Biohacking Capabilities and Threat/Attack Vectors

Jaime Ibarra, Hamid Jahankhani, and Jake Beavers

Abstract The Internet of Things is a cutting-edge technology that organisations are adopting them in order to increase their business productivity and speed the operations. It has been involved for homes, companies, industries and now it is present in healthcare. However, due to lack of standardisation and accelerated competition, providers are deploying devices focused on innovation without having the proper balance between security, performance and ease of use. This is leading to new attacking vectors easing attackers to penetrate systems with confidence and without the need to be an expert in hacking thanks to the variety of open source tools available on the Internet e.g. Kali Linux, Github. The increased number of cyber attacks through IoT devices has complicated the performance of forensic investigators, reaching to Chains of Custody (CoC) easy to challenge by defenders and the rejection of investigation cases. Healthcare organisations has become the most attractive targets for cyber crime due to the variety and value of information allocated on Electronic Health Records (EHR).

This chapter aim to highlight the Biohacking capabilities and presents a Digital Forensic Investigation Process Model (DFIPM) addressing IoMT devices and assuring data privacy during the process.

Keywords Biohacking · Attack vector · IoMT · Healthcare data · GDPR · Digital forensics · Cloud computing

J. Ibarra · H. Jahankhani (✉)
Northumbria University, London, UK
e-mail: Hamid.jahankhani@northumbria.ac.uk

J. Beavers
Sheffield Hallam University, Sheffield, UK

H. Jahankhani et al. (eds.), *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-030-35746-7_7

1 Introduction

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. 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 [31]. Implanted Medical devices in particular 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, insulin pumps and even neural implants are commonplace in everyday life [10, 11]. There are an estimated 25,000 people every year in the UK that have a pacemaker fitted [30], 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 [9].

Many of these varying implantable 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 [26], 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.

Malicious attackers are enhancing their tactics, techniques and procedures (TTPs) in order to cause security breaches within organisations leading to data theft, manipulation or blackmailing for instance. An article from Forbes (2019) claims that Electronic Health Records (EHRs) can be worth $1000 (£778) for hackers and therefore the steady increase of cyber-attacks towards the medical sector. One of the most relevant breaches affecting medical processes was the WannaCry ransomware attack over England National Health Service (NHS) [20] that caused a total of 19,000 appointments cancelled and £92 million in investment to remediate and recover from the incident. In addition, an article presented by DiGiacomo [11] presents that in January of 2018 there were reported approximately 115 cyber-attacks, which the one with highest damage rate was over Health South-East RHF, a healthcare organisation that manages hospitals in Norway with a possibility that over 2.9 million users are potentially affected by the breach [5].

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 X-Ray systems, CT Scanners and even Blood Refrigeration Units [36]. 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.

2 Value of Healthcare Data for Organised Crime

The article from Morgan [25] points out how data breaches on healthcare are increasing steadily, reaching to a number of 20,836,531 records leaked. Attackers are showing their high interest in this type of information within healthcare services as shown on the previous section, and furthermore, the selling or health records in the black market are rising sharply.

Healthcare has become part of CNI because of the sensitivity of data held by these organisations. Furthermore, the fact that IoT has been involved in this sector enhancing services and easing patient's life style connecting more devices to the internet implies more risks associated in terms of cybersecurity.

The research from Ibarra et al. [13] claims that EHRs offer a significant wealth of information, attracting hackers to exploit and steal. It contains information such as:

- Demographic information.
- Full names, same as shown personal IDs, driver licenses, passports.
- Address history.
- Work history.
- Names, ages, contact details from relatives, which can belong to parents, siblings, life partners or any representative the health provider contacts this person in case the patient faces an emergency.
- Financial information, including bank details, credit/debit cards.
- National Insurance Number (Social Security Number outside the UK).
- Medical history, which contains sensitive information. It includes details of previous medical appointments along with details from doctors, nurses. Moreover, it likely has critical information such as allergy details, surgeries the patient was submitted, results from medical diagnosis such as xrays, electromagnetic resonance. The appointments listed include diagnosis, prescriptions, treatments and dates for the next medical control organised in a chronological manner.

