A Study into Data Analysis and Visualisation to increase the Cyber-Resilience of Healthcare Infrastructures

ABSTRACT

In May 2017, a global ransomware campaign adversely affected approximately 48 UK hospitals. Response to the WannaCry cyber-attack resulted in many hospital networks being taken offline, and non-emergency patients being refused care. This is a clear example that data behaviour within healthcare infrastructures needs to be monitored for malicious, erratic or unusual activity. There is a perceived lack of threat within healthcare organisations with regards to cyber-security. Hospital infrastructures present a unique threat vector, with a dependence on legacy software, medical devices and bespoke software. Additionally, many PCs are shared by a number of users, all of whom use a variety of disparate IT systems. Every healthcare infrastructure configuration is unique and a one size fits all security solution cannot be applied to healthcare. Existing cyber-security technology within hospital infrastructures is typically perimeter-focused. Once a malicious user has compromised the boundary through a backdoor, there is a lack of security architecture monitoring active potential threats inside the network. Therefore, this paper presents research towards a system, which can detect unusual data behaviour through the use of advanced data analytics and visualisation techniques. Machine learning algorithms have the capability to learn patterns of data and profile users' behaviour, which can be represented visually. The proposed system is tailored to healthcare infrastructures by learning typical data behaviours and profiling users. The system adds to the defence-in-depth of the healthcare infrastructure by understanding the unique configuration of the network and autonomously analysing.

CCS CONCEPTS

• **Security and Privacy**→ **Network Security**; • **Computing Methodologies** → Machine Learning

KEYWORDS

Cyber-Security, Network Security, WanaCrypt0r, WannaCry Machine Learning, Visualisation, Healthcare Infrastructures

ACM Reference format:

IML '17, October 17-18, 2017, Liverpool, United Kingdom
© 2017 Association for Computing Machinery.
ACM ISBN 978-1-4503-5243-7/17/10…$15.00
http://dx.doi.org/10.1145/3109761.3109793

1 INTRODUCTION

Modern IT systems are crucial to clinical care service providers. They are relied upon to collect and store sensitive patient data, govern human life support devices and enable communication for archiving and information sharing [1]. Disabling or disrupting the any of these systems would have far reaching consequences within healthcare infrastructures. Relying on traditional security models to safeguard these systems has proven to be ineffective; particularly in relation to the emergence of new technology such as mobility, cloud, social and Bring Your Own Device (BYOD) [1].

Digitized data in healthcare is growing. Data is now processed from internal and external sources, including mobile devices, wearable sensor devices, Electronic Health Records (EHRs), Radiology Images, Videos, clinical notes, social media, blogs and remote health monitoring systems [2]. Terabytes of data generated from medical sensors is also used to increase the likelihood of reliable health diagnoses through accurate and detailed real-time data analysis [3]. However, this volume of data is growing beyond the capacity of the service providers and is expected to increase in the coming years [2]. The datasets produced are often unstructured, existing in formats which are isolated, disparate or incompatible [4]. There is often a lack of processing capabilities within healthcare networks to load and query the data effectively [2].

Additionally, the boundaries for healthcare systems are evolving, with many patients having the option of accessing their healthcare data from home PCs and mobile devices. This increases the attack surface significantly. A lack of security for healthcare devices leads to both loss of patients' privacy and potential physical harm to the patient. There is a risk that erroneous data is introduced or legitimate data is modified or suppressed by adversaries [5]. The security implications mean that bespoke systems need to be put in place to safeguard and protect data. However, the reliance on legacy software and bespoke systems result is an increased vulnerability to cyber-attacks [6]. The following successful hospital security breaches are testament to this:

- In May 2017, the WannaCry ransomware campaign exploited a Server Message Block (SMB) vulnerability on TCP Port 445. SMB is a legacy protocol used to share files and printers over local networks. The exploit enabled the malware to use worm-like network propagation, encrypting files and demanding ransom payment, unless the system had been patched by Microsoft security bulletin MS17-010. The attack resulted in network downtime for 48 UK hospitals, with 6 suffering disruption lasting several days.
- In October 2016, a UK Hospital in Lincolnshire was taken offline for four days due to a variant of the Globe2 ransomware. All planned operations, outpatient appointments and diagnostic procedures were cancelled, with patients turned away and 2800 patient appointments cancelled as a result of the disruption.

- In 2008, the UKs biggest hospital lost all network connectivity due to several malware infection by the MyTob worm [6].
- In 2005, a Chicago hospital lost its entire pharmacy database, and in order to reconstruct medication records for its patients, paper printouts were required to be collected from nurses' stations [7].

2 BACKGROUND

Traditional approaches to endpoint security are no longer viable in the modern cyber-threat landscape [1]. Attack models have changed from attacks on single PCs to large scale attacks on entities through Advanced Persistent Threats. For example, zero data exploits; spear phishing, watering hole models and encrypted side channel methods are being increasingly used to infect critical systems. In addition, modern malwares have adopted and evolved *Evasion Techniques*, such as malware packing, obfuscation and polymorphism [1]. As such, the discussion in this section is focused on the specific threats and attack vectors facing healthcare infrastructures.

