Modelling Medical Devices with Honeypots

Jouni Ihanus[1] and Tero Kokkonen[2]

[1] Huld Oy, Kuopio, Finland jouni.ihanus@huld.io
[2] Institute of Information Technology, JAMK University of Applied Sciences, Jyväskylä, Finland tero.kokkonen@jamk.fi

Abstract. Cyber security is one of the key priorities in the modern digitalised and complex network totality. One of the major domains of interest is the healthcare sector where a cyber incident may cause unprecedented circumstances. In the healthcare domain there are abundant networked systems, software and hardware, which may be vulnerable for a cyber intrusion or incident. For cyber resilience, it is important to know the status of the valuable assets under attention. Sensor information has a significant role for achieving the comprehension of the valuable assets in the cyber domain. While networked medical devices form an important asset group in healthcare environment, one interesting solution to gather sensor information are the honeypots. In this paper, honeypot technology is studied for the healthcare domain. Especially typical characteristics of medical devices are considered from the perspective of modelling the medical devices with honeypots. The technical priorities are studied and concluded with the discovered future research topics.

Keywords: Honeypots · Cyber Security · Situation Awareness · Intrusion detection

1 Introduction

Cyber domain is an extremely complex entity. For realising the status of the valuable assets in the cyber domain, sensor based Situation Awareness (SA) is required. The Endsley's well-known definition of SA is recognized as follows: *"Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future"* [9]. By reflecting on the Endsley's definition of SA, it can be comprehensively seen that technical visibility gained by sensor information has a fundamental role for achieving the relevant SA in the complex cyber domain. For understanding the current situation and for making decisions based on that understanding, the relevant SA is required. That can be appreciated by considering the two classical decision-making models, OODA-loop (Observation-Orientation-Decision-Action) [25] and Gartner's four stages of an adaptive security architecture (Predict-Prevent-Detect-Respond) [18].

One of the typical approaches for technical visibility is the Intrusion Detection System (IDS). IDSs are used for guarding the traffic by detecting possible illicit activity. In general, IDSs are classified as follows: anomaly-based detection

(anomaly detection) and signature-based detection (misuse detection). Anomaly detection is capable of detecting unknown attack patterns; however, the shortcoming of anomaly detection is its high false detection rate as it generating a large amount of false positive indications. Misuse detection has the capability to detect predefined known attacks with a high detection accuracy; however, it cannot detect undefined unknown attacks [26, 24].

For tackling the infirmities of IDSs the honeypots can be used. As stated in [13], honeypots are an advanced concept to gain information about intrusions. If an attacker is capable of intruding into the network, there is a honeypot resembling the asset under protection that will be assaulted by the attacker, and the original asset under protection remains safe behind the honeypot under attack [37]. Honeypots can be used for luring and alerting about intrusions or attacks and gathering beneficial technical information about the used techniques and methods of attacks [21]. Ordinarily honeypots are capable to be used for server-type systems [2].

Honeypots are widely used in different domains. Authors of [38] used honeybot for attack capture in Software Defined Networking (SDN), while Djanali et.al introduced a honeypot for emulating vulnerabilities for XSS and SQL injection attacks with the capability of exposing attacker's identity [8]. Study [29] proposed honeypots for a power grid against Advanced Persistent Threads (APT). Anwar et.al proposed an algorithm for honeypot allocation over attack graphs [3], while Mayorga et.al used honeypots for detection and prevention tool in a network through attack patterns [17]. Honware is a honeypot framework capable of emulating Customer Premise Equipment (CPE) and Internet of Things (IoT) devices for detecting earlier unknown vulnerabilities, so called zero day vulnerabilities [36]. In the study [5] honeybots were implemented for Direct Digital Controls (DDCs) of building automation systems. A five-year analysis of honeybots concluded the capability to avoid the majority of the attacks made by both humans and bots [16].

In the healthcare domain, honeybots are used for example in the mobile health concept [4] and for the security of Electronic Health Record (EHR) based big data [6]. When focusing on the healthcare sector and especially the medical devices, the main contributions of this paper are: what are the typical technical characteristics of the networked medical devices and how can the medical devices be modelled with honeypots?