EHRs contains precise details of the victim's life. Once a health provider was subject to a security breach compromising patient records, customers who got involved within the breach can likely get exposed to extortive blackmails for a lifetime. Furthermore, if EHRs contain additional information such as cancer diagnoses, STDs, psychological conditions established (i.e., asperger syndrome, autism, depression, alcoholic), the victim can be exposed to public embarrassment or political assassination depending on the goals of the attackers.

The research from Terry [33] claims that the development of electronic patient health record (E-PHR) systems, the usage of personal health technologies and the Internet of things (IoT), caused policy-makers to highlight a big concern regarding the massive increase of IoT devices used by consumers, whilst data is created and processed every second therefore, the increase of cyber threats and attacking vectors. In addition, he also points out a great challenge to protect healthcare data in the future. This is due to the lack of training and preparation for precision medicine, and usage of robotics for sensitive procedures like surgeries for instance. Therefore the need for the deployment of reliable frameworks, methodologies and standardisation of technologies that could allow organisations to protect their digital assets and respond effectively against any security breach attempt. In addition, the process model proposed for forensic investigation would support businesses to learn from their previous mistakes in order to harden the security posture. Nowadays cyber security is a vital component for businesses to continue competing within the market and it is paramount to adopt the last updated technologies along with training and awareness methodologies before, during and after an incident. This could support investigators to execute the expected top level reports in order to track the origin and author of the unauthorised activities.

3 GDPR in Healthcare

It is necessary to understand how the implemented GDPR has taken effect across IoT networks in order to determine the deliverables, and ascertain with the main stakeholders within the usage of IoT-based medical devices. This will be performed by critically analysing the research from O' Connor [29], which proposed an approach of the "Privacy by Design" principle for IoT environments. This research highlights the importance of an electronic consent (eConsent) in order to proceed with data management, being proactive and not reactive for instance. This regulation points out with emphasis the importance of assuring data privacy and the protection of owners when their personal data has being compromised. In forensic investigation, the assurance of transparency and privacy are vital because businesses must keep producing during an incident, otherwise it would imply significant financial losses, customer dissatisfaction and therefore, their reliability would decrease. In addition, the GDPR sets up to £17 m in fines if the local authority considers that the organisation was considered incapable of executing the necessary steps to protect personal information.

The research from Shu and Jahankhani (2017) claims the impact of the GDPR on the Information Governance Toolkit pointing out on healthcare. Mentioning the impact of cloud computing for allocation of huge amounts of data with focus on six benefited assets as shown in Fig. 1. Governance is one of the main components for effective cyber security regardless of the speciality area. Effective communication and control allows to achieve regulatory compliance and policy enforcement assurance. During a forensic investigation, it is possible that policies

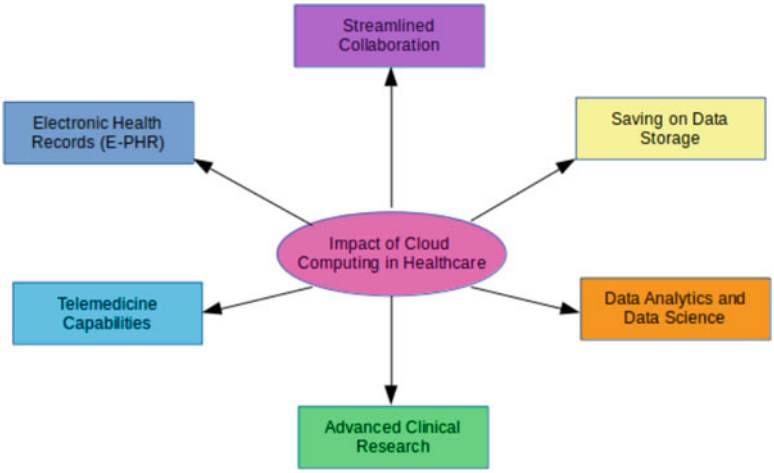

Fig. 1 Impact of cloud computing in healthcare

and procedures would get changed as result of the lessons learned during a cyber incident along with modifications on the technical infrastructure and configuration management procedures.

