A Matter of Life and Death: Analyzing the Security of Healthcare Networks

Guillaume Dupont, Daniel Santos, Elisa Costante, Jerry Den Hartog, Sandro Etalle

A Matter of Life and Death: Analyzing the Security of Healthcare Networks

Guillaume Dupont[1], Daniel Ricardo dos Santos[2], Elisa Costante[2], Jerry den Hartog[1], and Sandro Etalle[1] *

[1]Eindhoven University of Technology, [2]Forescout Technologies

Abstract. Healthcare Delivery Organizations (HDOs) are complex institutions where a broad range of devices are interconnected. This interconnectivity brings security concerns and we are observing an increase in the number and sophistication of cyberattacks on hospitals. In this paper, we explore the current status of network security in HDOs and identify security gaps via a literature study and two observational studies. We first use the literature study to derive a typical network architecture and the threats relevant to HDOs. Then we analyze in the first observational study data from 67 HDOs to highlight the challenges they face with regards to device security and management. The second study leverages the network traffic from 5 HDOs in order to point out a number of concrete observations which depict how patient data can be exposed and how cyber-physical attacks could impact patient health. Finally we offer in this paper a starting point for securing HDOs' network.

Keywords: Healthcare · Network security · Medical devices

1 Introduction

Healthcare Delivery Organizations (HDOs), such as hospitals and clinics, are complex institutions where a broad range of Information Technology (IT), Operational Technology (OT), and Internet of Things (IoT) devices are increasingly interconnected [28]. IT devices and enterprise systems process and exchange highly sensitive data (e.g., patients' health records and financial information), whereas OT and IoT devices are used for diverse functions such as building automation, and guest entertainment. Specialized IoT devices, refers to as Internet of Medical Things (IoMT) [11], are connected medical devices supporting clinical care and can generate and exchange patient data with other devices, such as Electronic Health Records (EHR) systems [20]. These new technologies and increased connectivity can help improve the efficiency and quality of care.

However, this reliance on such technologies can also introduce new privacy and security risks [16,1]. We are witnessing an increase in the number and sophistication of cyberattacks on hospitals [14]. So far, these attacks are mainly

* This work was supported by ECSEL joint undertaking SECREDAS (783119-2), EU-H2020-SAFECARE (no. 787002) and SunRISE (PENT181005).

in the form of ransomware [21], targeting mostly the IT part of the network. But the increased connectivity is not restricted to the IT systems as it also applies to the OT systems. Does this raise security and compliance risks for HDOs that have not been (sufficiently) considered so far?

Targeted attacks against life-supporting devices may have devastating consequences for patients and HDOs. Attacks already seen in different domains like Building Automation Systems (BAS) [32,27] show that OT may be targeted. Specialized tools (e.g., Shodan) for finding exposed OT devices and potential exploits can aid attackers in launching such attacks. All of this makes it essential to be prepared for attacks that exploit the complexity of HDO ecosystems.

Security assessment for IT infrastructures is a well covered topic [24], and work like [17] looks at the human factor in HDOs. Here we aim to establish the current technical state of readiness of HDOs with respect to cyberattacks targeting their networks and aiming at, for example, stealing or altering patients' data or even harming their health.

To achieve this aim, we address the following Research Questions (RQs):

RQ1 How is an HDO's network organized?
RQ2 What are some potential threats to an HDO's network?
RQ3 What kinds of devices and software are present in an HDO's network?
RQ4 What security vulnerabilities are linked to HDO's network protocols?

We answer RQ1 and RQ2 by investigating existing literature to give an overview of the network architecture and examples of threats on typical HDOs (Section 2). To answer RQ3, we conduct a large-scale investigation of 67 HDO networks (Section 3). To answer RQ4, we perform a network security assessment of 5 of these HDO networks (Section 4). Finally, we conclude the paper with a discussion on the results, a description of related work and an outlook on future research (Section 5). Our key findings are:

1. **HDO networks are very diverse**: the diversity of connected medical devices, including different vendors and operating systems, make it increasingly difficult to secure networks.
2. **Common services and legacy operating systems leave the network vulnerable**: Certain devices found in HDOs are not only running network services often exploited by malware and malicious actors (e.g., SMB and RDP) but also legacy operating systems no longer supported by vendors, thus providing potential access to attackers.
3. **Insecure protocols and communications are common**: these flaws in network security in healthcare organizations can expose sensitive data and create the potential to harm patients by tampering with the network communication of connected medical devices.

