[dstl]

The Science Inside

Defence Science and Technology Laboratory

Futures Student Essay Competition

Top 10

November 2021

Ministry of Defence

Essay Title: The WIMDs of change: present and future security concerns associated with Wearable and Implantable Medical Devices

Author: Richard Brown

Institute: Northumbria University

Abstract

The popularity of Wearable and Implantable Medical Devices (WIMDs) has risen dramatically in recent years and this technology is expected to be integrated into expanding medical networks in the years ahead. Data collection via networks of WIMDs promises to revolutionise healthcare by providing timely and effective diagnosis and delivery of care. The combination of big data practices with this emerging technology may provide vital insights into disease patterns and help to generate innovative health solutions. Despite boasting an array of potential benefits, the increased prevalence of WIMDs poses a threat to patient safety and national security. WIMDs may be hacked by malicious actors to administer fatal individual attacks or to overwhelm and disrupt critical infrastructure. The present and future national security risks associated with the emergence of WIMDs are likely to be underestimated. This is due to the unique vulnerability of this technology combined with the recent tendency to focus on data privacy issues when considering the potential impact of cybersecurity breaches. Greater attention should be given to the direct threat to life that hacks to WIMDs could cause, as well as the possibility for coordinated attempts to disrupt large medical networks. Future research should investigate the psychological and behavioural effects of interfering with WIMDs in order to mitigate the future risks of mass panic and societal disruption.

Introduction

The use of Wearable and Implantable Medical Devices (WIMDs) has exploded over the past decade and is expected to play an integral role in the delivery of healthcare in the forthcoming years. The ability to harness vast amounts of data from these devices could help to generate health solutions for a variety of long-term conditions, as well as to optimise the delivery of care. I will discuss the risks and security concerns associated with the increasing prevalence of WIMDs by considering the threat, vulnerability and potential impact of future attacks on these devices. The UK National Risk Register acknowledges the ability of cyberattacks to cripple essential networks such as the NHS (Cabinet Office, 2020). However, I will argue that the national security risks associated with the emergence of WIMDs are likely to be underestimated. This is due to the unique vulnerability of WIMDs and the tendency to focus on data privacy issues when considering the potential impact of security breaches. I will argue that greater attention should be given to the potential for direct attacks on individual safety, as well as the possibility for coordinated attempts to overwhelm and disrupt medical networks. I will also highlight the importance of considering the psychological and behavioural effects of interfering with WIMDs, and why this may threaten national security.

Wearable and Implantable Medical Devices (WIMDs): emergence, prevalence and future benefits

Wearable and implantable medical devices (WIMDs) represent a growing range of technology used for monitoring health and assisting in diagnosis and treatment. The latest generations of commercially available health trackers and smartwatches can be used to generate an array of health analytics by monitoring heart rate, blood pressure, blood oxygen, glucose levels, and respiratory irregularities (Liao et al., 2019). Implantable devices can also serve an active

function in maintaining health by automatically administering treatment. For example, insulin pumps, pacemakers and implantable cardioverter-defibrillators (ICDs) have long been used to manage long-term health conditions. WIMDs serve an important function as nodes in an expanding medical network by connecting patients and healthcare services through the Internet of Things (Jiang and Shi, 2021). This provides continuous data acquisition and the possibility for real-time information processing to administer timely diagnosis and treatment (Liao et al., 2019).

The increasing ubiquity of technology in recent years has led to a significant rise in the prevalence of WIMDs (Stiglbauer et al., 2019). This is expected to continue as commercial giants such as Apple, Google, Nike and Garmin look to generate innovative WIMDs in response to growing market demand (Casselman et al., 2017). The rise of WIMDs has thus been dubbed the dawn of a medical revolution (Dunn et al., 2018). Large healthcare institutions are predicted to initiate large rollouts of WIMDs in coming years as part of preventative care strategies (Dinh-Le et al., 2019). The use of WIMDs is expected to transform healthcare in the decades to come by enabling remote, continuous and longitudinal monitoring to provide automated health event prediction, prevention and intervention (Dunn et al., 2018). The next generation of WIMDs offer an exciting range of potential features such as the ability to detect cancer-related biomarkers (Yang et al., 2018) and recognise symptoms of infectious diseases such as COVID-19 (Ates et al., 2021).