4 The Role of Forensic Investigation in IoMT

Forensic investigation is an essential part of incident response in cyber security following the NIST Cyber Security Framework. It shows details of the performance of the intrusion, actions and methods that attackers performed, along with assets compromised (systems and/or data). Furthermore, it allows organisations to learn from those mistakes in order to mitigate risks and if applicable the modification or implementation of new cyber security strategies either technical, organisational or legal because compliance is a feature in this field.

Healthcare providers must get adapted to the last updated guidelines, frameworks and standards because the are holding sensitive data that could cause unmeasurable damage if it gets leaked. In addition, the adoption of IoT in medical environments expanded the risks within the industry and because IoT is not standardised yet, can cause extensive trouble for investigators to collect evidence and present comprehensive reports either for courts and the compromised organisation in order to mitigate risks.

However, the threat landscape is subject to modifications and it would depend whether the Internet of Things gets standardised or not during the next years. Otherwise, it will difficult the job from forensic investigators leading to cases rejected or lost due to lack of relevant evidence supporting the investigation.

4.1 Challenges of Digital Forensic Investigation in IoMT

Digital Forensic (DF) investigation is a process that works along with Incident Response in order to extract information from a particular device, system or infrastructure, which is submitted to analysis, preservation and presentation of digital evidence that can be used to identify activities related to security/policy violation or crime. Nevertheless, there is not a standardised model that can provide an overview of the entire investigation. In fact, some of these came from the experience of ethical hackers, system administrators and law enforcement entities without the solidity and consistency that involves every stage of the investigation (technical and non-technical). An investigator might present relevant and incriminating evidence in a comprehensive and consistent manner targeted to legal authorities, otherwise the case may be lost or discarded during the investigation process [22, 23, 24]. Considering that most of devices are unlikely to show or contain the necessary consent from users [29], the limitations that Internet of Things (IoT) present in terms of hardware and software, the complexity in its architecture, no standardisation present, along with the recently enforced European Global Data Protection Regulation (GDPR), the requirement to define a comprehensive and holistic forensic investigation model that ensures data privacy and compliance maintaining most discretion during an investigation in order to protect people during and after a security breach.

Khan et al. [18] claim that forensic investigation in the Internet of Things demands solutions from researchers, security and IoT experts, along with cloud computing providers to secure the infrastructure during a security incident. Nowadays, it is a fact that one of the main targets for malicious attackers are EHRs from patients and therefore, investigators muse assure privacy to data owners during the investigation process. This is because stolen records can lead to severe damage including terrorist-based attacks attempting against the person's life.

The information showed below following Fig. 2, shows the challenges that forensic investigation presents in medical IoT along with details of each component mentioned in the mind map. Considering that IoT works on a similar way as cloud it has been divided into three stages that require investigation. Firstly the device from users, secondly the network where the information is being transmitted and finally the cloud servers. It is important to recall that all digital evidence extracted and sent to courts must be reliable, authentic, complete, believable and admissible in order to present it showing the overall of the investigation.

In addition the evidence analysed must contribute to the incrimination of the malicious actor involved with the unauthorized action performed. Details of every component of forensic investigation in IoMT along with their own challenges are shown below.

Fig. 2 Digital forensics challenges in IoMT

5 Attack Vectors

All medical implants are required to operate on the MICS band [35], this range is 402 MHz to 405 MHz. There have been many successful hacking attempts on implants by hijacking the RF module [12], this is the most commonly used communication method for implants, this however is due to change and be updated to Bluetooth technology. There is a serious risk for medical equipment within third parties companies and institutions such as the NHS, there were 93 cyber-attacks taken place in healthcare organizations from 2013 to 2016 [2].