2 Network model and threats

In this section we conduct a literature study to answer the first and a second research questions, namely "How is an HDO's network organized?" (RQ1) and "What are some potential threats to an HDO's network?" (RQ2). We address RQ1

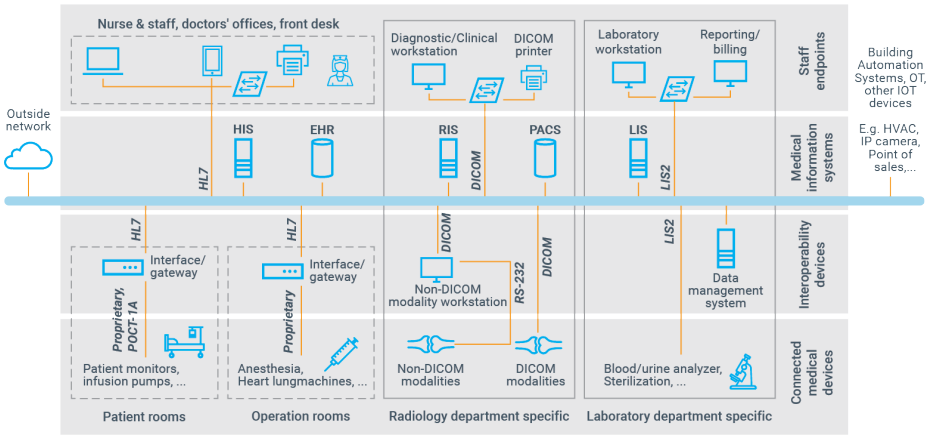

Fig. 1. Simplified network architecture of a typical HDO

by providing a network model of a typical HDO and RQ2 by listing examples of threats to HDOs. In addition we validate the attacks in a laboratory setting.

Organization of HDO's network

The major distinction between HDO networks and typical enterprise networks comes from (i) the type of devices deployed and (ii) the communication protocols used, both of which are described below.

Network devices. HDOs are generally divided into several departments, delivering specific clinical care (e.g., radiology) or organizational services (e.g., administration). We represent on Figure 1 a simplified model of typical HDO networks, including two departments in the plain-line boxes, as well as some of the IT, OT, and IoMT devices commonly found. While some departments can have specialized equipment related to their operations (e.g., imaging modalities in radiology department), there also are certain devices that can be found in multiple departments. In addition, there are systems that can be found ubiquitously across an HDO such as IT devices, as depicted in the upper left side of the figure.

We classify HDO's networked devices into 4 categories. The *connected medical devices* support clinical care, while *interoperability devices* assure communication for some devices on the network. Then *medical information systems* store and manage clinical data and finally *staff endpoints* provide human interfaces to information systems. *Connected medical devices* can be further divided into active or passive devices [15]. Active medical devices are meant to deliver medical treatment and sustain patient life (e.g., drug pumps). Passive devices monitor patient information such as vital signs or test results, and report events or need for treatment to clinical staff (e.g., patient monitors and laboratory equipment).

Depending on the network protocol used by the aforementioned devices, they may be connected to *interoperability devices*, which will convert network data into an interoperable format, allowing it to be further processed and/or stored

by *medical information systems*. Such systems can be seen as the backbone of an HDO, as they collect, store and manage various types of healthcare data. For example, health, radiology, and laboratory information systems (respectively HIS, RIS and LIS), will manage electronic medical records, radiology pictures from imaging modalities and laboratory analysis results, respectively. Finally, HDOs also have other types of devices represented together under Building Automation Systems, OT and other IoT devices.

Communication protocols. Medical devices in HDOs transmit data using standard or proprietary protocols. Table 1 summarizes the most important medical protocols we identified during our research. Depending on the protocol, specific information about the device can be found in packets' payload such as the firmware version and hardware version for that device.

HL7v2 is the most widely used interoperability and data exchange protocol in medical networks. This messaging standard allows the exchange of patient, clinical and administrative information. DICOM defines both the format for storing medical images and the communication protocols used to exchange them. As de-facto standard, it is implemented by all major vendors of devices involved in medical imaging processes (e.g., modalities and diagnostic workstations). POCT1-A and LIS2-A2 are used for point-of-care and laboratory devices, respectively. These protocols can issue test orders with patient information and transfer the results of tests to a Data Management System (DMS). The proprietary protocols Philips Data Export [29] and GE RWHAT [23] are used to control patient monitors of their respective vendors. They allow patient monitors to communicate the vital readings of patients to a central monitoring system.

While supporting critical operations in HDOs, these medical protocols support neither encryption nor authentication (or support them without enforcing their usage, in the case of DICOM), a situation similar to what is found in other cyber-physical systems, e.g., Industrial Control Systems (ICS) [4] and Building Automation Systems (BAS) [5]. We also identified other protocols such as HL7 FHIR, as well as other proprietary protocols. However we choose to ignore them in this paper as they are not as widely deployed as the ones in Table 1.

