Exposure Assessment on Medical Devices in the Netherlands

Christodoulos Tziampazis
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
c.tziampazis@student.utwente.nl

ABSTRACT

In recent years, the internet connected devices and systems are an inseparable element in the healthcare industry. Alongside with the necessity of such medical-related apparatus, comes the need for cybersecurity awareness concerning the hospitals' network infrastructures. Given the importance of the healthcare domain, this study aims to identify medical devices and characterize the healthcare environment in the Netherlands. More specifically, keywords were formed–based on the findings collected from the literature review–and queried with Shodan. The obtained IP addresses were further examined based on their available services and broadcasted data. In general, the study found hospitals to be secure as long as medical apparatus are concerned. Nonetheless, a few Digital Imaging servers were discovered to be directly exposed to the public internet.

Keywords

Keywords–Medical Devices; Healthcare; Exposure; Shodan; Netherlands.

1. INTRODUCTION

Nowadays, the healthcare domain became solely dependent on ubiquitous systems which enabled hospitals, clinics, nursing homes and many other healthcare institutions to remotely monitor and manage medicine, patients and devices[1]. The emerging pervasive technologies have given raise to internet enabled medical devices like MRI machines, insulin pumps, pacemakers and many others. The use of such devices has significantly increase the quality of the healthcare domain and created more convenient medical facilities.

With the adoption of the Electronic Health Records(EHRs), medical devices were empowered to become networked connected with the capabilities of monitoring patients health, administer medicine and managing health records. The combination of these technologies unveiled new attack vectors on medical devices. Due to the network capabilities of the devices, attackers could capture the network traffic of such devices and exploit the data accordingly to retrieve critical information like protocols of communication, the type of web server and the type of database used[2].

Due to the high concentration of private information, medical devices have received a large cybersecurity attention. As a relatively new topic, attacks on such devices could trigger ransom extortions[3] and patients identity theft. Nevertheless, various researchers demonstrated that attacks do not only revolve around ransoms but they could also target the remote controlling of a device in order to alter its normal behavior. In 2015, researcher Billy Rios announced a flawed drug pump owned by Hospira. The researcher disclosed a vulnerability that could allow attackers to administer deadly dosage by accessing the device over the Internet [4].

Given the fatal impacts that such intrusions could trigger, this study aims to characterize any potential exposed medical devices and services in the Netherlands. Since the exploitation can be risky and imply ethical problems, the investigation will be conducted under a completely passive approach. The research aims to answer the following questions:

- How to identify internet-connected medical devices in the Netherlands?
- What types of devices are exposed?

In order to answer these questions, a search engine called Shodan–a scanner for internet-connected devices–was utilized to identify exposed medical devices. Shodan's database has been found to contain a lot of valuable information about various healthcare organisations, medical software and devices that will be discussed further in Section 5.

The remainder of this paper is organized as follows. Firstly, we reviewed a literature of healthcare devices and services. Secondly, we justify the usage of the acquired background knowledge, and thirdly, we lay out the research methodology. At last, we summarize the key findings and the results of this research alongside with potential future directions.

2. LITERATURE REVIEW

The literature review is an attempt to gain as much knowledge as possible about medical devices alongside with their services and communication protocols.

The papers reviewed for this study were collected from scholar literature search engines–namely Google Scholar, Scopus and IEEE Xplore–by using the keywords depicted in *A. Literature Keywords* [1]. Accompanying the information from the research papers, we took into consideration manuals of medical devices from various vendors.

[1]https://github.com/ChristodoulosTziampazis/Exposure-Assessment-on-Medical-Devices-in-the-Netherlands/issues/1

31th Twente Student Conference on IT July. 5th, 2019, Enschede, The Netherlands.

Initially, the integration of the wireless connected medical devices have enhance the reliability and the quality of healthcare. However, despite all the benefits that such technologies could provide, various studies showed that hackers could maliciously exploit their wireless capabilities in order to infect the devices, gather sensitive information or even threaten human lives[5].

