Medical Device Forensics

Veronica Schmitt | Noroff University

Traditionally, medical devices were built with a focus on clinical care, not security. As health care moves to Industry 4.0, practitioners need to evolve and determine what digital forensics and incident response entail when dealing with medical devices.

©SHUTTERSTOCK.COM/VEKTORJUNKIE

In 2020, the world was turned on its head. With the pandemic not showing any signs of regressing, the medical industry has had to adapt quickly to ensure that patients receive the necessary care. More than ever before, physicians needed to be able to monitor their patients while at home. This brought about what is referred to as "Health Care 4.0,"[1] derived from "Industry 4.0."

This article details how health care has moved to form part of the digital frontier. This change meant that the push for interconnected medical devices was no longer a pipe dream but had to be made a reality much faster. It became a necessity for a physician to have real-time access to patients' data.

Generally, the medical industry has not had the best track record when it comes to incorporating fast-paced changes. As we introduce these instruments into our hospital infrastructure and patients' homes, the age-old question is asked: "Can these devices be hacked?" Although this is a valid concern, it would be far better to determine the likelihood that a medical device will be hacked. The easy answer to this is probably one that every digital forensics practitioner is familiar with: "It depends." Many factors are involved—for example, how the device is connected, how the network is segmented, and the manufacturing specifications of the device.

It is often proposed that the likelihood of a medical device being hacked is not very high.[9] When one examines the threat landscape around health care, the probability starts looking much greater. In 2020, there were an alarming number of incidents in which health-care information was exposed, with 24.1 million records being disclosed in one occurence.[4] These events represent an alarming 91.2% of all breached records for that year.

Health-care data are a significant source of concern. Generally, within health care, it takes anywhere between 96 and 236 days to detect and recover from an IT breach.[9] Overall, health care has seen an increase of 25% in the frequency of breaches in the sector.[5] Hacking and IT incidents accounted for about 67% of all data breaches and 92% of all data breaches for 2020.[4] These numbers indicate that health care, as a whole, is under attack. When dealing with interconnected instruments, medical devices could potentially be a stepping-stone toward obtaining access to a hospital network or electronic health-care records.

There have been numerous hcal devices. It should be no surprise that these devices, like any other system, have flaws that could lead to a more significant compromise. According to the Center for Devices and Radiological Health,[2] security researchers identified 12 vulnerabilities, which they named *SweynTooth*. These particular vulnerabilities were associated with the wireless communication technology Bluetooth Low Energy. This communication technology allows two devices to effectively pair and perform their intended function without excessively impacting battery life. The potential attacks that could stem from this vulnerability would crash the device, stopping the communication from working and causing the device to freeze, much like a denial of service. This would leave the device unable to respond and allow researchers

Digital Object Identifier 10.1109/MSEC.2021.3127490
Date of current version: 25 January 2022

to bypass security to access functions on the device that otherwise would not be available. There are many manufacturers affected by this vulnerability.[2]

The question is whether these devices have logging capabilities to offer early detection or even allow postmortem investigations to occur. From the research and examinations I have done, this would seem not to be the case. The focus should be on early detection and mitigation for vulnerabilities like this. There have been other suggestions made in the industry relating to managing the manufacturing material and code libraries used in terms of introducing the software bill of materials, which certainly helps manufacturers be in a position to identify whether a vulnerability impacts their devices. However, this does not solve the problem of determining whether a device has been compromised by a vulnerability and exploited.[3]

When I have these conversations with patients and medical personnel, I am often asked whether the risk outweighs the benefit of these devices. There is no satisfactory answer here, except it depends on many variables. One cannot argue that medical devices stand between life and death for patients. I have had an implantable device that ensures that my heart functions as it should and does not stop. This device has added many years to my life expectancy.

The concern when dealing with medical devices has always been one of legacy. When a device is manufactured, it goes through many checks and tests to ensure that it is safe and built appropriately. It is essential to understand that security is not a functional requirement of a medical device. *Functional requirements* are defined as necessary functions of the system or its components. These are described as a specification of the behavior between the inputs and outputs. Medical devices are manufactured to last for an extended period and apply treatment to patients. On a functional level, they were not built with security in mind.

