	Help with a disability, Extend your natural life, Increase accessibility (eg. Understanding Languages, or controlling a robot)
11/30/2020 17:31:16	No		No		Yes	No, I don't	PaceMaker, Neural Implant, RFID Implant	Yes	Yes	Help with a disability, Increase accessibility (eg. Understanding Languages, or controlling a robot), Open Doors, Other
11/30/2020 17:33:47	No		No		Yes	If they become faulty		Yes	Yes	Help with a disability, Extend your natural life, Open Doors
11/30/2020 17:36:11	No		No		Yes	Problems with the technology such as a pacemaker may not be discovered until they have stopped working	PaceMaker	No	No	Nothing
11/30/2020 17:38:21	No		No		Yes	No	PaceMaker, Neural Implant	Yes	No	Extend your natural life, Increase accessibility (eg. Understanding Languages, or controlling a robot), Open Doors
11/30/2020 17:38:47	No		No		Yes	No	Neural Implant	Yes	Yes	Help with a disability
11/30/2020 17:48:13	Yes		No		Yes	The tech being able to track people	PaceMaker, Neural Implant, RFID Implant	Yes	No	Help with a disability, Extend your natural life, Increase accessibility (eg. Understanding Languages, or controlling a robot), Other
11/30/2020 18:20:01	Yes	PaceMaker, Neural Implant, RFID Implant	No		Yes	No worries so far	PaceMaker, Neural Implant, RFID Implant	Yes	Yes	Help with a disability, Extend your natural life, Increase accessibility (eg. Understanding Languages, or controlling a robot)
11/30/2020 18:26:53	Yes	PaceMaker	No		No	error in the decive when needed	PaceMaker	Yes	Yes	Help with a disability, Extend your natural life
11/30/2020 18:32:30	No		No		No	Don't know enough about them	PaceMaker	No	No	Help with a disability
11/30/2020 20:16:12	Yes	PaceMaker, Neural Implant	No		Yes	No	PaceMaker, Neural Implant, RFID Implant	Yes	Yes	Help with a disability, Extend your natural life, Increase accessibility (eg. Understanding Languages, or controlling a robot), Other
12/2/2020 8:06:15	Yes		No		Yes	no	PaceMaker, Neural Implant, RFID Implant	Yes	Yes	Help with a disability, Extend your natural life, Increase accessibility (eg. Understanding Languages, or controlling a robot)
12/2/2020 8:06:53	No		No		No	Reliability		Yes	Yes	Help with a disability, Increase accessibility (eg. Understanding Languages, or controlling a robot), Other
12/2/2020 8:09:27	Yes		No		Yes	No	PaceMaker, Neural Implant, RFID Implant	Yes	No	Help with a disability, Extend your natural life
12/2/2020 8:52:35	Yes		No		No	yes concerned that some one can control you if you have one	PaceMaker	No	No	Help with a disability
12/2/2020 9:15:38	Yes		No		Yes	The same issues would potentially be present here as with all technology. The understanding that the "bad guys" are always ahead would still be crucial consideration to ensure that these devices wouldn't be tampered with, especially as the functionality extends.	PaceMaker, Neural Implant, RFID Implant	No	Yes	Help with a disability, Increase accessibility (eg. Understanding Languages, or controlling a robot), Open Doors
12/2/2020 13:29:49	Yes		No		Yes	Yes, hacking could be a problem.	PaceMaker	No	Yes	Nothing
12/2/2020 13:42:02	No	PaceMaker	No		Yes	I didn't until now	PaceMaker, Neural Implant, RFID Implant	Yes	No	Help with a disability, Extend your natural life
12/2/2020 13:44:56	No		No		No	Being Hacked or taken control of.	PaceMaker	Yes	No	Extend your natural life
12/2/2020 14:47:27	Yes		No		No	Nothing is safe	PaceMaker	No	No	Nothing
12/4/2020 20:15:13	No		No		Yes	No		No	Yes	Help with a disability
12/7/2020 16:24:16	No		No		Yes	Being used against me. Being controlled or spied on!	PaceMaker	Yes	No	Increase accessibility (eg. Understanding Languages, or controlling a robot)
12/7/2020 16:24:28	No		No	N/A	Yes	I have never considered any security issues before.	PaceMaker	No	No	Help with a disability
12/7/2020 16:24:28	Yes		No		Yes	No, if they benefit Health then I believe and trust them	PaceMaker	No	No	Help with a disability
12/7/2020 17:31:04	Yes		No		Yes	Provided all suppliers meet data protection laws, I have no worries.	PaceMaker, Neural Implant, RFID Implant	Yes	Yes	Help with a disability, Extend your natural life, Increase accessibility (eg. Understanding Languages, or controlling a robot), Open Doors, Other
12/8/2020 12:06:28	No		No		Yes	N/A	PaceMaker, Neural Implant, RFID Implant	Yes	Yes	Help with a disability, Increase accessibility (eg. Understanding Languages, or controlling a robot)
12/8/2020 15:28:56	Yes		No		No	They can be hacked	PaceMaker, RFID Implant	No	Yes	Help with a disability, Open Doors
12/8/2020 17:23:40	Yes	RFID Implant	No		Yes	No	PaceMaker, Neural Implant, RFID Implant	Yes	Yes	Help with a disability, Extend your natural life, Increase accessibility (eg. Understanding Languages, or controlling a robot)
12/8/2020 20:17:45	No		No		No	They can break causing death	RFID Implant	No	No	Nothing