In the last couple of years, security researches presented their work in different conferences proving to companies and organizations around the world that attackers could compromise their medical products and services. In a Black Hat conference in 2011, the researcher Jerome Radcliffe, a diabetic himself, demonstrated that he could remotely control his own insulin pump delivering lethal doses of insulin[6].

In DerbyCon, security researchers reported that more than 68,000 medical devices were identified in Shodan to be directly exposed on the public internet. The devices were ranging from MRI machines, PACS servers, infusion and pacemaker systems. The researchers pointed out that the devices and systems found, were having default configuration settings that are accessible by everyone on the public internet. By analyzing the devices further, the researchers were able to extract information like software versions and operating systems, healthcare organisation's floor and office numbers, employee names, default credentials for remote connections and many more [7]. Similarly in another study, devices were found to be vulnerable not only from their naive configuration settings but also from the outdated software versions they were running on, uncovering in that way the names of various medical vendor such as Animas, Roche and Carefusion [8].

Particularly, Cybersprint conducted a study in 2019 concerning the cyber security level of hospitals in the Netherlands. The team confronted a total of 28 hospitals with various vulnerabilities and most importantly with critical outdated systems. However, what draw our attention was that larger hospitals had significantly lower security measurements in comparison with smaller hospitals. Cybersprint stated that "Outdated software could have severe consequences on the security of patient records, it is a matter of downloading a certain program and applying it to the website". In the same manner as the aforementioned studies, Cybersprint disclosed vulnerabilities associated with outdated software and default configuration settings [9].

At last, medical vendors and manufactures seems to focus on the robustness of the devices and overlook the potential security threats. These kind of security analysis and the effort of disclosing potential cyber targets are of great importance since they deliver a more clear view on the present security threats and trends.

3. BACKGROUND

The main objective at this phase is to gain a background knowledge about default communication protocols and services that are used by medical devices. As a result, keyword lists would be assembled that will be later used to query Shodan's database in an attempt to identify medical devices.

When it comes to personal medical devices–like infusion pumps, pulse oximeters, etc–technologies like Bluetooth and Zigbee are used to communicate data from the devices to the gateways. The transmitted health data should be then transformed into standard form in order to be stored and used in a later stage [10] (Figure 1). With that being said, the International Standard Organisation (ISO) laid out standards for the communication and the interoperability of non compatible medical devices. The most widely known communication standards are the following: DICOM (Digital Imaging and Communication in Medicine), HL7 (Health Level 7) standards for exchanging healthcare data, ISO/IEEE-1073 that enables communication between different medical devices and external medical systems, ENV 13606 the European standard for Electronic Healthcare Record (EPR)[11] [12].

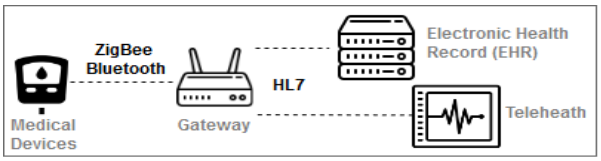

Figure 1: Data Transition

Exchanging medical data does not require any unfamiliar protocols, what drew our attention though is the communication of medical imaging. Picture Archiving and Communication Systems (PACS) are designed to provide a more convenient way of storage and retrieval of medical imaging by utilizing the DICOM protocol that enables this type of data transaction[13].

Finally, looking further into some medical devices manuals we were able to extract a list of medical-related ports[14] [15], presented in Appendix B. Nevertheless, in order to create a more accurate representation of the exposed medical devices we extended the keywords with a list of Digital Imagining open source software and a list of medical devices, as depicted in *B3. Digital Imaging Open Source Software*[1] and Appendix C respectively.

4. METHODOLOGY

In this section, we will describe the methodology used to characterize medical devices in the Netherlands. As explained before we will make use of the information provided by Shodan in order to carry out this research. An overview of the methodology is depicted in Figure 2.