The paper is organised as follows. First, in section 2, the overview of healthcare environment with common technical elements and threats is presented. After that, in the section 3, modelling of medical devices is described. Lastly, the study is concluded with found future research topics in section 4.

2 Overview of Networked Medical Devices

The honeypots tend to imitate a defined information system service to invite illicit users to interact with them [19]. In order to model the medical devices with the honeypots, it is important to understand how to masquerade the honeypot

as an authentic system. For this conclusion, understanding of the information system under review should be reached.

2.1 Healthcare Environment

Medical devices are widely used at different levels of medical treatment. To comprehend the security challenges of the medical devices, it is significant to understand the architecture. The network model proposed by Yaqoob et.al states a three-tiered model as presented in Fig. 1. *Tier 1* presents a considerable number of different medical devices for diagnosis, treatment and monitoring of medical conditions. These devices include wearable, implantable and on-site medical devices. *Tier 2* depicts the gateway level which is responsible for transmitting and processing data received from tier 1. *Tier 3* presents systems utilized to store and analyse the gathered data. These elements form highly interconnected information systems with multiple attack vectors [40].

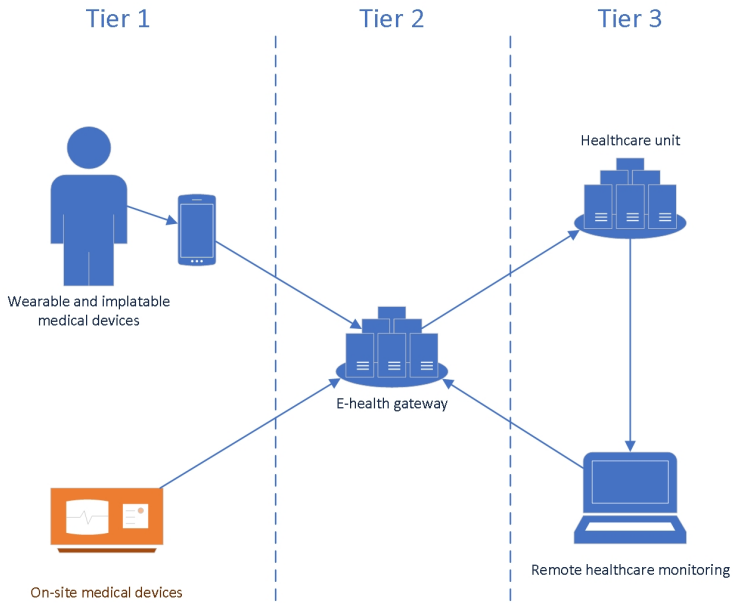

Fig. 1: Tiers [40]

The structure is presented in Fig. 2 on a more practical level. This example presents concretely some of the assets on Tiers 1 and 3. The example aims to emphasize the connection between medical devices and interconnected information systems. Previous studies present that these assets are seen as the most critical ones in the context of smart hospital environment [28].

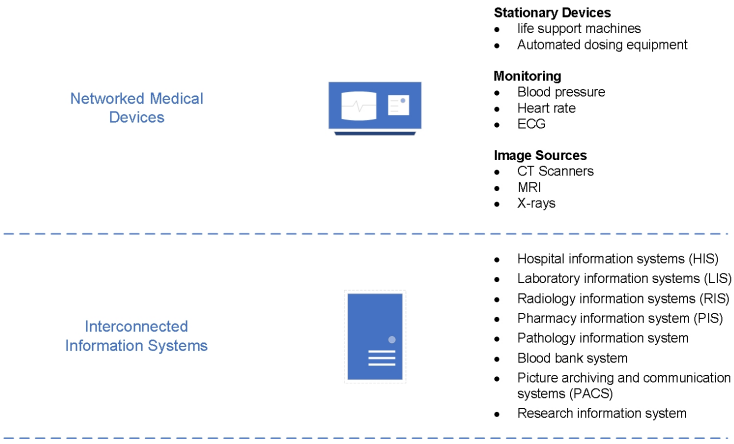

Fig. 2: Structure [28]

When estimating the number of devices, the per-patient devices emerge from the data. Study by [12] states that these devices form the majority of the healthcare devices in a typical healthcare environment. As analysis presents, this is logical, as per-patient devices track and monitor patients on a 1:1 ratio while devices such as CT scanners are shared with multiple patients.