The benefits to public health of using WIMDs include helping to identify long-term patterns of disease that would ordinarily be blurred by the daily fluctuation of symptoms (Austin et al., 2020). By using big data public health practices, the information collected by WIMDs can be analysed to provide insights into numerous health conditions, as well as to optimise the delivery of individual care (Roski et al., 2014, Hulsen, 2020). The effective use of WIMDs may also help to increase the efficiency of diagnosis and treatment in order to reduce the surging costs of long-term health care in the UK. In England, approximately 20 million people are currently living with a long-term health condition (Roddis et al., 2016). Due to the steady increase in life expectancy in recent decades (Vaupel, 2010), it is projected that the number of people with four or more chronic health conditions in the UK is likely to double by 2035 (Kingston et al., 2018). The annual total expenditure on long-term care in the UK is estimated to be £48.3 billion (Office for National Statistics, 2020). Therefore, the enhanced efficiency of diagnosis and treatment through the increased use of WIMDs in healthcare has the potential to reduce government expenditure and improve the nation's health.

Security concerns associated with WIMDs

In cybersecurity, risk is often calculated by applying the formula 'Risk = Threat x Vulnerability x Impact' (Jacobsson et al., 2016, Casselman et al., 2017).

Threat

The threat to health data from cyberattack is widely discussed (Luna et al., 2016, Kruse et al., 2017). In the US, the black market value of stolen health credentials is believed to be more than 10 times the price of a stolen credit card number (Humer and Finkle, 2014). This is likely to incentivise hackers to develop new strategies to infiltrate health networks. Additionally, a new class of threat has surfaced in cybersecurity known as Advanced Persistent Threats (APTs)(Deal, 2021). APTs constitute an active and sophisticated threat to governments and large institutions and are believed to be orchestrated by complex hacker groups and rogue nations (Chen et al., 2014). For example, the extensive disruption to the NHS from the 2017 WannaCry ransomware attack showed how medical networks can be targeted and that high profile attacks can damage public confidence in the ability of institutions to protect personal data (Saxena et al., 2019, Ghafur et al., 2019).

Vulnerability

WIMDs are uniquely vulnerable to cyberattack due to certain limitations that arise when designing medical devices (Woods, 2016). WIMDs are often required to be extremely small, and the immediate proximity to human flesh limits manufacturing options in terms of battery supply, computing power, memory space, heating and cooling (Woods, 2016). Therefore, many WIMDs are built without considering cybersecurity (Burleson and Carrara, 2014). Furthermore, connecting WIMDs to remote networks that exchange data irrespective of time and place raises the potential for data leakage and increases the vulnerability to attack (Jiang and Shi, 2021). As more WIMDs are used, there will be a rise in wireless body area networks (WBANs), which establish networks of sensors located both in and around the body to communicate seamlessly with one another and to automatically exchange data with existing devices such as smartphones (Casselman et al., 2017). Remote and mobile WBANs composed of inherently vulnerable WIMDs present a palpable threat to data security, and as recently highlighted, “these devices were not designed to withstand terrorist attacks.” (Woods, 2016).

Impact

Discussions concerning cybersecurity in health have typically focussed on risks to electronic health records from digital theft and related breaches to data privacy (Ronquillo et al., 2018, Ghafur et al., 2019). However, the potential impact of compromised WIMDs in expansive future medical networks poses a direct threat to patient safety as well as to the ability of medical networks to function. Such breaches also pose indirect threats to patients through the potential for inaccurate or doctored health readings that could lead towards misdiagnosis or ineffective treatment. Informational breaches of this severity could erode public confidence in medical networks and induce a state of panic by raising concerns for public safety.