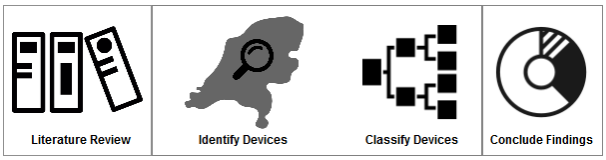

Figure 2: Methodology Overview

To begin with, it is important to get an overview of how medical data is stored and distributed in the Netherlands. Dutch Electronic Medical Record(EMR) is supported by a decentralized infrastructure managed by each healthcare organisation. The exchange of patient's data between different healthcare professionals could be achieved through a national organisation switch, the *Landelijk Schakelpunt* (LSP), which is responsible to redirect clients to the desired organisation's database[16]. Having said that, it will suffice to focus solely on the institutions software infrastructures since there is no central management point of the data.

Search engines, such as Shodan[17] and Censys are examples of some online scanner services that are constantly scanning the Internet. As for example, Shodan, crawls the entire internet at least once a month probing all the avail-

able IP addresses and analyzes their responses for approximately 250 services. For each available service, Shodan also provides a response banner as in Figure 3. In this research, Shodan's database will be utilized in order to gather as much information as possible about healthcare devices and analyze them in a later stage.

```
HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "323347221"
Last-Modified: Mon, 17 Sep 2018 01:32:05 GMT
X-Frame-Options: SAMEORIGIN
Content-Length: 36678
Date: Sun, 23 Jun 2019 03:07:19 GMT
Server: lighttpd/1.4.49
```

Figure 3: Example of a banner

The literature shows that search engines, like Shodan, is a common practice in various researches that aim to characterize and evaluate various services around the world. In order to query the database in the most efficient way we utilized Shodan's Developers API in Python.

4.1 Device discoverability

Shodan provides a database which contains a vast amount of devices from the Netherlands. However, Shodan is not classifying the devices thus from the information provided we will attempt to address which of them are medical related. As explained before, Shodan updates its database at least one time in a month, therefore, to prevent losing valuable data all the results were concentrated in a local database.

To obtain the desired results, we queried Shodan's database with all the aforementioned lists of keywords, as shown in *B. Shodan Keywords*[1]. Due to the enormous size of the database, the use of various filters was essential in order to narrow the results down to the medical-related IP addresses. For instance, *Country:NL* was used as a prefix for all the queries to capture only IP addresses corresponding to the Netherlands alone. In addition, filters like *port*, *ip*, *title*, *org*, *asn*, *os* and *product* were also used. Examples of such queries are depicted in Figures 4 and 5. The word *Ziekenhuis*, for example, resulted in 610 results and 6 healthcare organisations in total.

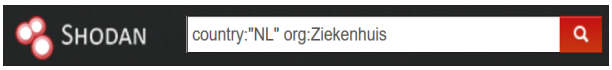

Figure 4: Querying organisations advertised as Ziekenhuis

Figure 5: Querying all devices running on port 104

Investigating the devices found, requires a set of features that will classify them either as true positives or false positives. If a device does not provide enough information then it will be classified as unknown.

The identification features are comprised by the following lists:

- Protocols related to medical devices
- Medical Devices
- Medical Open Source Software
- Dutch Medical Institutions

4.2 Processing Results

The approach of processing the extracted results is depicted in Figure 6.

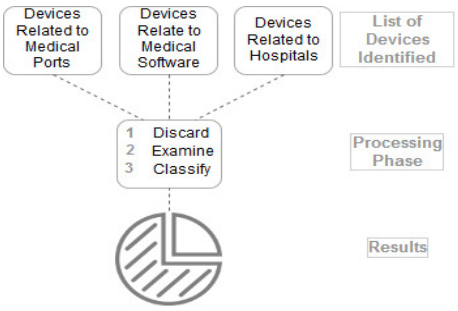

Figure 6: Processing Approach

The end result of all the queries revealed a total number of 2108 IP addresses. From the collected data, all the repeated entries with the same IP address and ports were discarded. Next, the stand alone IP addresses, which had no connection with any of the healthcare organisations or did not matched any of the medical protocols listed in Appendix B, were filtered and discarded too. In that way the database was narrowed down to 1178 IP addresses related with healthcare organisations and 893 with medical protocols and medical software.