2.2 Restrictions on the implementation of technical security controls

Medical devices make a crucial contribution in diagnosing, preventing, monitoring, treating illness as well as overcoming disabilities. This role places demands for the safety and efficacy of the medical devices. The domain is highly regulated. [10, 34] Medical device manufacturers are under exact regulations to establish and maintain procedures to validate the device design. Changes in device design have to go through appropriate verification procedures for approval before their implementation [34]. These regulations also affect how cybersecurity updates and controls can be implemented to medical devices. In certain cases, even routine updates and patches require reporting to authorities [33]. While [22] states that many medical devices are sold without typical security controls, implementing security controls to a medical device can cause challenges and/or design changes. For example, [32] present a severe incident occurred during the medical procedure. In this case, the misconfiguration of antivirus software caused the crashing of patient monitoring system. The root cause behind this incident was that the instructions delivered by the medical device manufacturer were not followed. In another example presented by [31], one healthcare professional expressed challenges to follow given instructions, as antivirus software version validated by manufacturer was no more available for purchase.

2.3 Common Technical characteristics

According to study of [28], networked medical devices are seen as critical assets by 67 percent of responders. At the same time maintaining the cyber security of these devices has proven challenging: the analysis presented in [12] indicates that in 2019, 70 percent of the medical devices were running operating system versions that will have been unsupported during the first quarter of 2020. The data set under review included 75 healthcare deployments. According to [23], the situation seems particularly bad for medical imaging systems, as 83 percent of all of them run an end-of-life operating system with known vulnerabilities. The problematics of outdated operating systems relating to the medical devices has also been recognized in other studies [30, 7, 23, 12, 35]. While patching these devices is clearly challenging, the study by [39] presents a steady increase in the number of vulnerabilities related to the medical devices. These devices can form a prominent risk to the hospital assets if compromised. As an example, some of the identified cases show that the medical devices were used to enable backdoors into the hospital networks. In these cases, this channel was further utilized for lateral movement and for exfiltration of the confidential hospital data [30]. One of the reasons behind the threats relating to lateral movement is insufficient network segmentation. The analysis by [23] states that 72 percent of healthcare VLANs contained a mix of a wide variety of different devices, also including medical devices.

On the operating system level, the data set analysed in the study of [12] states that most of the devices in medical networks were running the Windows operating system. The rest of the devices detected included Linux, Unix and embedded systems. The emphasis of Windows systems on medical devices can also be observed in other studies [23]. Many of these devices were running high-risk services. The most common Windows services relating to medical device networks presented in the study by [12] are as follows: SMB, RDP, FTP, SSH, Telnet, and DICOM Imaging Protocol.

It should be noted that SMB and RDP implementations have both been lately exploited by modern automated threats: In 2017 WannaCry ransomware was used in a massive attack, which infected systems in over 150 countries. WannaCry worm component used SMB vulnerability for initial infection [1]. In 2019 similar wormable vulnerability concerning RDP was found [20].

Another key observation is that some unencrypted protocols such as Telnet and FTP are still present. Unencrypted traffic, especially while concerning medical data, poses a great threat to cyber security [12]. At the same time encrypted traffic poses a challenge for network IDS systems as the detection capabilities are limited [11, 15].

2.4 Typical threats

Threat modelling can be seen as a practical discipline to use different techniques to find security problems [27]. Regarding the medical devices, multiple reports

have addressed this issue [30, 23, 12, 35]. In this study this information is used as a motivation for defining key use cases for the honeypot usage.