Potential threats to an HDO's network

Malicious actors may have various motivations to attack HDOs [14,15]. All reported attacks on HDOs (see, e.g., [36,8,37]) seem to have been motivated by

Table 1. Main medical protocols identified

Protocol	Type	Devices
DICOM	Standard	Imaging modalities, PACS
HL7v2	Standard	Connected Medical Devices, Medical Information Systems, Interoperability Gateways
POCT1-A	Standard	Point of Care Testing
LIS2-A2	Standard	Laboratory devices
Data Export	Prop. (Philips)	Patient monitors
RWHAT	Prop. (GE)	Patient monitors

financial gains directly via ransomware and cryptomining, or indirectly via stolen information and use of infected computers in botnets.

However in the light of the security research done on medical devices and their protocols [25,23,31,30,42,6,13,3], one can wonder how an attacker could leverage vulnerabilities on such devices. We provide below some examples of attacks, considering an attacker on the network. Such foothold can be established in various ways [14]. These attacks can be the final step in a multi-step attack [15].

Attack examples. Security research in healthcare focuses either on devices or network protocols. Vulnerabilities in specific medical devices have been found over the past years (see, e.g., [12,31,30]), and the number of security advisories in the medical space has been growing [42,39]. Currently, there is a trend of research into protocol insecurity [7,10]. Vulnerabilities of the protocols below have been demonstrated.

HL7 standards, which are used to exchange patient data between systems, can be abused in several ways and are often insecurely implemented [6,13,3]. As HL7 data is sent over unauthenticated communications, attackers can intercept and modify information in transit, which may lead to life threatening consequences.

Similarly, unauthenticated and unencrypted DICOM communications also allow attackers to tamper with medical images, misleading medical staff to wrong diagnostics. The DICOM standard supports user authentication and message encryption, however while their implementations and usage are left to product vendors and HDOs, we observe in a number of HDOs that these security mechanisms are not implemented. To demonstrate the possible consequences of this situation, researchers implemented a proof-of-concept to add or remove tumors from CT scan images being transferred over the network, leading to dramatic consequences for patients [25].

Proprietary protocols have also caught the attention of security researchers, who have shown [23] how one could intercept a patient's vital signs sent by a GE patient monitor over their RWHAT protocol. Once intercepted, a malicious actor could modify the patient signs arbitrarily. In the same fashion, we reproduced in our lab a similar attack with a Philips patient monitor. Such monitors send information over the Data Export protocol, which can be intercepted, decoded and modified on the fly.

Attacks against unprotected protocols such as POCT1-A and LIS2-A2 have not yet been demonstrated but can follow the same procedure. In Table 2, we summarize seven example attacks against these protocols.

3 Large-scale Study

In this section we answer the third research question, "What kinds of devices and software are present in an HDO's network?" To this end we leverage data from various HDOs, providing us insights into the devices connected on their networks. We present the charts resulting from our analysis, alongside our conclusions.

Methodology We collected data in 67 HDOs, consisting in traffic gathered and analysed by network monitoring appliances connected to network switches in

Table 2. Potential attacks on the main medical protocols identified

ID	Protocol	Target	Attack	Description
A1	HL7v2	Patient data	Data theft	An attacker can retrieve sensitive patient data such as clinical and financial information as the data is sent unencrypted
A2	HL7v2	Patient health	Tamper with EHR	An attacker can modify arbitrarily the electronic health records of patients (e.g., change the allergies or medication prescription)
A3	DICOM	Patient health	Tamper with test results	An attacker can tamper with medical images by virtually adding or removing tumors for respectively healthy or sick patients
A4	POCT1-A	Patient health	Tamper with test results	An attacker can change the results of point of care equipment (e.g., blood glucose analysis)
A5	LIS2-A2	Patient health	Tamper with test results	An attacker can modify the test results of laboratory equipment (e.g., blood analysis)
A6	Data Export	Patient health	Tamper with vitals	An attacker can tamper with patients' vital signs read by Philips patient monitors
A7	RWHAT	Patient health	Tamper with vitals	An attacker can tamper with patients' vital signs read by GE patient monitors

each HDO. The appliances collect data both by passively listening and actively interacting with the devices on the network (e.g., using Nmap and other network scanning tools). The data is then analyzed by the appliance to find *attributes* of devices (e.g., MAC address or operating system).

Some of these attributes, called *raw attributes*, can be directly obtained from the network traffic, like the MAC address. Other attributes we refer to as *Classified attributes* are obtained by classifying devices using a *Device Profile Library*. It is a set of rules which assign a profile to a device once a given combination of raw attributes have been detected for that device. A profile is a triple of attributes (*vendor, OS, function*), where the first two elements are self-explanatory and the third element represents the function of a device in the network (e.g., 'OT/Healthcare/X-ray machine' or 'IT/Printer'). The classification of devices is not the focus of this work and we assume that the Device Profile Library is correct. We comment on that assumption in Section 5. The data is anonymized and sent to a data lake which aggregates the data collected in all HDOs. We further analyze the data retrieved by executing a number of queries.