The paper "Hacking NHS Pacemakers: A Feasibility Study" [1] demonstrates a blackbox test on NHS implants, in this case pacemakers were chosen. Based on the results the most common attack vectors can be defined as:

- Denial of Service (DoS)
- Replay Attacks
- Code Injection Attacks

5.1 Denial of Service (DoS)

DoS is a type of cyber-attack, the intended aim of which is to take the targeted source offline [7]. 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 [16].

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 (Thakur n.d). 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.

5.2 Replay Attack

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.

5.3 Code Injection

Code injection is a generic term that refers to the unauthorised uploading of potentially malicious code [6]. 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.

5.4 Summary

Radio Frequency has been previously stated as being easily breakable, however, the results from the 2019 work 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 in 2019 were provided by the NHS, they were standard modern units and as such it is expected that they should have a reasonable defence against hacking. The conclusion of the work was that for the attacks to work, the individual must have expertise and knowledge of both wireless commination (in this instance RF) and the inner workings of the devices being targeted.

6 Forensic Investigation on the Internet of Things and Considerations on 5G Networks

As shown in Sect. 4.1, performing forensic investigation on IoT is complex due to the multiple architectures that investigators have to deal with. In addition, the arrival of 5G makes it more complex because of the massive use of Software Defined Networks (SDNs). Performing forensic investigation on IoT could mean to interact with cloud servers, communication between different VPSs, performing packet analysis between transport networks and SDNs and also analysing infected devices of end users that could violate their rights in terms of data privacy.

The proposed forensic investigation process model is done considering the main components that involve an IoT architecture as mentioned on the previous sections. It has been designed from high to low-level approach allowing forensic investigators to obtain precise information and retrieve a better perception over the detailed components, named processes, stages, sub-stages and principles. It consists of 7 processes, which each one is formed by a different number of stages. This guideline is shown only at its high level, and details of the model can be found at the research from Ibarra et al. [13]. The overview of this model works along with eight concurrent processes regardless of the architecture investigators are interacting with (Fig. 3):

- Preserve Digital and Physical Evidence – Evidence must be retained in its original form and its integrity must be preserved from the opening to the closing stage of the investigation for both physical and digital evidence. It is paramount for investigators to show that evidence has not been altered and if some unavoidable changes were made to report them and justify. IoT networks deal with massive amounts of personal data therefore, the requirement of ensuring privacy during the investigation to assure GDPR compliance. Achieving privacy and integrity of physical and digital evidence ensure a high quality investigation and reliable evidence to present it to a court. The preservation process might involve investigators to prevent people without authorisation to enter or leave the crime scene, system/device/network/VPS isolation to acquire the volatile data and locate suspicious processes running. Preservation also includes the assurance of log files before its removal and a full backup of the imaged system.
- Preserve Chain of Custody – Digital evidence is often prone to be handled by different parties, and in some cases its poor preservation allows courts and defensive members to challenge it with confidence leading to its rejection.