By reflecting the studies above, following challenges can be observed:

- Most of the medical devices use an outdated Windows operating system
- There is a significant challenge to patch medical devices
- There is a challenge in sufficient network segmentation in healthcare environments
- Technical visibility to medical devices is limited

By reflecting the studies above, the following threats have materialized:

- Malware infections in medical devices
- Utilization of a medical device in lateral movement
- Utilization of a medical device as a backdoor to hospital network
- Utilization of a medical device as a pivot device in cyber attack

In summary, a considerable part of the medical devices are running outdated and insecure operating systems, which may pose several threats to the operating environment. At the same time the visibility to these devices can be limited due to restrictions to implement security controls on them.

3 Construction

A typical use case for using honeypot technology is to gain more technical visibility. Honeypots are used as a source of sensor data, which supports perceiving elements in cyber environment. In this chapter honeypot specific features are correlated with typical characteristics of healthcare environment and medical devices to support technical visibility. The main contribution of this study is summarized in the form of a construction model.

3.1 Technical definition

To understand possibilities to reduce the threats presented above with honeypots, challenges relating to technical visibility should be summarized. Based on the studies presented above, the key challenges to gain the needed technical visibility are presented as follows.

1. Host level visibility
   (a) Challenges to implement host based security controls
   (b) Challenges to implement host based security monitoring
2. Network level visibility
   (a) Usage of encrypted protocols
   (b) Insufficient network segmentation – Visibility relating to lateral movement

To model devices with honeypots, the operational elements of the sensor need to be taken into account. From the technical point of view, a networked medical device appears as a rather typical device in a healthcare network. However, there are individual characteristics that can be noted. These characteristics can be divided into following levels:

1. Operating system level
   (a) Most commonly older versions of Windows operating system
2. Service level
   (a) Quite typical service profile with healthcare specific services like DICOM
3. Network level
   (a) Mixed networks with low segmentation profile

3.2 Model

In the chapters presented above, following elements relating to networked medical devices have been discussed:

- Threats relating to networked medical devices
- Challenges relating to technical visibility
- Individual characteristics of networked medical devices

Combining these elements with a modified construction model based on [14], refined cyber situation awareness can be reached. The construction presented in Fig. 3 leans heavily to **risk management**. The actual need for situation awareness together with **technical visibility** should be defined through an organization's risk management functions. From a technical point of view, the defined need should be fulfilled with appropriate sensor technology, which in this case is the honeypot technology. **Sensor elements** relating to honeypot should be defined with the emphasis on typical characteristics of the operating environment. When a need for technical visibility encounters capabilities of sensor technology, the wanted refinements for situation awareness can be reached.

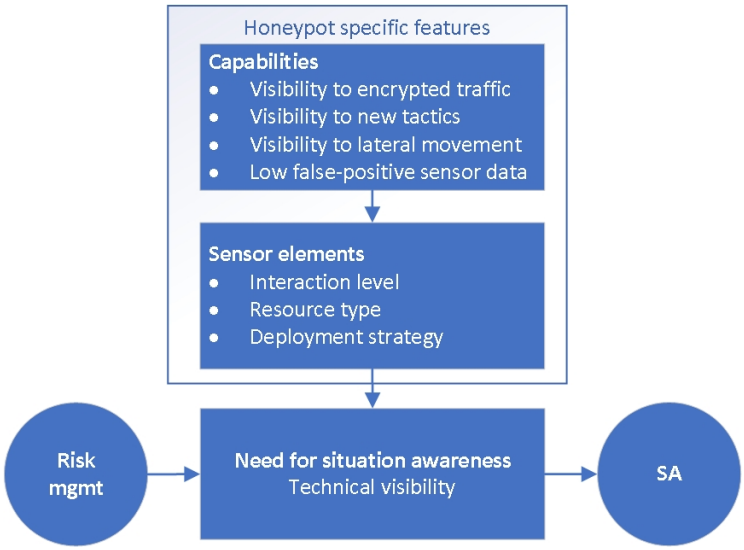

Fig. 3: Construction model [14]