To conclude our findings, a dictionary was created containing all the banners and the number of times that each occurs in the database. The dictionary was divided into a list of known service banners–like HTTP, SSH, etc–and to a list of all unknown service banners that will be further analysed (Figure 7).

Each entry in the dictionary will be analyzed based on its banner. Standard ports cannot be used as evidence to determine the supported service. For instance, a device was found to support HTTP services on port 104–a standardized port for DICOM communication.

Finally, this last phase of filtering provided us the final database which it will be presented in section 5 Results & Discussion.

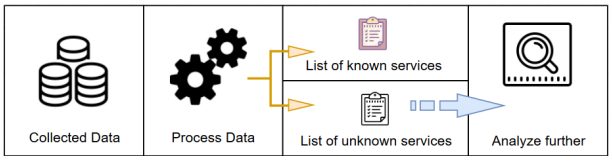

Figure 7: Analyze Unknown Results Methodology

5. RESULTS & DISCUSSION

In this section we will present the results of this research as also the classification process. The expected outcome, based on the knowledge gained from the literature, is to find a little to no directly exposed medical devices but rather mediator services and servers.

To begin with, for each found device we recovered: the IP address, host organisation, operating system, software version and all the available open ports alongside with their response banners. In total, Shodan was able to discover

9,555,506 million devices that are located in the Netherlands. Only 0,02% (2071) where identified and examined in this research. Particularly, the devices were found to be accommodated from more than a hundred(163) different Internet Services Providers, Web Hosting companies and Healthcare Organisations.

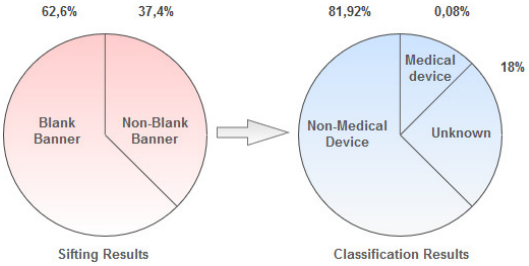

Figure 8: Overall Results

Overall, the devices combined, are running a total of 1594 different services. The combination of the devices found and the available services yielded a total of 36,337 entries where, as depicted in Figure 8, 62% (22,748) of them had no response banner whereas the rest 37% were furthered examined and classified. In order to examine the remaining 37% of the banners, the data was divided into the following categories: devices that have as host organisation a healthcare institution, related to open software services and stand alone devices. All three categories will be discussed further in an ascending order of importance in the subsections 5.1, 5.2 and 5.3 respectively.

At last, the classification results were divided into the following 3 classes (Figure 8): Unknown(18%), Non-Medical Devices(81,92%) and Medical Devices(0,08%). A device is classified as *Unknown* if the data that appears in the banner cannot be interpreted(as for example Figure 11). Moreover, in order to classify IP addresses as *Non-Medical Devices*, their banners must meet one of the features listed in *E. All Responses Identified*[1], whereas addresses classified as *Medical Devices* are determined by the features listed in *B. Shodan Keywords* [1].

5.1 Hospital Devices

As described above, we utilized Shodan's database in order to retrieve all the IP addresses located in the Netherlands. Despite the data collected from medical protocols and software, we decided to enrich the dataset by adding IP addresses related to well-known dutch healthcare organisations, listed in *G. List of Hospitals*[1], with the intent to uncover medical devices that some healthcare organizations may prefer to host on cloud providers abroad.

This exploration extended our dataset by adding 1178 IP addresses hosted by healthcare organisations. Overall, the data collected from the hospitals did not uncover any services that could be classified as medical related. The services broadcasted by these hospitals are further discussed in Appendix A.