As a result, some devices were the most advanced at one point. However, as time has moved on, they have become vulnerable due to the progression of technology. Many of the more traditional medical devices cannot dynamically evolve in the way that software might. The medical device software is built on hardware that might be embedded within a patient's body and so cannot be updated. As software and firmware grow over time and become more sophisticated, they surpass the capabilities of the physical hardware. In 10 years, we will still be dealing with legacy devices, which are the biggest pitfall when it comes to traditional incident response and digital forensics.

Forensic readiness is a term that has many definitions, partially because it is relatively new. Unclear definitions lead to confusion when discussing how forensic readiness can be achieved in medical devices. There is a balance to forensic readiness, specifically, the ability to collect credible digital evidence while reducing the costs to perform digital forensics on a medical device.[8] To determine whether a medical device has forensic readiness maturity means that the digital forensics practitioner or manufacturer has to determine what information is stored on the file system.

The first step is to understand what hardware architecture is used on a particular device. Hardware is very diverse across a manufacturer. The functionality and firmware support determine its selection. Next, we should consider the file system, which is the link between the hardware and software components. It is the guiding principle for storing the data and recording the file creation, deletions, and modification. These could even apply to devices that do not have a file system but function as "bare-metal devices." These can be likened to memory-based devices, which pose many challenges to digital forensics.

Other file systems in medical devices are ones that most digital forensics practitioners are already familiar with. The file system I have encountered the most is the File Allocation Table (FAT), which has unique features that allow easier data recovery. The Extensible FAT (exFAT) is the next most common, a UNIX file system with its own rules that govern data storage.

The next area of understanding in the layers of medical devices is the operating systems; these vary across devices, manufacturers, and many other factors. One you can expect to encounter is VxWorks (https://www.windriver.com/products/vxworks), an embedded real-time operating system. You might even encounter embedded Microsoft Windows or Windows CE, which has since been deprecated. However, as previously discussed, medical devices last for many years. An investigator might encounter medical device forensics that includes the Android and iOS operating systems. These, again, have forensic artifacts a digital forensics practitioner is accustomed to. We could also encounter some operating systems that are custom versions of Linux or BusyBox (https://busybox.net/).

We then proceed to the application layer, which contains the information generated by the application itself. This area is unique to each application regarding what is created in terms of artifacts. However, how data are stored is governed by the operating and file systems. Knowing the forensics rules surrounding these components enables the digital forensics practitioner to digest the application level's information. It is critical to record the application functionality, the settings or calibration of the device, patient data, and clinical information. The data from these devices in terms of clinical and health data are often integrated with different cloud solutions at the health-care facility and connected with the electronic health-care systems.[4] The question is whether there are logs that can be ingested from medical devices into cloud solutions for log aggregation (Figure 1).

When a medical device is compromised, several things are needed to respond to and remediate the incident. The first is whether the medical device manufacturer, hospital, or patient is in a position to detect the breach. Since 2015, reports indicate that early detection in all industries has been challenging.[2] Medical devices are not manufactured with breach detection in mind. Presently, however, the landscape is changing, with medical manufacturers exploring security by design and including this as part of their operating models.

When we talk about medical device forensics, there is no clear definition in the literature. The field is made up of three main disciplines, called the *triangle approach*, as seen in Figure 2.[13] There is also a wide variety of medical devices. We explore some in more detail, as this is important to understand the problem statement. Infusion pumps make up more than half of all of the medical Internet of Things devices deployed within hospitals. They play a critical role in patient care and ensuring that the hospital controls the infusion of medicine. These pumps have given medical professionals the ability to care for patients remotely and automate some health-care delivery. This type of technology invites malicious threat actors interested in disrupting these life-sustaining advances in medicine.[5]

In January 2020, a security vulnerability was published involving certain GE Healthcare clinical information central stations and telemetry servers.[4] These devices are specifically used in health-care facilities to display information about patients, including physiological parameters, such as temperature, heartbeat, blood pressure, for monitoring. A statement made by the U.S. Food and Drug Administration says that, to date, there have been no reports of incidents related to these vulnerabilities.[4] The question that should be raised here, the same as before, is whether these devices can retain information forensically, allowing possible malicious access through this vulnerability. When explored, concerns around logging and forensic data indicate that the maturity of forensic readiness within medical devices is very low.