Honeypots have certain unique technical **capabilities** which can be used to gain the technical visibility observed in this study: Honeypot architecture is based on emulating the target system on an adequate level. Thereby, on the network level the honeypot appears as a rather typical networked medical device. While using encrypted protocols, a honeypot operates as one of the endpoints. For this reason, there is no need for additional decryption methods. Honeypots can also be used to detect lateral movement, when located in the same network segment with the primary assets. This architecture also offers visibility to new tactics as the methods used against device can be highly monitored. It should be noted that the restrictions relating to the original system do not inherit to the honeypot system, as the original system is left untouched. On the host level, this offers possibilities to implement security controls and monitoring features for the required purpose. This architectural model also affects the liability of the sensor data received from the honeypot. As the system has no real legit function from users' point of view, all interaction can be defined as illicit action with high certainty.

Sensor elements present how honeypots operate on a more detailed level: Interaction level defines how deeply a system emulates the target system, which also affects the monitoring capabilities that a sensor can offer. For example, the capability to detect new tactics and methods might be affected by this feature. The resource type defines the type of information system resource emulated by the honeypot. The resource type can be defined on protocol level, which in this use case can include typical protocols used in medical devices. To support the effectiveness of the honeypot sensor, also the deployment strategy should be considered. This feature indicates the tactics of deploying honeypots in a defined

operating environment. A wide variety of approaches can be selected to support priorities of technical visibility.

4 Conclusion

This study proposes a new construction model to specify how medical devices can be modelled with honeypots. The main attributes identified behind this model are threats facing the healthcare environment, typical technical characteristics of the medical devices and challenges in technical visibility. Sensor technology based on the honeypots can offer added value by gaining technical visibility in areas that are typically challenging in a defined operating environments. It can be concluded that the honeypots can be used to model the assets under review.

For future research, the effectiveness of this model should be demonstrated in production. Additionally, a deeper technical specification of protocol level modelling should be defined. While a plethora of different resource type specific honeypots are available, appropriate ones should be selected. Additionally, it should be noted that the usability of sensor data is dependent on capabilities to process this data. This phase supports the comprehension of the elements which have been perceived from the cyber environment. Hence, future research topics should also include cooperation with technologies such as security information and event management (SIEM). The usability of honeypot sensor data in terms of SIEM use cases should be evaluated.

Acknowledgement

This research is partially funded by the Regional Council of Central Finland/Council of Tampere Region and European Regional Development Fund as part of the *Health Care Cyber Range (HCCR)* project of JAMK University of Applied Sciences the Institute of Information Technology.

References

1. Akbanov, M., Vassilakis, V.: Wannacry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. Journal of Telecommunications and Information Technology **1**, 113–124 (04 2019). https://doi.org/10.26636/jtit.2019.130218
2. Anagnostakis, K.G., Sidiroglou, S., Akritidis, P., Xinidis, K., Markatos, E., Keromytis, A.D.: Detecting targeted attacks using shadow honeypots. In: Proceedings of the 14th Conference on USENIX Security Symposium - Volume 14. p. 9. SSYM'05, USENIX Association, USA (2005)
3. Anwar, A.H., Kamhoua, C., Leslie, N.: Honeypot allocation over attack graphs in cyber deception games. In: 2020 International Conference on Computing, Networking and Communications (ICNC). pp. 502–506 (Feb 2020). https://doi.org/10.1109/ICNC47757.2020.9049764