5.2 Open Source & Medical Vendors Devices

By querying Shodan with the list of open source software (*B1, B3, B4 Open Source Software*[1]) and the list of known vulnerable vendors (*B2. Vulnerable Vendors*[1]), 15 open source software & operating systems were extracted as shown in Figure 9. From the bar chart we can conclude that Electronic Health Record software appears to be more tolerant in discoverability than the rest of the services. The complete list can be found in *F. Results of Open Source Software & OS* [1].

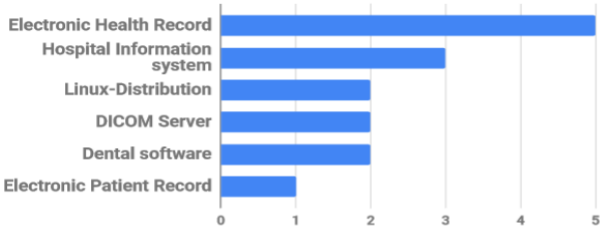

Figure 9: Total Open Source Software Identified

In total, 1358 banners were extracted with 111 of them to be blank. In Figure 10 we present the *list of known services* with the top 10 services depicted, revealing valuable services like Telnet and SSH. The complete list can be found in *E. All Responses Identified* [1].

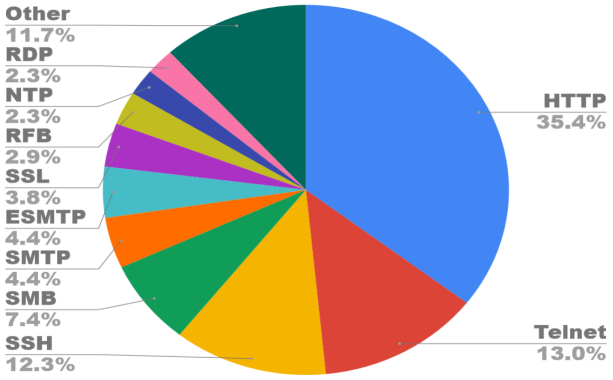

Figure 10: Services for the IP Addresses Identified

Concluding the results, together with the *list of unknown services*, we manage to extract some worth mentioning information. As depicted in Figure 10, HTTP occupies 34.7% of the available services that are mainly redirect to the login page of each software. What was observed is that there is no restriction on who can reach their login pages thus it raises security concerns. Furthermore, a Philips web service was found under the name of Leiden University Medical Center that redirects to the pathology sector of the hospital. Lastly, from the unknown services, an IP address revealed a *WEB DICOM Viewer Server* hosted by SOFTNETA–a PACS server provider–that runs on port 104 and is accommodated by Microsoft Azure services. The DICOM Viewer was deducted by searching for a HL7 platform called MIRTH.

Finally, beside the aforementioned findings, no other noteworthy information was deduced.

5.3 Stand Alone Devices

The last set of data covers all the stand alone addresses that were retrieved by querying medical-related ports. The outcome of all the addresses that are running services of the presumptive medical ports, listed in Appendix B, revealed 31,594 entries. However, only the 29% (9,296) of the banners had an actual response.

The *known services* are the 76%(7067) of the total of 9,296 responses. To that end, after analyzing the banners of the *known services* no further realization could be derived and thus they were excluded from being a potential medical device. The remaining 24% (2229) is comprised by two types of responses: unknown banners and banners related to medical ports.

In total, the unknown banners occupy the 76%(1699) of the 2229 responses. By analyzing further this results, we were not able to derive any information that could lead us to conclude an unknown response as a medical device, thus, all the 1699 unknown responses were classified as Unknown Devices. An example of a banner that is classified as unknown can be seen in Figure 11.

```
0\x0c\x02\x01\x01a\x07\n\x01\x00\x04\x00\x04\x00
```

Figure 11: Example of banner that could not be classified

The rest 24% (530) of the 2229 banners were responses related to medical ports as explained above. In Figure 12, the number of occurrences for each banner related to a medical port is presented, indicating also whether their responses were blank or non-blank.