Individual attacks. Firstly, it has been well documented that a range of WIMDs have been compromised in recent years (Beavers and Pournouri, 2019). For example, it was demonstrated at the Black Hat security conference in Las Vegas that an insulin pump could be remotely hacked and controlled from 200 feet away (Casselman et al., 2017). By broadcasting a stronger signal than the intended monitoring device, it was shown that blood glucose readings could be manipulated and that a lethal dose of insulin could be remotely administered. The potential for similar attacks on pacemakers and ICDs has also been shown. A team of ethical hackers demonstrated how they could gain remote access to a series of pacemakers in order to deliver fatal shocks (Pauli, 2016, Beavers and Pournouri, 2019). Additionally, the recent rise in digital theft by using contactless point of sale terminals on public transport to surreptitiously charge a victim’s credit card, has been suggested as a possible means of targeting pacemakers (Horton, 2016, Beavers and Pournouri, 2019). It may be possible to attack a pacemaker or ICD from close range by simply swiping a programmed reader across a victim’s chest (Beavers and Pournouri, 2019). These methods could plausibly be used for assassination attempts on individuals known to have implanted medical devices. It was reported that former US vice-president Dick Cheney requested that his doctor disable the wireless function of his heart defibrillator due to his belief that the technological vulnerability of WIMDs posed a credible threat to his life (BBC News, 2013). As implantable devices become increasingly pervasive across society, influential individuals could be targeted via their WIMDs if efforts are not made to bolster the cybersecurity of medical networks.

Network disruption. Additionally, manipulating the monitoring and tracking capabilities of WIMDs could threaten long-term health and damage the stability of medical networks.

For example, devices that are controlled to overlook health warnings could detrimentally affect patient health by failing to encourage medical consultation and intervention. Alternatively, devices that are manipulated to falsely detect symptoms of ill health may lead patients to urgently seek out unnecessary medical attention thus placing a strain on medical networks. If coordinated attacks were orchestrated across multiple devices, a surge in requests for urgent assistance could overwhelm healthcare services. Furthermore, if a large number of WIMDs already connected to a medical network were compromised, multiple devices could be controlled to send synchronised alerts to inundate medical networks, causing them to shut down. For example, a large number of cyberattacks involve Distributed Denial of Service (DDOS), in which a targeted network is flooded with superfluous requests from multiple corrupted sources (Kaur Chahal et al., 2019, Deal, 2021). Such attacks, choreographed across an extensive web of WIMDs, could cause devastating disruption to critical infrastructure in the UK, such as the NHS.

***Attacks on critical infrastructure*.** Hackers may also exploit the vulnerability of WIMDs to strategically target individuals that serve a particular function in an organisational network. Such a strategy could be used in coordination with additional focussed cyberattacks in order to infiltrate or disrupt critical infrastructure. For example, attempts could be made to neutralise known threat intelligence analysts and management operation leads at the National Grid by infiltrating their WIMDs to provide health warnings that urge them to seek out immediate medical attention. If such efforts were coordinated with focussed attacks on the cybersecurity systems of the National Grid, the remaining personnel may be ill equipped to repel the threat. In the US, former Secretary of Defence Leon Panetta stated that cyberattacks on critical infrastructure could result in “a cyber Pearl Harbour, an attack that would cause physical destruction and the loss of life.”(Panetta, 2012). It has been suggested that such a catastrophic cyberattack could arise through coordinated efforts to infiltrate and manipulate WIMDs (Woods, 2016).