4. Basnet, R., Mukherjee, S., Pagadala, V.M., Ray, I.: An efficient implementation of next generation access control for the mobile health cloud. In: 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC). pp. 131–138 (April 2018). https://doi.org/10.1109/FMEC.2018.8364055
5. Bauer, J., Goltz, J., Mundt, T., Wiedenmann, S.: Honeypots for threat intelligence in building automation systems. In: 2019 Computing, Communications and IoT Applications (ComComAp). pp. 242–246 (Oct 2019). https://doi.org/10.1109/ComComAp46287.2019.9018776
6. Bhargavi, U., Gundibail, S., Manjunath, K., Renuka, A.: Security of medical big data images using decoy technique. In: 2019 International Conference on Automation, Computational and Technology Management (ICACTM). pp. 310–314 (April 2019). https://doi.org/10.1109/ICACTM.2019.8776696
7. Davé, N.: Cyberattacks on Medical Devices Are on the Rise—and Manufacturers Must Respond. https://spectrum.ieee.org/the-human-os/biomedical/devices/cyber-attacks-on-medical-devices-are-on-the-riseand-manufacturers-must-respond (2019), accessed: 29 April 2020
8. Djanali, S., Arunanto, F.X., Pratomo, B.A., Baihaqi, A., Studiawan, H., Shiddiqi, A.M.: Aggressive web application honeypot for exposing attacker's identity. In: 2014 The 1st International Conference on Information Technology, Computer, and Electrical Engineering. pp. 212–216 (Nov 2014). https://doi.org/10.1109/ICITACEE.2014.7065744
9. Endsley, M.: Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors **37**(1), 32–64 (1995). https://doi.org/10.1518/001872095779049543
10. European Commission: Medical Devices. https://ec.europa.eu/growth/sectors/medical-devices_en (2020), accessed: 17 May 2020
11. Fadlullah, Z.M., Taleb, T., Ansari, N., Hashimoto, K., Miyake, Y., Nemoto, Y., Kato, N.: Combating against attacks on encrypted protocols. In: 2007 IEEE International Conference on Communications. pp. 1211–1216 (2007)
12. Forescout Technologies, Inc.: Putting Healthcare Security Under the Microscope. https://www.forescout.com/company/resources/forescout-healthcare-report/ (2019), accessed: 20 April 2020
13. Fraunholz, D., Zimmermann, M., Schotten, H.D.: An adaptive honeypot configuration, deployment and maintenance strategy. In: 2017 19th International Conference on Advanced Communication Technology (ICACT). pp. 53–57 (Feb 2017). https://doi.org/10.23919/ICACT.2017.7890056
14. Ihanus, J.: Expanding Cyber Situation Awareness with Honeypots in Corporate Environment. M. eng. thesis, Jyväskylä University of Applied Sciences, Finland (2019)
15. Kovanen, T., David, G., Hämäläinen, T.: Survey: Intrusion detection systems in encrypted traffic. vol. 9870, pp. 281–293 (09 2016). https://doi.org/10.1007/978-3-319-46301-8_23
16. Lihet, M., Dadarlat, V.: Honeypot in the cloud five years of data analysis. In: 2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet). pp. 1–6 (Sep 2018). https://doi.org/10.1109/ROEDUNET.2018.8514128
17. Mayorga, F., Vargas, J., Álvarez, E., Martinez, H.D.: Honeypot network configuration through cyberattack patterns. In: 2019 International Conference on Information Systems and Computer Science (INCISCOS). pp. 150–155 (Nov 2019). https://doi.org/10.1109/INCISCOS49368.2019.00032
18. van der Meulen, R.: Build Adaptive Security Architecture Into Your Organization. https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization/ (Jun 2017), accessed: 3 April 2020