IV. Reflective Statement

Learning Outcome	Your Reflection
1. Use technical and educational resources including presentational software effectively and critically apply different approaches to the collection of data and information, understanding strengths and weakness of different approaches.	1. **Use technical and education resources** The research paper allowed me to carry out a literature review within it, requiring me to analyze multiple academic papers which relates to (Lo1). This skill is extremely useful in any workplace as it shows the ability to read and understand a point which is being made. 2. **Including presentation software effectively** The assessment stated that a powerpoint presentation was required, from my powerpoint i was able to show the ability to transfer the information from a paper to a presentation changing the means as to which the information that was researched was delivered and is also closely related to (Lo2), on top of this the presentation skills provide a strong ability to communicate with those who your are presenting to 3. **Critically apply different approaches to the collection of data information** The use of a questionnaire shows that we are capable of designing data collection tools and provides the ability to enquire within a specific sample group for data and relates to (Lo1), the ability to gather information from a group of people can be extremely useful within the tech industry as it can allow for people to come forward with bugs and exploits for systems and devices. 4. **Understanding strengths and weakness of different approaches** The introduction and abstract of this paper show an understanding of problem solving as a problem was identified and multiple solutions were applied showing that (Lo1) has been achieved. Problem solving is one of the most sought after skills in workplaces. This skill has assisted me in getting multiple types of jobs, and will continue within my future workplace.

2. Communicate technical information presentation and documentation to a professional standard.	1. **Communicate technical information** The paper that has been written is capable of explaining technical knowhow to those that aren't professionals within the industry as I have had multiple people read the paper with non cyber/biomedical backgrounds and understand the points made. 2. **Presentation and documentation to professional standards.** The skill of presenting data in this form is extremely useful in a business as this is a common way of explaining and communicating the information and data to employees, shareholders and customers.
3. Demonstrate a systematic and practical understanding of the methods employed in research and an awareness of ethical and access issues related to research and industrial collaboration both in terms of data collection and utilisation of data.	1. **Demonstrate a systematic and practical understanding of methods employed in research and Awareness of ethical and access issues related to research** Within the beginning of the project there was documentation to ensure that the project would comply with staffordshire universities ethics board, this included an ethics form as well as a data collection tool which showed a knowledge of what questions you could ask and what type of data could be stored and how it could be stored this shows that the first part of (Lo3) is being achieved.The use of this within a work environment is important as every company will have strict regulations which must be followed religiously. 2. **Industrial collaboration both in terms of data collection and utilisation of data** Reading through multiple research papers and discovering their legitimacy via Q-values provides a good amount of learning as to how a research paper is to be written and the process that takes place along the way and shows part 2 of (Lo3) has been met. Understanding if a source is legitimate is important as relaying wrong information within any company can cause serious negative effects. The final part of the module's learning outcome is reflection which is shown by this section of the assignment, it concludes that the learning objectives have been achieved and explains how they were met.