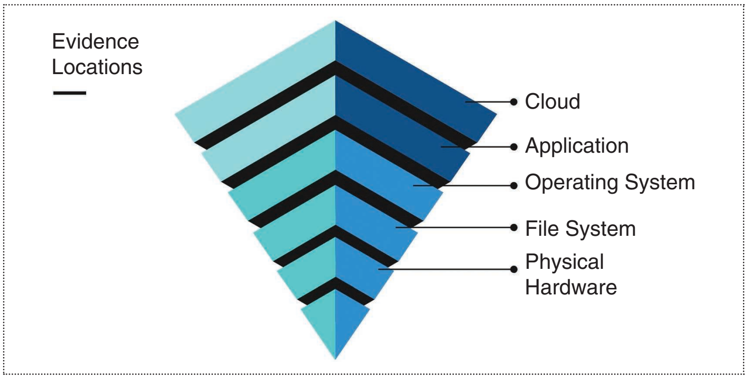

Figure 1. The medical device locations of the investigation.

Medical Device Forensics

Medical device forensics is made up of three distinct processes:

- medical device engineering
- digital forensics
- medical forensics.

These three disciplines cover the skill sets needed when looking at medical devices, which are often are composed of complex hardware, software, and data structures. Medical device engineering is the process of designing, manufacturing, and maintaining a medical device. An understanding of the hardware and operating system is needed. This process is also used extensively to examine whether a medical device functions as it should and does fault finding. It is useful when considering the process of acquiring a forensic image from a medical device, as this often requires an understanding of the hardware and constraints you might face dealing with these devices.[7]

Knowledge of device functionality can aid the digital forensics investigation by determining what condition the medical device was in during acquisition. The second part of what needs to be understood is the sequence of events on the device and whether there are any data that need to be recovered.

The discipline of digital forensics involves reconstructing events on a digital device and recovering data that may have been lost. Data recovery is the second portion of examining the forensic image that you have acquired. Recovery and reconstruction require a low-level understanding of the disk structures and file systems used to store the data on a medical device. It is important to note that a file system should not be confused with an operating system. Some medical devices, from a digital forensics point of view, look more like what we know in traditional memory forensics.

Once the sequence of events has been established, one more aspect needs to be looked at: the actual recorded medical data. Recorded medical data should be examined to reconstruct events and determine the overall medical sequence of them. This analysis requires knowledge of the medical nature of the device and patient. It is essential to understand that these devices vary in how data can be acquired, the data they store, and the medical information they record. Some devices run on bare-metal systems and are primarily memory based. The analysis of these can be time-consuming and cumbersome. They are also often implanted within a patient, making the data more complicated to acquire. With implanted devices, one cannot simply plug something in to make a forensic acquisition, as there is a person attached to the device.

Informal medical device forensics is not a new discipline; it has been done by manufacturers for years when receiving back faulty devices. They have been fault finding and determining why a device failed as part of the medical engineering portion. It is possible to analyze a medical device to provide an overall picture of its functionality, the sequence of events, and the recorded medical information.

Important to note is that most medical devices do not contain robust logging capabilities designed for incident response. I have a saying: "When nothing goes right, just go left;" this way, you build what you do not have. The landscape should change from simply hoping that medical devices will not be compromised. Instead, manufacturers must build in the detection and forensic evidence needed to prove that is the case or adequately deal with an incident. It is probably not when but whether you would even know about such an incident. That being said, medical devices save lives and extend the life expectancy of patients. It is time we focus on building forensics for future breaches.