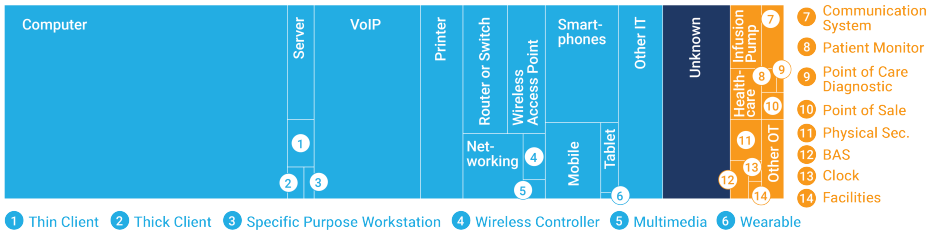

Fig. 2. Average distribution of IT and OT Devices found on HDOs' networks

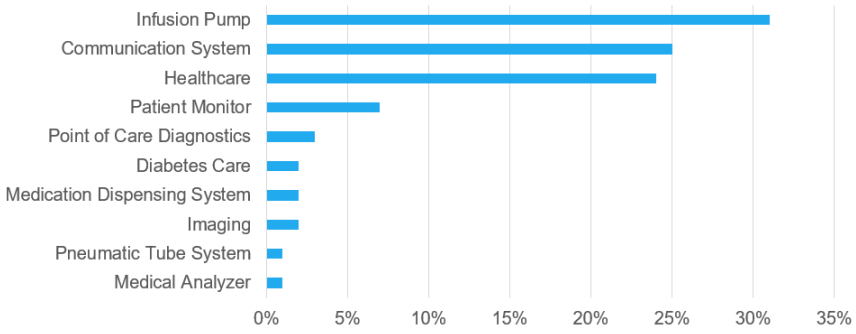

Fig. 3. Top-10 connected medical devices on HDO networks

Sample description The dataset comprises a total of 2.3 million devices. The amount of unique devices per HDO, regardless of their type, ranges from 597 to 234305 with an average of 50078 and a median value of 12766. We see a wide range of sizes across the sample, but most are in the thousands to tens of thousands of devices. To help better understand the composition of HDO networks we provide below different perspectives through our data analysis.

High-level device overview Figure 2 represents the three main classes of device found in HDOs, namely IT, OT and unknown devices. On average, these classes correspond to respectively 84%, 7% and 9% of the total number of devices. *IT devices* include personal computers, VoIP devices, network printers, mobile devices, and various networking equipment among other things. *OT devices* are comprised of not only healthcare devices and infusion pumps, but also BAS devices, points of sale, physical security and other facilities-related devices such as IP security cameras. Finally, the devices that were not possible to be classified are referred to as *unknown devices*.

Figure 2 also shows the average distribution of device types in HDOs. One can observe that more than roughly a third of the connected devices are computers (36.4%), followed by VoIP devices (13.8%) and smartphones (5.7%). Understanding the distribution of devices is important because many networks still operate in organizational silos, where different departments are responsible for different sections of the network. This situation tend to leave gaps in security [22].

Types of medical devices Since connected medical devices are especially critical for HDOs, it is important to understand the distribution of these devices in a finer granularity. Figure 3 shows the most common types of connected medical devices. Per-patient devices, such as infusion pumps and patient monitors represent the majority of healthcare devices on HDO networks, as well as per-personnel devices like communication systems. This makes sense as they are the devices deployed mostly on a 1:1 ratio. Devices such as those used in laboratory diagnostics or medical imaging represent a smaller number because they are shared devices. The "healthcare" device type on Figure 3 refers to medical devices that cannot be further categorized into a more specific type.

Diversity of vendors and operating systems We now look at the diversity of the device ecosystem in HDOs in terms of vendors and Operating Systems (OS). Our analysis shows that on average, HDOs have a total of 152 different device vendors. When looking at the number of unique vendors for specific device types in HDOs, we observe for example that IT computers have on average 51.5 unique vendors and networking and VoIP equipment have respectively 25.5 and 7.2 unique vendors. Regarding medical devices, infusion pumps, patient monitors and point of care diagnostics devices have respectively 2.5, 2.2 and 2.6 unique vendors on average.

The complexity of device management is linked to the number of unique vendors whose devices are deployed on a network. Vendors have different support, maintenance, and patching programs, which can affect the time between the disclosure of a vulnerability and the patching of the related systems. As an example, consider the recently disclosed set of vulnerabilities on the IP stack of the VxWorks real-time OS [34]. Some medical devices run this particular OS, but it is not immediately clear to the users whether a particular device is affected, if there is a patch available and how it can be applied. Contacting each vendor for inquiry would be very time consuming.