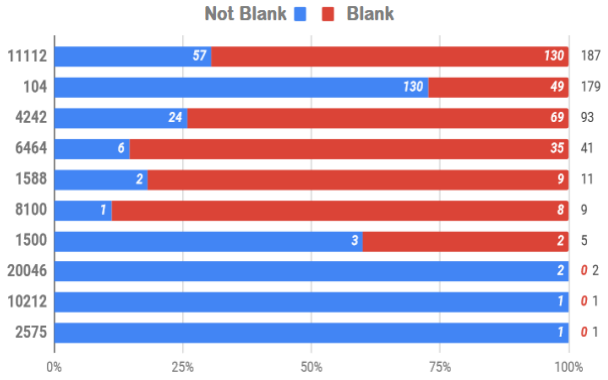

Figure 12: Banners Retrieved from Querying Medical Ports

While investigating those responses, we manage to recover 11 banners clearly indicating DICOM services. As it was described in section *3. Background*, DICOM is a protocol for communicating medical images and so such devices could have a direct connection with medical systems like MRI, X-Ray and Ultrasound machines. Nevertheless, the devices found are presumed to be servers and not medical apparatus. If the servers are exploited properly, they might reveal crucial information that could led attackers to identify other medical imaging devices. An example of such banner is depicted in Figure 13.

Briefly, the DICOM response–*FINDSCU*–it is used by servers as query/retrieval message for performing different operations with medical images like C-FIND, C-STORE and C-MOVE.

```
DICOM Server Response
\x02\x00\x00\x00\x00\xaf\x00\x01\x00\x00ANY-SCP         FINDSCU
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x10\x00\x00\x151.2.840.10008.3.1.1.1!\x00\x00\x19\x01\x00\x02
\x00@\x00\x00\x111.2.840.10008.1.2P\x00\x001Q\x00\x00\x04\x00
\x00@\x00R\x00\x00\x131.3.6.1.4.1.30071.8U\x00\x00\x0efo-dicom 4.0.0
```

Figure 13: DICOM Response

The available information from the DICOM servers is summarized and presented in Table 1. The data is categorized by the service ports and the host organisations together with their associated Autonomous System Number(AS).

At last, the 11 DICOM servers identified were classified as medical devices representing the 0,08% of the total findings (Figure 8). The rest of the entries associated with

Table 1: DICOM Details

Ports	Organisations	ASNs
104	Microsoft Azure	AS8075
11112	SURFsara	AS1103
–	LeaseWeb Netherlands B.V.	AS60781
–	Transip B.V.	AS20857
–	KPN	AS1136
–	Ziggo	AS6830

medical ports from the Figure 12, were classified as unknown since there was not enough information to indicate the type of service they provide.

5.4 Overall Results & Discussion

As it was expected, no medical devices were identified to be directly exposed on the internet other than the DICOM servers. Most of the identified devices did not provide enough information in order to be classified, however, the overall results of this preliminary study showed sufficient amount of data that could be used to characterize public medical services and their vulnerabilities.

Two major factors made the filtering process challenging. As can be seen from the list of medical ports in Appendix B, infusion pumps could also communicate through the HTTP/HTTPS ports 80 and 443 adding in that way more complexity in the discarding phase. Lastly, medical apparatus are expected to use Dynamic Host Configuration Protocol (DHCP) for the allocation of their IP addresses and even worst use non-standard ports for their communication creating an unstable environment of information that is hard to address.

Furthermore, what is remarkable from the identified DICOM servers is that their level of network security is poor since there is no protection of the data advertised in the public Internet and there is not even a virtual private network (VPN) protection. Medical software, as described in the subsection 5.2, revealed log in pages that are presumably redirecting to Electronic Health Records(EHR) databases, but due to the non-intrusive nature of the research this claim is only an assumption. Other services identified like NTP, Firewalls and Remote Desktop Protocols could be further exploited with the potential of revealing valuable information about the private devices behind them.

Overall, more than 80% of the collected data was classified as non-medical devices, however, we were able to extract a few(11) devices that are directly linked with medical apparatus. Although this study was conducted with a passive approach and we concluded our findings only by analyzing banner responses, the assembled dataset has even more to unveiled if it is analyzed further.