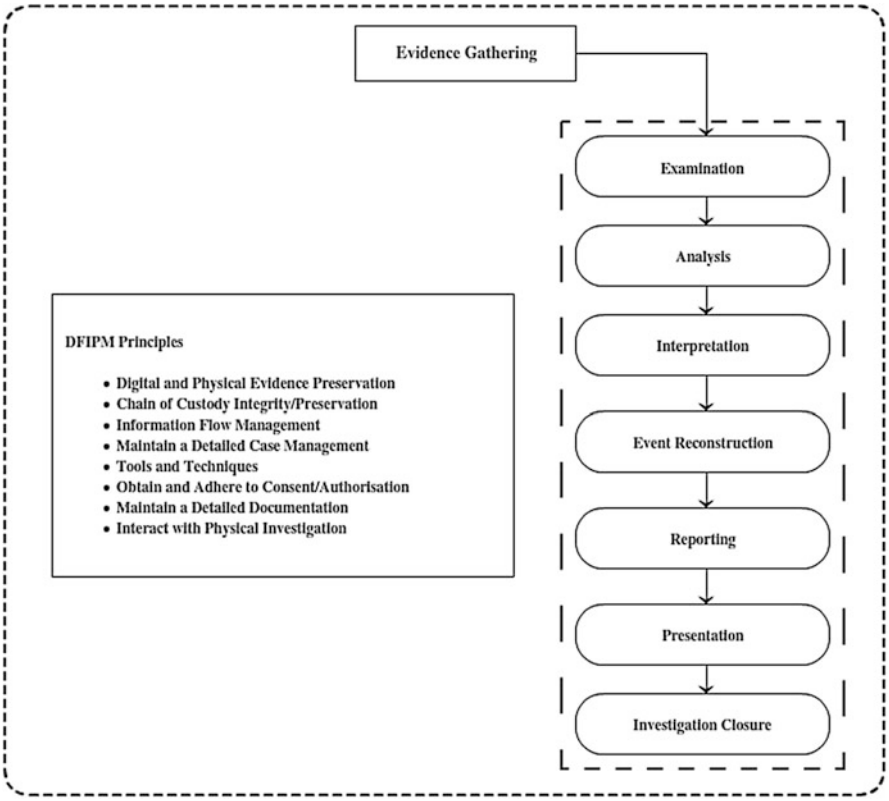

Fig. 3 Guideline for forensic investigation on IoMT

Events are correlated in order to reconstruct the crime scene within a CoC, and this must be considered the main component for any forensic investigation. Potential digital evidence is gathered from threat hunting and incident response (IR) detection stages, processing physical and digital crime scenes, hence the initiation of the CoC and this principle should be observed from the IR detection stage. Proper, accurate and detailed documentation are essential to preserve the CoC as well as supporting evidence such as videos, pictures and drawings. In addition, a reliable CoC demands from investigators to records of the personnel responsible for handling evidence including actions taken with dates and it might require the development of supporting documents that would contribute to the final report prior to its presentation in courts.

- Manage Information Flow – This principle is about the permission for investigators to interact with the variety of laws, languages, etc. appropriately during the entire investigation. One example is the interaction between two investigative entities responsible for the same case, or digital evidence exchange between parties. It can be protected using hashing algorithms such as MD5, SHA-1 or any PKI-based encryption.

- Maintain a Detailed Case Management – It refers to manage wisely the investigation, record and keep track of evidential items, events and crucial forensic findings. Casey [4] points out the importance of this principle as one of the main components of scaffolding to bind all evidence, reports, supporting documentation for the building of a strong case. Likewise, Khatir et al. [19] highlights the effectiveness of an investigation based on strong case management.
- Prepare Tools and Techniques – Forensic investigators must need to use diverse tools and techniques to perform each process during the investigation. This principle is extensively covered by standardised documents such as NIST [17], The International Organisation for Standardisation (2005), (2013), same as technical reporting like the Information Assurance Advisory Council (IAAC) [32]. The known tools can be used for system imaging and data carving i.e. FTK, EnCase, as well as for packet analysis i.e. Wireshark, Tcpdump, Solarwinds. However for IoT devices it is likely to perform some reverse engineering techniques to assess the behaviour of the firmware and determine any malicious code modified against the original with tools such as IDAPro, GDB for instance and the execution of MITM attacks to extract the current firmware from the device depending on the communication protocols developed by the provider. For IP address tracking there are a variety of open source and online tools i.e. ping, nslookup, dig, traceroute, Whois, WhatIsMyIPAddress [34] or IP Location [14].
- Obtain and Adhere to Consent – Any investigation requires authorisation either internal or external. This principle requires from investigating entities to obtain proper consent from: governments, system administrators, users., when carrying out an investigation. Now that GDPR has been implemented across Europe, it is paramount for investigators to execute processes precisely because personal data must not be compromised during an investigation and the protection of people is crucial. In addition, it is possible that users must not allow the retrieval of potential evidence for security reasons that could likely interfere with the performance of investigators. One option is the proposal of a smart contract [21], based on blockchain technologies that allows to perform a secure and reliable forensic investigation.
- Maintain a Detailed Documentation – Activities and actions performed must be logged and documented in detail using comprehensive vocabulary that would allow legal courts to understand the details of the crime executed in order to make fair decisions when the case is presented on audiences. The documentation includes possible changes across the investigation that should be recorded and mentioned during the presentation to justify the actions that investigations performed.
- Interact with Physical Investigation – Even the crime was performed in the digital world, the main component of technology is people. Investigators must interact with people involved in the scene that might witness some unusual event that could contribute to the development of the investigation. However, details should be recorded and authorised by the witness to be presented due to the GDPR regulation. The more supporting evidence investigators collect to present at courts, the stronger and more reliable the CoC gets.