Additionally, it is important to consider the diversity in OS as it can bring some security concerns as well. Figure 4 shows the OS variants of devices on HDO networks. For each OS, its proportion relative to the others is given and, for some of them, a breakdown of the version in use. Windows is the most common OS across HDO's devices (41%). Windows 7, 10 and Windows Server 2012 represent respectively 11%, 8% and 1% of the OS, while we still observe a non-negligible amount of other variants such as Windows XP, Windows Server 2008 and 2003.

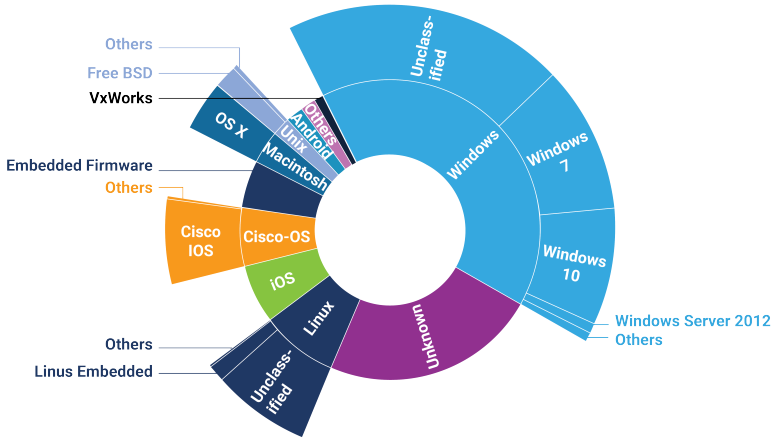

Fig. 4. Distribution of OS variants in devices on HDO networks

Our analysis revealed that 40% of networks have more than 20 different OS. We see that 0.4% of devices are running an unsupported version of Windows and

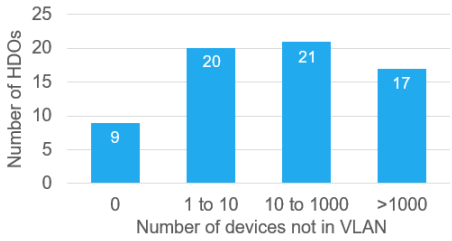

Fig. 5. Occurrences of HDOs with devices not in VLAN

70% of devices a version of Windows for which Microsoft support is planned to expire by January 14, 2020[1], such as Windows 7, Windows 2008 and Windows Mobile. Running unsupported OS is a well known security issue. HDOs' networks will most likely continue to have medical devices running legacy OS since updating can be too costly or even infeasible, due to unacceptable downtime required or (software) compatibility issues. Consequently many devices would have to keep operating while remaining potentially vulnerable. This situation calls for additional protections, such as appropriate segmentation of systems, which can be achieved through Virtual Local Area Networks (VLAN) for example.

VLAN analysis Network segmentation is a commonly advised security measure [24]. VLANs can segment the network by effectively isolating critical systems, segregating similar devices by function, and limit access to data and other assets in a segment. In this context, isolating medical devices in VLANs could help to keep them separated from the rest of the network. However, our study shows that, on average less than 20% of the medical devices are deployed in a VLAN and, as Figure 5 shows, 86.5% of the HDOs have medical devices outside of VLANs.

In addition we also found that 61 of these HDOs have at least one VLAN with a combination of medical devices and other OT devices, thus undermining the segmentation that use of a VLAN may provide. Examples of such cases that we saw in the data are VLANs containing both medical imaging modalities and IP cameras or HVAC systems, or even blood glucose monitors with points of sale.

This observation confirms the statement of the ISE regarding HDO's network being improperly segmented [15].

Enabled common services Some common network services are often targeted by recent malware and malicious actors [26]. Table 3 shows the amount of devices that have the given service's port open. Server Message Block Protocol (SMB) is the transport protocol used by Windows machines for a variety of purposes such as file sharing and access to remote Windows services. WannaCry and NotPetya are two examples of ransomware that exploit vulnerabilities in SMB. Remote Desktop Protocol (RDP) is another common protocol exploited by modern automated threats. Secure Shell (SSH) may be abused by brute-force attacks to log remotely onto machines. Telnet and File Transfer Protocol (FTP) are often-exploited vectors: these protocols do not secure nor encrypt network sessions.

[1] `https://bit.ly/38e9QXc`

Overall, after analyzing the kinds of devices and software present in an HDO's network, we can conclude that a large number of devices on HDO networks have high-risk services turned on. The access requirements of medical vendors and outsourced suppliers often require devices to have services like RDP enabled. Other times, the network ports are left open by default without the knowledge of IT and security staff. In the next section we look closer at HDO networks to better understand the security vulnerabilities linked to network protocols.