Panic and societal disruption. Finally, WIMDs are expected to proliferate across medical networks and become an integral part of healthcare delivery (Dinh-Le et al., 2019). Therefore, it is likely that breaches to highly sensitive health data and potential threats to patient safety would provoke mass fear and panic. Inducing widespread panic is considered a form of information-psychological warfare that occurs due to a lack of reliable information about frightening phenomena (Panchenko, 2020). Malicious actors intent on undermining national security could look to provide misinformation via WIMDs in order to bring about a state of panic. For example, as future WIMDs are designed to detect symptoms of infectious disease to prevent outbreaks of viruses such as COVID-19 (Ates et al., 2021), the coordinated manipulation of WIMDs could instil an unwarranted sense of panic by reporting that an infectious outbreak was underway. Such attacks would erode public confidence in the ability of medical networks to provide reliable information, as well as having the potential to cause mass panic and societal disruption.

Conclusions and Recommendations

WIMDs have the potential to produce vast amounts of data that could be used to generate innovative healthcare solutions and optimise the delivery of care (Deal, 2021). The emergence of WIMDs, combined with big data practices, could become a goldmine for public health researchers. However, greater effort is needed to rectify some of the inherent vulnerabilities of WIMDs. Discussions of the cybersecurity of health data must go beyond considering threats to data privacy in order to address the direct threat to life posed by breaches to WIMDs, as well as the potential for future disruption and panic. Multi-disciplinary approaches that combine the expertise of cybersecurity specialists with behavioural scientists may also help to anticipate how

the public is likely to respond to future breaches to WIMDs and integrated medical networks. Such combined efforts may be able to enact strategies that inform the public of relevant risks in order to mitigate the potential for disaster whilst still being able to reap the benefits promised by this emerging technology.

References

ATES, H. C., YETISEN, A. K., GÜDER, F. & DINCER, C. 2021. Wearable devices for the detection of COVID-19. Nature Electronics, 4, 13-14.

AUSTIN, L., SHARP, C. A., VAN DER VEER, S. N., MACHIN, M., HUMPHREYS, J., MELLOR, P., MCCARTHY, J., AINSWORTH, J., SANDERS, C. & DIXON, W. G. 2020. Providing 'the bigger picture': benefits and feasibility of integrating remote monitoring from smartphones into the electronic health record: findings from the Remote Monitoring of Rheumatoid Arthritis (REMORA) study. Rheumatology, 59, 367-378.

BBC NEWS. 2013. Dick Cheney: Heart implant attack was credible. BBC Online.

BEAVERS, J. & POURNOURI, S. 2019. Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions. Blockchain and Clinical Trial. Springer.

BURLESON, W. & CARRARA, S. 2014. Security and Privacy for Implantable Medical Devices, Springer.

CABINET OFFICE 2020. National Risk Register 2020. UK Government.

CASSELMAN, J., ONOPA, N. & KHANSA, L. 2017. Wearable healthcare: Lessons from the past and a peek into the future. Telematics and Informatics, 34, 1011-1023.

CHEN, P., DESMET, L. & HUYGENS, C. A study on advanced persistent threats. IFIP International Conference on Communications and Multimedia Security, 2014. Springer, 63-72.

DEAL, J. M. 2021. Exploring the Security Control Techniques Cybersecurity Specialists Need to Protect Medical Wearable Devices. Colorado Technical University.

DINH-LE, C., CHUANG, R., CHOKSHI, S. & MANN, D. 2019. Wearable health technology and electronic health record integration: scoping review and future directions. JMIR mHealth and uHealth, 7, e12861.

DUNN, J., RUNGE, R. & SNYDER, M. 2018. Wearables and the medical revolution. Personalized medicine, 15, 429-448.

GHAFUR, S., KRISTENSEN, S., HONEYFORD, K., MARTIN, G., DARZI, A. & AYLIN, P. 2019. A retrospective impact analysis of the WannaCry cyberattack on the NHS. npj Digital Medicine, 2, 98.

HORTON, H. 2016. Contactless card owners warned against public transport scanner hack. The Telegraph.