The adoption of IoT must be heavily considered as an important use case in 5G because of the resource constraints that these devices currently have (e.g. e-home, wearable/implantable devices, industrial IoT). It is paramount to consider that 5G networks offer higher download/upload speed rates, and the current cyber attack trend that is currently affecting 4G. Therefore, 5G will offer more efficient execution of attacks especially affecting the most of software-defined layers.

For instance, as shown in the research by Nomikos et al. [28], the communication in 5G is defined by software as well bringing the challenge of creating a Dynamic Radio Access Control Network (DyRAN). Hence, controlling unusual behaviour in this part is important to avoid resource consumption, and this lack of accountability is of course a clear problem for IoT as shown in Nieto et al. [27], which clearly affects 5G networks as well.

Other important feature of 5G is the Device-to-Device (D2D) communication created to increase the coverage of the network e.g. network relays [28]. This could facilitate the set of vulnerabilities and attacks propagated hop by hop leading to possible access to critical parts of the infrastructure i.e. software controllers. As shown in the ENISA 5G security report [3], SDN controllers are prone to attacks to the communication APIs between controllers and between controllers and the SDN elements close to the end user.

One of the most important topics to discuss in 5G is the Mobile Edge Computing (MEC), bringing improvements in terms of data, storage and performance exploiting the latests changes in this new architecture. Therefore, the requirement of working with massive data traffic amounts. Finally, a critical feature is the ability to virtualise network functions and thus, using Network Function Virtualisation (NFV) allows to replace software with more ease compared with hardware based networks. This can allow to isolate attacks immediately by just stopping the service and containing the infected VPS, but on the other side the use of software leads the system to vulnerabilities related to coding errors and the requirement of constant patching.

References

1. Beavers J (2019) Hacking pacemakers: a feasibility study. In: IEEE 12th international conference on global security, safety and sustainability (ICGS3)
2. Beavers J, Pournouri S (2019) Blockchain and clinical trial. Springer. Chapter 11: recent cyber attacks and vulnerabilities in medical devices and healthcare institutions
3. Belmonte Martin A, Marinos L, Rekleitis E, Spanoudakis G, Petroulakis N (2015) Threat landscape and good practice guide for software defined networks/5G. European Union Agency for Network and Information Security (ENISA), Heraklion
4. Casey E (2011) Digital evidence and computer crime: forensic science, computers and the internet, 3rd edn. Elsevier Academic Press, New York
5. Cimpanu C (2018) Hacker might have stolen the healthcare data for half of Norway's Available at: https://www.bleepingcomputer.com/news/security/hacker-might-have-stolen-the-healthcare-data-for-half-of-norways-population/. Accessed 25 Dec 2019
6. Code Injection (2013). Retrieved from https://www.owasp.org/index.php/Code_Injection