4 In-Depth Study

The in-depth study described in this section aims at answering our fourth research question, "What security vulnerabilities are linked to HDO's network protocols?" We analyze network traffic of HDOs in order to provide a detailed view on their network security posture, identify insecure protocols and susceptibility to attacks.

Methodology We captured raw network traffic and perform various analyses, looking at network activities and communication protocols among other things. Collecting all network data from all HDOs is clearly not feasible. Instead, the study leverages datasets from five HDOs captured at key locations in their network. These HDOs are referred to as HDO_{1-5}.

The network traffic is analyzed using Forescout's SilentDefense[2] solution, enhanced with our *Protocol Dissectors* for the key medical protocols presented earlier in Table 1. For each of those protocols, we created a dissector which allows us to identify its presence in traffic and parse the contents of network packets.

Sample description The datasets used in this study correspond to raw network traffic of five different HDOs. For HDO_1 and HDO_2 the data was captured over a period of 2 days and it comprises a total of respectively 2207 and 1513 devices. For HDO_3 the capture lasted one day and it collected data from 12289 devices. Finally for HDO_4 and HDO_5 the captures ran over four days and account for 11051 and 4423 devices respectively.

Overview and network activities In the datasets, we found the healthcare network protocols presented on the left side of Table 4. Recall that these protocols are used by diverse device types in HDOs as described previously in Section 2.

The presence of these protocols indicates that these HDOs are susceptible to some of the attacks described in Section 2. We propose in Table 2 a list of attacks leveraging these protocols' weaknesses that an attacker could execute

[2] `https://www.forescout.com/platform/silentdefense/`

Table 3. Common enabled network services

Network service (port number)	Devices (%)	Devices (absolute)
SMB (445)	26%	573,455
RDP (3389)	14%	318,634
SSH (22)	8%	187,135
Telnet (23)	5%	113,071
FTP (21)	5%	107,719

once having access to the HDO's network. As one can see in Table 4, all five HDOs in our analysis are susceptible to be vulnerable to at least two attacks on medical device protocols. We also found obsolete versions of other protocols such as SNMPv1 and v2 and NTPv1 and v2. We do not elaborate on those findings because they do not fit the attack examples that we defined in Section 2.

Weak encryption As presented on the right side of Table 4, we found that SSLv3, TLSv1.0 and TLSv1.1 are still used. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols used to secure network communications of higher-level protocols, such as HTTPS or FTPS. SSLv3, TLSv1.0/1.1 are known to be insecure. They are impacted, for instance, by the POODLE and BEAST attacks [35], in which an attacker can downgrade a connection and decrypt the traffic. Our analysis shows that these weak protocols are used internally in HDOs, where one could still argue that other additional security measures could compensate. However, they are also used externally, even to connect to organizations such as Microsoft and Google.

Additionally, our analysis revealed issues with the SSL/TLS certificates used in HDOs. Such certificates play a critical role in authentication and data encryption. We found that all HDOs use certificates with non-whitelisted issuers. For security purposes, it is usually recommended to only use certificates delivered by trusted issuers (i.e., whitelisted issuers). Also two of the HDOs displayed are still using expired certificates, both for healthcare applications and network equipment.

External interfaces and communication As discussed, HDO networks are complex and use many different protocols, including ones dedicated to healthcare. For operational reasons, some medical applications can be reached from the outside of the network, sometimes using healthcare protocols. This adds to the complexity of managing such systems and increases the probability of sensitive information or systems being exposed. For example we found in one HDO a system containing an EHR application exposed on the public Internet.

In addition, in all HDOs except for HDO_2, we observed communications between public and private IP addresses using HL7v2. As these communications are unencrypted, they can be easily read, and leak sensitive patient information such as names and addresses, employment status, phone number, allergies and

Table 4. Findings of network traffic analyses in five HDOs

	Healthcare protocols						Susceptible to attacks							Weak protocols			Certificates	
Dataset	HL7v2	DICOM	POCT1-A	LIS2-A2	Data Export	RWHAT	A1	A2	A3	A4	A5	A6	A7	SSLv3	TLSv1.0	TLSv1.1	Issuer not whitelisted	Expired
HDO_1	✓	✓				✓	✓	✓	✓				✓		✓	✓	✓	
HDO_2		✓			✓				✓			✓			✓		✓	
HDO_3	✓	✓		✓			✓	✓	✓		✓			✓	✓		✓	✓
HDO_4	✓	✓	✓				✓	✓	✓	✓				✓	✓	✓	✓	✓
HDO_5	✓	✓		✓			✓	✓	✓		✓				✓	✓	✓	

also test results. Other information regarding the care provider can also be found such as the doctor's name in charge of the patient, with his or her license number.