Logging and Monitoring on Medical Devices

Logging and monitoring are critical steps in the early detection of IT incidents. Log monitoring speeds up the identification of specific exceptions; for example, when a device is not behaving expectantly, the logs can alert people to that fact. Additionally, log monitoring provides developers and support personnel with observability and visibility of the behavior of their applications. Cauchi et al.[11] state that their research examined the logs from Braun Infusomat Space pumps and found that they are split between two files. The first that they encountered was the device log, which contains comprehensive device event information. The second is the keystroke log, which records inputs. These logs are deficient in many ways.

For example, logs are often incomplete and contain anomalies.[12] Ingest logs in real time via cloud-based solutions can help detect and clean these anomalies. The key to having these logs ingested is that the logs remain time synchronized and tamper evident. This would allow for the real-time monitoring of the condition of patients and their medical devices. Nguyen et al.[12] recommend using Software Guard Extension (SGX) and the Trusted Platform Module (TPM). They propose that the logger relies on SGX, TPM, and standard encryption to facilitate secure communication. This process is used assuming that the communication channel is in a hostile environment and operating system. The article identifies options that have promise. However, the concern is how older systems can be refactored to use a cloud solution for real-time logging, given that the hardware potentially does not support this.

Building a secure cloud logger is something that should be considered for future medical device manufacturing. Medical devices generally have logs that developers design to do fault and error finding and pull statistics to understand the device's functionality. Instead, devices should contain logs with an equal balance among the system, performance, and debugging, and security logging should be considered. The balance needs to have multiple stakeholders look at the same logs and understand if the provided data suits their needs.

A developer looks at logs to determine whether something within the workflow is working as it should. A digital forensics practitioner looks at logs to rebuild events that took place across a given period. Upcoming work must ensure that legacy devices can be monitored and forensic readiness applied in some form, and medical devices should be built with future breaches in mind.

The biggest constraint in dealing with medical devices includes

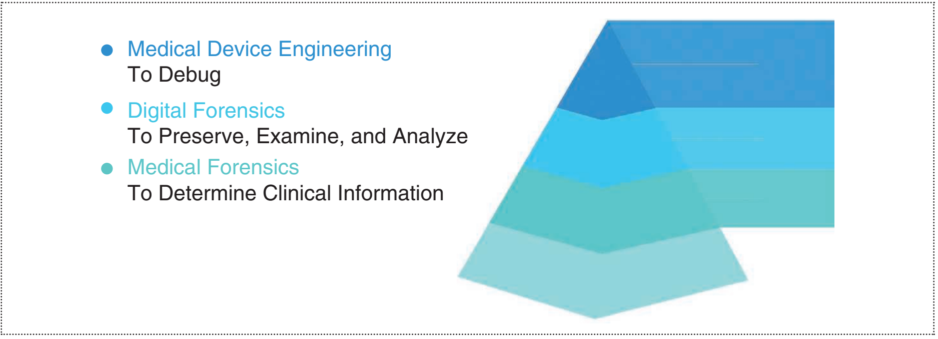
Medical Device Engineering
To Debug
Digital Forensics
To Preserve, Examine, and Analyze
Medical Forensics
To Determine Clinical Information

Figure 2. The medical device forensics triangle.

legacy systems, which have been an ever-growing problem in the medical device world. This means that a digital forensics practitioner investigating medical devices should be versed in older systems. These devices are not forensically ready; they do not have the hardware build, sufficient logging, or necessary artifacts to conduct incident response or perform digital forensics adequately.

We have the opportunity to influence how companies build future devices by building forensic readiness within the manufacturing phase. However, it also means that there are potentially legacy devices that cannot support a costly upgrade to make significant changes in terms of forensic readiness. There needs to be a layered approach to device usage within a hospital network and its protection. The future of more secure and better forensics-ready medical devices rests in the hands of those building them. More research is needed in unpacking the forensic needs to better reconstruct information on a medical device. ■

Acknowledgments

I would like to thank Prof. Barry Irwin from Noroff University, who has been instrumental in supporting my writing and research; Emlyn Butterfield from Noroff University for the support and editing that have gone into the article and being a sounding board for the digital forensics component; and the Biohack Village at DEF CON, especially Janine Medina, for the late-night conversation about how we can get better manufactured medical devices. Then, there are others—you know who you are—who have given me the support to explore my ideas. Last but not least, I would like to thank William Hagestad for his continuous support and many interesting conversations as well as Kyle Erickson for his support and knowledge.