At last, based on the findings, the healthcare institutions together with the open source software and medical vendors, appear to utilize the following Operating Systems and Distribution listed in *D. Operating Systems* [1].

6. FUTURE DIRECTIONS

There is no doubt that the Internet its a essential element for the healthcare sector. Although it establishes a more convenient communication environment, at the same time it raises major security concerns. This study showed promising steps towards an unsecured environment that could unveiled various vulnerabilities and security gaps in healthcare organisations and medical devices.

Having said that, there are several encouraging future direction that could be addressed based on the dataset assembled by this research. Firstly, future studies could expand significantly the depth of this research by addressing potential vulnerabilities for the devices and services found. Secondly, the services advertised by the medical open source software could be further examined with the potential to determine the type of the medical data that are possibly exposing. Lastly, future work could focus on identifying the owners of those exposed delicate devices and informed them accordingly about the insufficient level of network security. All the aforementioned directions could help enhance the security capabilities of healthcare organisations and medical devices.

7. REFERENCES

[1] A. Rahmani, N. K. Thanigaivelan, T. Nguyen Gia, J. Granados, B. Negash, P. Liljeberg, and H. Tenhunen. Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems. In *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, pages 826–834, Jan 2015.

[2] HelpNetSecurity. Hackers are finding creative ways to target connected medical devices. https://www.helpnetsecurity.com/2018/09/28/target-connected-medical-devices/.

[3] C. Scott Kruse, B. Frederick, T. Jacobson, and D. Kyle Monticone. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1):1–10, 2017.

[4] K. Zetter. Hackers can send fatal doses hospital drug pumps. https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps , 2015.

[5] J. Sametinger, J. W Rozenblit, R. Lysecky, and P. Ott. Security challenges for medical devices. *Commun. ACM*, 58(4):74–82, 2015.

[6] J. Radcliffe. Hacking medical devices for fun and insulin: Breaking the human scada system. 2011, 2011.

[7] D. Pauli. Thousands of directly hackable hospital devices exposed online. https://www.theregister.co.uk/2015/09/29/thousands_of_directly_hackable_hospital_devices_found_exposed/, September 29,2015.

[8] E. McMahon, R. Williams, M. El, S. Samtani, M. Patton, and H. Chen. Assessing medical device vulnerabilities on the internet of things. In *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pages 176–178. IEEE, 2017.

[9] Cybersprint. Dutch hospitals vulnerable to cyber attacks. https://www.cybersprint.com/insights/dutch-hospitals-vulnerable-to-cyber-attacks/, 2019.

[10] Continua Health Alliance. Fundamentals of Medical-Grade Data Exchange. https://www.pchalliance.org/sites/pchalliance/files/Fundamentals_Medical-Grade_Data_Exchange_Sep2018.pdf.

[11] M. Galarraga, L. Serrano, I. Martínez, and P. de TOLEDO. Standards for medical device communication: X73 poc-mdc. *Studies in health technology and informatics*, 121:242, 2006.

[12] L. Schmitt, T. Falck, F. Wartena, and D. Simons. Novel iso/ieee 11073 standards for personal telehealth systems interoperability. In *2007 Joint Workshop on High Confidence Medical Devices, Software, and Systems and Medical Device Plug-and-Play Interoperability (HCMDSS-MDPnP 2007)*, pages 146–148. IEEE, 2007.

[13] F. Valente, L. Bastião Silva, T. Marques Godinho, and C. Costa. Anatomy of an extensible open source pacs. *Journal of digital imaging*, 29(3):284–296, 2016.

[14] General Electric. AW Server Site Requirments. https://www.gehealthcare.com/-/media/0730cd225cbd4778994a8a244ad43b42.pdf.

[15] G. OḂrien, S. Edwards, K. Littlefield, N. McNab, S. Wang, and K. Zheng. Securing Wireless Infusion Pumpsin Healthcare Delivery Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-8.pdf.