Moreover, there were also in two HDOs medical devices communicating over non-medical protocols with external servers. For example, a medical information system was seen to communicate over SSH, and another to reach a web server over HTTP. In one instance, a communication with an external file server over FTP was observed, and we confirmed (using Shodan) that this external machine contains up to 25 vulnerabilities. If exploited, it could potentially lead to the compromise of such a server and create an entry point into the HDO's network.

Additionally, we also observed in an HDO a machine behaving suspiciously. In our sample, this computer was trying to reach a number of public IP addresses over various ports. We noted a number of port scans executed and other host discovery attempts. Finally, it was communicating internally with 11 other machines over Telnet. These signs of compromise require further investigation, and we are validating our hypothesis with the network's owners.

Firmware Versions and Vulnerabilities Certain firmware are known to be vulnerable, as reported in *ICS Medical Advisories* [39]. To determine whether HDOs have medical devices running known vulnerable firmware, we employ the protocol dissectors we developed (see Section 2). We find that in HDO_2 Philips IntelliVue patient monitors deployed in intensive care units have a firmware which could potentially be abused. If successfully exploited, the vulnerabilities could allow an attacker to read and write the memory of the device, and force it to restart, potentially leading to delays in diagnosis and treatment of patients[3].

In HDO_4, we find vulnerable Roche Accu-Chek Inform II blood glucose meters. This model, popular and commonly found in HDOs, presents multiple vulnerabilities in which attackers could execute arbitrary code on the device by crafting POCT1-A packets and change the instrument configuration. This could lead to false analysis results and inaccurate diagnosis[4].

5 Conclusion

We explore the technical state of readiness of HDOs through studies across 67 organizations. The key findings, given in Section 1 indicate gaps such as insecure protocols, weak encryption, and private-to-public network communications which can directly expose patient data to attackers. Filling these gaps is challenging: HDOs are large diverse ecosystems of devices, including legacy and safety critical systems, processing sensitive data. They are also difficult to manage and secure because they comprise a variety of software, vendors, and protocols. Solutions that address the combination of these characteristics will be needed.

Related work Most work on cybersecurity in healthcare focuses on connected medical devices (e.g. [18,38,41,2]), with special attention on implantable devices because of their potential direct harm to patients [33]. These works mostly

[3] `https://bit.ly/2E8wCC2` and `https://bit.ly/2YFCwnE`

[4] `https://www.us-cert.gov/ics/advisories/ICSMA-18-310-01`

ignore other kinds of devices present in an HDO's network and that can be used during cyberattacks. Some works discuss the security threats not only to medical devices, but also to medical data (see, e.g., [19]). Jaigirdar et al. [16] analyzed the trust that physician's place in secure end-to-end communication of healthcare data. Kune et al. [9] surveyed medical and non-medical protocols used in HDOs and analyzed their security properties. Wood et al. [40] introduced a method to capture network traffic from medical IoT devices and automatically detect cleartext information that may reveal sensitive medical conditions.

Limitations and future work We were not in control of the traffic captured in the HDOs and the location of the appliances has an impact on the traffic they see. Device classification is based on a set of heuristics that is continually improved, but which can contain errors (see Section 3). We plan to work on improving the device classification heuristics and vulnerability matching for medical devices.

References

1. Alsubaei, F., Abuhussein, A., Shiva, S.: Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. In: LCN (2017)
2. Altawy, R., Youssef, A.: Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices. IEEE Access **4**, 959–979 (2016)
3. Bland, M., Dameff, C., Tully, J.: Pestilential Protocol: How Unsecure HL-7 Messages Threaten Patient Lives (2018)
4. Bodungen, C., Singer, B., Shbeeb, A., Wilhoit, K., Hilt, S.: Hacking Exposed Industrial Control Systems. McGraw-Hill (2016)
5. Ciholas, P., Lennie, A., Sadigova, P., Such, J.: The Security of Smart Buildings: a Systematic Literature Review. arXiv e-prints (2019)
6. Duggal, A.: Understanding HL7 2.X Standards, Pen Testing, and Defending HL7 2.X Messages. Black Hat US 2016 - `https://youtu.be/MR7cH44fjrc` (2016)
7. Fiebig, T., Lichtblau, F., Streibelt, F., Krueger, T., Lexis, P., Bush, R., Feldmann, A.: SoK: An Analysis of Protocol Design: Avoiding Traps for Implementation and Deployment. arXiv e-prints (2016)
8. FireEye: Double Dragon. `https://bit.ly/38nj6bU` (2019)
9. Foo Kune, D., Venkatasubramanian, K., Vasserman, E., Lee, I., Kim, Y.: Toward a Safe Integrated Clinical Environment: A Communication Security Perspective. In: MedCOMM (2012)
10. Forshaw, J.: Attacking Network Protocols. No Starch Press (2017)
11. Gatouillat, A., Badr, Y., Massot, B., Sejdic, E.: Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine. IEEE IoT Journal **5**(5), 3810–3822 (2018)
12. Hanna, S., Rolles, R., Molina-Markham, A., Poosankam, P., Fu, K., Song, D.: Take Two Software Updates and See Me in the Morning: The Case for Software Security Evaluations of Medical Devices. In: HealthSec (2011)
13. Haselhorst, D.: HL7 Data Interfaces in Medical Environments: Attacking and Defending the Achille's Heel of Healthcare. Tech. rep., SANS (2017)
14. HIMSS: 2019 HIMSS Cybersecurity Survey. Tech. rep. (2019)
15. ISE: Securing Hospitals: A Research Study and Blueprint. Tech. rep. (2016)
16. Jaigirdar, F., Rudolph, C., Bain, C.: Can I Trust the Data I See?: A Physician's Concern on Medical Data in IoT Health Architectures. In: ACSW (2019)