7. Denial of Service (2015). Retrieved from https://www.owasp.org/index.php/Denial_of_Service
8. DiGiacomo J (2018) Data beach statistics for 2018 plus totals from 2017 | Revision Legal %. [online] Revision Legal. Available at: https://revisionlegal.com/data-breach/2018statistics/. Accessed 10 Feb 2019
9. 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/
10. 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
11. Focus on: Pacemakers (n.d.). Retrieved from https://www.bhf.org.uk/heart-matters-magazine/medical/pacemakers
12. Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, Fu K, Kohno T, Maisel WH (2008) Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. IEEE symposium on security and privacy
13. Ibarra J, Jahankhani H, Kendzierskyj S (2019) Cyber-physical attacks and the value of healthcare data: facing an era of cyber extortion and organised crime. In: Blockchain and clinical trial. Springer, Cham, pp 115–137
14. IP Location (2016) Where is geolocation of an IP address? Available at: https://www.iplocation.net/. Accessed 30 Aug 2019
15. Jack B (2017). Retrieved from https://en.wikipedia.org/wiki/Barnaby_Jack
16. Jamming & Radio Interference: Understanding the impact (n.d.) The institute of engineering and technology. https://doi.org/10.1049/etr.2012.9002
17. Kent K, Chevalier S, Grance T, Dang H (2006) Guide to integrating forensic techniques into incident response. NIST Spec Publ 10(14):800–886
18. Khan S (2017) The role of forensics in the internet of things: motivations and requirements. IEEE Internet Initiative eNewsletter
19. Khatir M, Hejazi M, Sneiders E (2008) Two-dimensional evidence reliability amplification process model for digital forensics. In: Third international annual workshop on digital forensics and incident analysis, pp 21–29
20. Lam B (2017) NHS cyber attack: views from the front line. Pharm J. Retrieved from https://www.pharmcaceutical-journal.com/opinion/qa/nhs-cyber-attack-views-from-the-front-line/20202794.article
21. Lone AH, Mir RN (2018) Forensic-chain: ethereum blockchain based digital forensics chain of custody. SPCSJ 1(2):21–27; Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587–4667
22. Montasari R (2016) The comprehensive digital forensic investigation process model (CDFIPM) for digital forensic practice. PhD thesis, University of Derby
23. Montasari R (2017a) A standardised data acquisition process model for digital forensic. Int J Inform Comput Secur 9(3):229–249
24. Montasari R (2017b) Digital evidence: disclosure and admissibility in the United Kingdom Jurisdiction. In: International conference on global security, safety, and sustainability. Springer, Cham, pp 42–52
25. Morgan L (2018) List of data breaches and cyber attacks in March 2018. [online] IT Governance Blog. Available at: https://www.itgovernance.co.uk/blog/list-of-data-breachesand-cyber-attacks-inmarch-2018/. Accessed 26 Apr 2018
26. New York Post (2016) Yes, pacemakers can get hacked. Retrieved from http://nypost.com/2016/12/29/yes-pacemakers-can-get-hacked
27. Nieto A, Roman R, Lopez J (2016) Digital witness: safeguarding digital evidence by using secure architectures in personal devices. IEEE Netw 30(6):34–41
28. Nomikos N, Nieto A, Makris P, Skoutas DN, Vouyioukas D, Rizomiliotis P, Lopez J, Skianis C (2015) Relay selection for secure 5G green communications. Telecommun Syst 59(1):169–187
29. O'Connor Y, Rowan W, Lynch L, Heavin C (2017) Privacy by design: informed consent and internet of things for smart health. Proc Comput Sci 113:653–658

30. Pacemakers (n.d.). Retrieved from https://www.bhf.org.uk/heart-health/treatments/pacemakers
31. 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/
32. Sommer P (2008) Directors' and corporate advisors' guide to digital investigations and evidence. U.K. Information Assurance Advisory Council. Available at: https://www.ucisa.ac.uk/~/media/Files/members/activities/ist/DigitalInvestigationsGuide.ashx. Accessed 30 Aug 2019
33. Terry N (2017) Existential challenges for healthcare data protection in the United States. Ethics Med Pub Health 3(1):19–27
34. WhatIsMyIPAddress (2016) How you connect to the world. Available at: http://whatismyipaddress.com/. Accessed 30 Aug 2019
35. Yuce MR, Islam MN (2016) Review of medical implant communication system (MICS) band and network. ICT Express 2(4):188–194. https://doi.org/10.1016/j.icte.2016.08.010
36. 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/