HULSEN, T. 2020. Sharing is caring—data sharing initiatives in healthcare. International journal of environmental research and public health, 17, 3046.

HUMER, C. & FINKLE, J. 2014. Your medical record is worth more to hackers than your credit card. Reuters. com US Edition, 24.

JACOBSSON, A., BOLDT, M. & CARLSSON, B. 2016. A risk analysis of a smart home automation system. Future Generation Computer Systems, 56, 719-733.

JIANG, D. & SHI, G. 2021. Research on Data Security and Privacy Protection of Wearable Equipment in Healthcare. Journal of Healthcare Engineering, 2021.

KAUR CHAHAL, J., BHANDARI, A. & BEHAL, S. 2019. Distributed denial of service attacks: A threat or challenge. New Review of Information Networking, 24, 31-103.

KINGSTON, A., ROBINSON, L., BOOTH, H., KNAPP, M., JAGGER, C. & PROJECT, F. T. M. 2018. Projections of multi-morbidity in the older population in England to 2035: estimates from the Population Ageing and Care Simulation (PACSim) model. Age and Ageing, 47, 374-380.

KRUSE, C. S., FREDERICK, B., JACOBSON, T. & MONTICONE, D. K. 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25, 1-10.

LIAO, Y., THOMPSON, C., PETERSON, S., MANDROLA, J. & BEG, M. S. 2019. The future of wearable technologies and remote monitoring in health care. American Society of Clinical Oncology Educational Book, 39, 115-121.

LUNA, R., RHINE, E., MYHRA, M., SULLIVAN, R. & KRUSE, C. S. 2016. Cyber threats to health information systems: A systematic review. Technology and Health Care, 24, 1-9.

OFFICE FOR NATIONAL STATISTICS 2020. Healthcare expenditure, UK Health Accounts: 2018. Healthcare expenditure statistics, produced to the international definitions of the System of Health Accounts 2011.

PANCHENKO, O. 2020. Panic as a factor of information security threat. Public Administration and Law Review, 4-9.

PANETTA, L. 2012. Remarks by secretary Panetta on cybersecurity to the business executives for national security. New York City, 11.

PAULI, D. 2016. Fatal flaws in ten pacemakers make for Denial-of-Life attacks. Viitattu, 14, 2017.

RODDIS, J. K., HOLLOWAY, I., BOND, C. & GALVIN, K. T. 2016. Living with a long-term condition: Understanding well-being for individuals with thrombophilia or asthma. International journal of qualitative studies on health and well-being, 11, 31530.

RONQUILLO, J. G., ERIK WINTERHOLLER, J., CWIKLA, K., SZYMANSKI, R. & LEVY, C. 2018. Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. JAMIA open, 1, 15-19.

ROSKI, J., BO-LINN, G. W. & ANDREWS, T. A. 2014. Creating value in health care through big data: opportunities and policy implications. Health affairs, 33, 1115-1122.

SAXENA, N., BHADORIA, R. S., DICKERSON, S., BRANCH, S., DALLEY, L. & CHURCHILL, N. 2019. Security and privacy issues in UK healthcare. Security and Privacy of Electronic Healthcare Records: Concepts, paradigms and solutions, 283.

STIGLBAUER, B., WEBER, S. & BATINIC, B. 2019. Does your health really benefit from using a self-tracking device? Evidence from a longitudinal randomized control trial. Computers in Human Behavior, 94, 131-139.

VAUPEL, J. W. 2010. Biodemography of human ageing. Nature, 464, 536-542.

WOODS, M. 2016. Cardiac defibrillators need to have a bulletproof vest: the national security risk posed by the lack of cybersecurity in implantable medical devices. Nova L. Rev., 41, 419.
YANG, Y., YANG, X.,

YANG, Y. & YUAN, Q. 2018. Aptamer-functionalized carbon nanomaterials electrochemical sensors for detecting cancer relevant biomolecules. Carbon, 129, 380-395