17. Koppel, R., Smith, S.W., Blythe, J., Kothari, V.H.: Workarounds to computer access in healthcare organizations: you want my password or a dead patient? ITCH **15**(4), 215–220 (2015)
18. Kramer, D., Baker, M., Ransford, B., Molina-Markham, A., Stewart, Q., Fu, K.: Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. PLoS ONE **7**(7) (2012)
19. Kumar, C.: New Dangers In the New World: Cyber Attacks in the Healthcare Industry. Intersect **10**(3) (2017)
20. Lee, I., Sokolsky, O., Chen, S., Hatcliff, J., Jee, E., Kim, B., King, A., Mullen-Fortino, M., Park, S., Roederer, A.: Challenges and Research Directions in Medical Cyber–Physical Systems. Proc. of the IEEE **100**(1), 75–90 (2011)
21. Mansfield-Devine, S.: Ransomware: Taking Businesses Hostage. Network Security (2016)
22. McAdams, A.: Security and Risk Management: A Fundamental Business Issue. Information Management **38**(4), 36 (2004)
23. McKee, D.: 80 to 0 in Under 5 Seconds: Falsifying a Medical Patient's Vitals. `https://bit.ly/2LJI8bB` (2018)
24. McNab, C.: Network Security Assessment. O'Reilly Media (2016)
25. Mirsky, Y., Mahler, T., Shelef, I., Elovici, Y.: CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning. In: USENIX Security (2019)
26. MITRE: ATT&CK Tactic: Lateral Movement. `https://bit.ly/2qwuUaE` (2019)
27. Mundt, T., Wickboldt, P.: Security in building automation systems - a first analysis. In: Cyber Security (2016)
28. O'Brien, G., Edwards, S., Littlefield, K., McNab, N., Wang, S., Zheng, K.: Securing Wireless Infusion Pumps In Healthcare Delivery Organizations (2017)
29. Philips: Data Export Interface Programming Guide (2015)
30. Regalado, D.: Inside the Alaris Infusion Pump, not too much medicine, plz. DEF CON 25 IoT Village - `https://youtu.be/w4sChnS4DrI` (2017)
31. Rios, B.: Infusion Pump Teardown. S4x16 - `https://youtu.be/pq9sCaoBVOw` (2016)
32. Roberts, P.: Let's Get Cyberphysical: Internet Attack shuts off the Heat in Finland. `https://bit.ly/33XQgeK`
33. Rushanan, M., Rubin, A., Kune, D., Swanson, C.: SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks. In: IEEE S&P (2014)
34. Seri, B., Vishnepolsky, G., Zusman, D.: Critical Vulnerabilities to Remotely Compromise VxWorks, the Most Popular RTOS. Tech. rep., Armis (2019)
35. Sheefer, Y., Porticor, Holz, R., TU Munchen, Saint-Andre, P.: Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS) (2015)
36. Symantec: New Orangeworm Attack Group Targets the Healthcare Sector in the U.S., Europe, and Asia. `https://symc.ly/33Rpp3S` (2019)
37. Symantec: Whitefly: Espionage Group has Singapore in Its Sights. `https://symc.ly/2qoF3WG` (2019)
38. Taylor, C., Venkatasubramanian, K., Shue, C.: Understanding the Security of Interoperable Medical Devices Using Attack Graphs. In: HiCoNS (2014)
39. US DoH CISA: ICS-CERT Advisories. `https://bit.ly/369pLnZ` (2019)
40. Wood, D., Apthorpe, N., Feamster, N.: Cleartext Data Transmissions in Consumer IoT Medical Devices. In: IoTS&P (2017)
41. Xu, J., Venkatasubramanian, K., Sfyrla, V.: A Methodology for Systematic Attack Trees Generation for Interoperable Medical Devices. In: SysCon (2016)
42. Xu, Y., Tran, D., Tian, Y., Alemzadeh, H.: Poster: Analysis of Cyber-Security Vulnerabilities of Interconnected Medical Devices. In: CHASE (2019)