19. Mokube, I., Adams, M.: Honeypots: concepts, approaches, and challenges. pp. 321–326 (01 2007). https://doi.org/10.1145/1233341.1233399
20. Myllykangas, T.: You Need to Patch the BlueKeep RDP Vulnerability (CVE-2019-0708). https://blog.f-secure.com/patch-bluekeep-rdp-vulnerability-cve-2019-0708/ (2019), accessed: 29 April 2020
21. Nagpal, B., Singh, N., Chauhan, N., Sharma, P.: Catch: Comparison and analysis of tools covering honeypots. In: 2015 International Conference on Advances in Computer Engineering and Applications. pp. 783–786 (March 2015). https://doi.org/10.1109/ICACEA.2015.7164809
22. Nelson, R., Staggers, N.: Health Informatics - E-Book: An Interprofessional Approach. Elsevier Health Sciences (2016), https://books.google.fi/books?id=eROwDQAAQBAJ
23. Palo Alto Networks, Unit 42: 2020 Unit 42 IoT Threat Report. https://unit42.paloaltonetworks.com/iot-threat-report-2020/ (2020), accessed: 3 May 2020
24. Puuska, S., Kokkonen, T., Alatalo, J., Heilimo, E.: Anomaly-based network intrusion detection using wavelets and adversarial autoencoders. In: Lanet, J.L., Toma, C. (eds.) Innovative Security Solutions for Information Technology and Communications. pp. 234–246. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-12942-2_18
25. Rogova, G.L., Ilin, R.: Reasoning and decision making under uncertainty and risk for situation management. In: 2019 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA). pp. 34–42 (2019). https://doi.org/10.1109/COGSIMA.2019.8724330
26. Sahu, A., Mao, Z., Davis, K., Goulart, A.E.: Data processing and model selection for machine learning-based network intrusion detection. In: 2020 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR). pp. 1–6 (2020)
27. Shostack, A.: Threat modeling: Designing for Security. John Wiley and Sons, Inc, BoulevardIndianapolis, IN (2014)
28. The European Union Agency for Network and Information Security (ENISA): Smart hospitals, security and resilience for smart health service and infrastructure (Nov 2016). https://doi.org/10.2824/28801
29. Tian, W., Ji, X., Liu, W., Liu, G., Zhai, J., Dai, Y., Huang., S.: Prospect theoretic study of honeypot defense against advanced persistent threats in power grid. IEEE Access pp. 1–1 (2020). https://doi.org/10.1109/ACCESS.2020.2984795
30. TrapX Labs - A Division of TrapX Security, Inc.: ANATOMY OF AN ATTACK: MEDJACK (Medical Device Hijack). https://trapx.com/trapx-labs-report-anatomy-of-attack-medical-device-hijack-medjack/ (2015), accessed: 29 April 2020
31. U.S Food and Drug Administration: MAUDE Adverse Event Report: GE HEALTHCARE MACLAB. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/Detail.CFM?MDRFOI__ID=3239402 (2013), accessed: 21 May 2020
32. U.S Food and Drug Administration: MAUDE Adverse Event Report: MERGE HEALTHCARE MERGE HEMO PROGRAMMABLE DIAGNOSTIC COMPUTER. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/detail.cfm?mdrfoi__id=5487204 (2016), accessed: 21 May 2020
33. U.S Food and Drug Administration: Postmarket Management of Cybersecurity in Medical Devices. https://www.fda.gov/media/95862/download (2016), accessed: 15 May 2020

34. U.S Food and Drug Administration: Department of health and human services, Medical Devices, Part 820, Quality System Regulation. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=820&showFR=1&subpartNode=21:8.0.1.1.12.3 (2019), accessed: 21 May 2020
35. Vectra: 2019 Spotlight Report: Healthcare's legacy infrastructure of unmanaged devices exposes a vulnerable attack surface. https://www.vectra.ai/download/spotlight-report-on-healthcare-2019#form-download (2019), accessed: 16 May 2020
36. Vetterl, A., Clayton, R.: Honware: A virtual honeypot framework for capturing cpe and iot zero days. In: 2019 APWG Symposium on Electronic Crime Research (eCrime). pp. 1–13 (Nov 2019). https://doi.org/10.1109/eCrime47957.2019.9037501
37. Wafi, H., Fiade, A., Hakiem, N., Bahaweres, R.B.: Implementation of a modern security systems honeypot honey network on wireless networks. In: 2017 International Young Engineers Forum (YEF-ECE). pp. 91–96 (May 2017). https://doi.org/10.1109/YEF-ECE.2017.7935647
38. Wang, H., Wu, B.: Sdn-based hybrid honeypot for attack capture. In: 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). pp. 1602–1606 (March 2019). https://doi.org/10.1109/ITNEC.2019.8729425
39. Xu, Y., Tran, D., Tian, Y., Alemzadeh, H.: Poster abstract: Analysis of cybersecurity vulnerabilities of interconnected medical devices. In: 2019 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE). pp. 23–24 (2019)
40. Yaqoob, T., Abbas, H., Atiquzzaman, M.: Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—a review. IEEE Communications Surveys Tutorials **21**(4), 3723–3768 (2019). https://doi.org/10.1109/COMST.2019.2914094