References

1. P. P. Jayaraman, A. R. M. Forkan, A. Morshed, P. D. Haghighi, and Y.-B. Kang, "Healthcare 4.0: A review of frontiers in digital health," *Wiley Interdisciplinary Rev., Data Mining Knowl. Discovery*, vol. 10, no. 2, p. e1350, 2019, doi: 10.1002/widm.1350.
2. "SweynTooth cybersecurity vulnerabilities may affect certain medical devices: FDA safety communication," U.S. Food and Drug Administration. https://www.fda.gov/medical-devices/safety-communications/sweyntooth-cybersecurity-vulnerabilities-may-affect-certain-medical-devices-fda-safety-communication (accessed Jun. 24, 2021).
3. S. Carmody *et al.*, "Building resilient medical technology supply chains with a software bill of materials," *npj Digit. Med.*, vol. 4, p. 34, Feb. 23, 2021, doi: 10.1038/s41746-021-00403-w.
4. J. Johnson, "Percentage of U.S. healthcare data breaches caused by hacking from 2014 to 2020," Statista, Feb. 12, 2021. [Online]. Available: https://www.statista.com/statistics/972228/health-data-breaches-caused-by-hacking-us/ (accessed Jun. 24, 2021).
5. F. Langston, "Top 6 hackable medical IoT devices," Critical Insight. https://www.criticalinsight.com/resources/news/article/top-6-hackable-medical-iot-devices (accessed Jun. 24, 2021).
6. "Cybersecurity vulnerabilities in certain GE healthcare clinical information central stations and telemetry servers: Safety communication," U.S. Food and Drug Administration. https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-certain-ge-healthcare-clinical-information-central-stations-and (accessed Jun. 24, 2021).
7. F. E. Block, "The role of forensic engineering investigations in medical device reports," *J. Clin. Eng.*, vol. 42, no. 2, pp. 85–88, doi: 10.1097/JCE.0000000000000208.
8. A. Kyaw, B. Cusack, and R. Lutui, "Digital forensic readiness in wireless medical systems," in *Proc. 2019 29th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, pp. 1–6, doi: 10.1109/ITNAC46935.2019.9078005.
9. "Resources for retail delivery leaders," Convey. https://www.getconvey.com/resource/medical-devicex-statistics/ (accessed Jun. 24, 2021).
10. R. Irimia and M. Gottschling, "Taxonomic revision of Rochefortia Sw. (*Ehretiaceae, Boraginales*)," *Biodiversity Data J.*, vol. 4, p. e7720, Jun. 2016, doi: 10.3897/BDJ.4.e7720.
11. A. Cauchi, H. Thimbleby, P. Oladimeji, and M. Harrison, "Using medical device logs for improving medical device design," in *Proc. 2013 IEEE Int. Conf. Healthcare Inform.*, pp. 56–65, doi: 10.1109/ICHI.2013.14.
12. H. Nguyen *et al.*, "Cloud-based secure logger for medical devices," in *Proc. 2016 IEEE 1st Int. Conf. Connected Health, Appl., Syst. Eng. Technol. (CHASE)*, pp. 89–94, doi: 10.1109/CHASE.2016.48.
13. N. Ellouze, S. Rekhis, N. Boudriga, and M. Allouche, "Cardiac implantable medical devices forensics: Postmortem analysis of lethal attacks scenarios," *Digit. Investigation*, vol. 21, pp. 11–30, Jun. 2017, doi: 10.1016/j.diin.2016.12.001.

Veronica Schmitt is an assistant professor at Noroff University, Oslo, 4645, Norway. Her research interests include security vulnerabilities in medical devices forming part of the Internet of Things and how these could be exploited by malicious attackers as well as what types of forensic artifacts could be identified from any attacks. Schmitt received an M.S. degree in information security with a specialization in the forensic analysis of malware from Rhodes University. She is involved in DEF CON and various conferences and has spoken on this topic.