[16] Walfare Ministry of Health and Sport. Ict in duct healthcare: An international perspective. https://joinup.ec.europa.eu/sites/default/files/document/2014-12/ICT%20in%20Dutch%20Health%20Care%20-%20An%20international%20Perspective.pdf, 2006.

[17] J. Matherly. What is Shodan. https://help.shodan.io/the-basics/what-is-shodan.

APPENDIX

A. HEALTHCARE ORGANISATIONS ENVIRONMENT

The network environment and the software infrastructure of healthcare organisations was characterized by academic, large and small hospitals in the Netherlands. By querying Shodan's database with the keywords from the list *B5. Hospital Related Words*[1] we were able to extract in total 33 hospitals listed in *G. List of Hospitals*[1], with their associate IP ranges.

By summarizing all 3184 entries and excluding all the blank banners we concluded the *list of known services* presented in Figure 14. One can observe that the most common service–healthcare institutions broadcasts–is HTTP on ports 80, 443, 8080, 8443, etc. Each IP address seems to run, on average, 2.77 services. The complete findings can be seen in *E. All Responses Identified* [1].

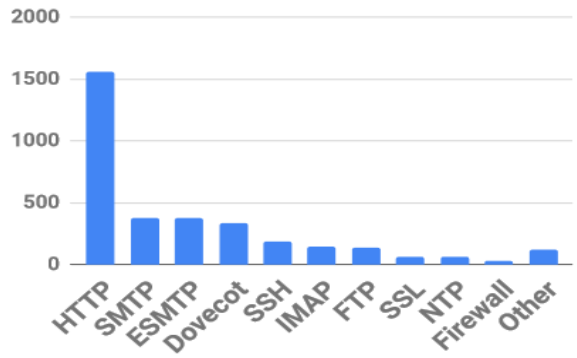

Figure 14: Top 10 Hospital Services

The *list of the unknown services* occupies the 4.5% (142) of the total results.

After examining the banners with the unknown responses, as discussed in 4.2 Processing Results, we were not able to derive their type of services due to the insufficient information broadcasted.

Finally, the hospital data did not reveal any suspicious responses and by considering the list of medical ports in Appendix B, we concluded that no exposed medical device was found.

B. LIST OF MEDICAL PORTS

Medical ports	
104	(DICOM)
11112	(ACR/NEMA DICOM)
6464	(IEEE 11073-20701)
4242	(Orthanc-DICOM Server)
2761/2762	(DICOM ISCL/TLS)
10212	(GE HMI/SCADA)
4006	(GE DICOM transfers)
2575	(Health Level 7)
20046	(HL7 Message Transfer)
1500, 4080, 443, 80	(B. Braun Pump server)
8100,9292,11443, 11444	(Hospira Pump server)
51244	(Baxter Pump Server)
3613	(Carefusion Pump Server)
1588	(Smiths Pump Server)
9292, 443, 8443, 51243	(Other Pump Server ports)

C. MEDICAL DEVICES

List of Medical Devices Names
ACHIEVA 1.5
AIDA
ALPHA10
ALT HDI 5000
APLIO300
AQUILION
AW Fast link 17
AXION ARTIS DFC
BIOVISION
BRIGHTSPEED
BRILLIANCE 16
BV Pulsera
CR
DL Image Processor
DRY6800
Drystar 5300
DryStar 5502
EDGE
Emotion 6
ENVISOR
EPIC7C1
GATE
HD15
HDI11X
HDI11XE
IE33
Infinia
INGENIA
INNOV A
INTELLISPACE
KODAK 8000C
LITHOSKOP
LOGIQ 5
LOGIQ P5
MAMMOMAT Inspiration 3159
MAMMOMAT Inspiration 3630
MILLENUM
Nemio XG
PAXPORT
PETCT
Positioner
Precision T7400
PROSOUND 10 PREMIER
SIREGRAPH CF
SONIALVISION SAFIRE 17
14 Sonus 1000 0
VENTRI
VIVID2
VIVID3
VIVID7
WS-RM-VF1