2.1 Medical Devices

Medical devices, in particular sensors within the body, have finite resources and therefore limited capabilities to self-protect. Wireless technologies, such as Wi-Fi, can suffer from interference caused by medical devices and allow malicious persons to access the network by masquerading as legitimate traffic. These medical devices often have no safeguards and are susceptible to buffer overflows when unexpected signals are received. Mechanical Ventilators are susceptible to total switch-off and change in ventilation rates. In addition, Syringe Pumps can be completely stopped. External Pacemakers, have a tendency to malfunction and Renal Replacement Devices have been shut off through successful attacks [8].

Most wearable devices record and collect medical data and then transmit the data to a remote server. This leaves the data vulnerable to man in the middle attacks [9]. It has been considered that security policies should be implemented between the wearable devices and the remote server, however this is unsuitable as it does not protect the patient wherever they travel, unless they carry a portable device to perform the security policy and communicate with the server about their persons at all times [9]. Further to this, an adversary can induce fatal blood glucose levels in patients with blood glucose sensors using two techniques [10]. Firstly, by forging or replaying packets sent from the Doctor. In this way, the attacker can introduce blood glucose imbalances through specifying an extremely large correction bolus. Or secondly from forging or replaying the patient, in this way false sensor data can be replayed to the Doctor to trick them into specifying a fatal dose.

In light of the above threats, cryptography based techniques (data encryption or cryptographic protocols) are commonly used to protect medical data [11]. However this may be too expensive in terms of processor usage and power consumption meaning that it is an unfeasible approach for biomedical devices [10]. Additionally, cryptographic methods introduce new challenges in terms of key management and dissemination. It is problematic to know in advance who will treat a patient, and there is difficulty in relaying that information to the healthcare provider. This process needs to be quick enough so as not to interfere with treatment of the patient, but secure enough so as not to compromise the key [10]. Medical devices, such as insulin pumps and pacemakers communicate wirelessly, with a wearable external monitoring and control unit, which needs to be accessible to emergency responders and medical personnel. It is therefore challenging to implement effective key-based encryption techniques due to the complexities of key management and revocation. Additionally, issues of limited power and heat-dissipation within the device compound the problem [10].

2.2 Healthcare Security Challenges

Within healthcare infrastructures, Medical Cyber-Physical Systems (MCPSs) are personal monitoring devices that can record and transmit multiple physiological signals [12]. The most prominent feature of a MCPS is the feedback loop that interacts with the physical environment. The data is provided to the MCPS through sensors that feed into the control algorithms to drive the actuators, which in turn change the physical environment. For safety-critical MCPSs, the ability to detect attackers, whilst limiting false alarms in order to protect the well-being of patients, is of critical importance [13]. However, threats to MCPS components are increasing with the malicious users aiming to cause node compromise [13]. This process can be initiated through over-the-air software updates, stack overflow exploits or '*logic bombs*' through third party developers. Security is a concern especially for small medical devices attached to a patient [14]. Compromise of storage of data could potentially result in patient death. Similarly, attacks on pharmacy systems could result in the wrong medication being prescribed leading to long term health concerns for the patient [14].

Yet, the most frequent outcome of a cyber-attack on a system is the unavailability of patient care due to computer outages [15]. Other common attacks, which are a challenge to healthcare security systems, are outlined as follows:

- Scanning attacks involve adversaries gathering meaningful information in order to launch a sophisticated attack upon an infrastructure [16]. These scans commonly include, IP address canning, port scanning and version scanning. With regards to Healthcare Infrastructures, an adversary can carry out segment scanning on HL7 information in order to learn personal identifiers, order numbers or patient visit information [16].
- Spoofing attacks involve malicious users masquerading as legitimate [16]. Masquerading is a passive spoofing attack where attackers exhilarate legitimate account credentials and then log in. Impersonation is an active spoofing attack, sometimes known as a replay attack, wherein attackers capture authentication traffic and replay the traffic in order to gain access to the healthcare infrastructure.
- Injection attacks involve exploiting vulnerabilities of Structured Query Language (SQL), JavaScript and other computer programs in order to successfully insert untrusted data [16]. In doing so, attackers may gain access to healthcare databases, attack web users and propagate viruses. Additionally, they may inject malicious segments commands or responses in order to reduce the security of healthcare infrastructures.
- Broken Authentication and Session Management involves attackers exploiting vulnerabilities in authentication mechanisms in order to assume the identities of legitimate users [16]. A brute force attack is an example of this kind of attack, taking advantage of weak passwords and small encryption keys, ultimately allowing a malicious user to perform all the functions available to a legitimate user.

- Distributed Denial of Service attacks (DDoS) involve exhausting system and network resources in order to make them unavailable [16]. For example a flooding-based DDoS sends a large number of packets to a web server, in doing so; legitimate requests are blocked as the CPU is overwhelmed.

To address these security challenges, we propose a solution that detects unusual data behaviours within healthcare infrastructures using advanced data analytics techniques.

3 APPROACH

Our research to date has focused on the development of a system for modelling data flow within healthcare infrastructures. The system assists information security officers, within healthcare organisations, to improve the situational awareness of cyber-security risks [17].

3.1 System Overview

The system provides contextual awareness to detect anomalous behaviour within network activity and is presented in Figure 1.

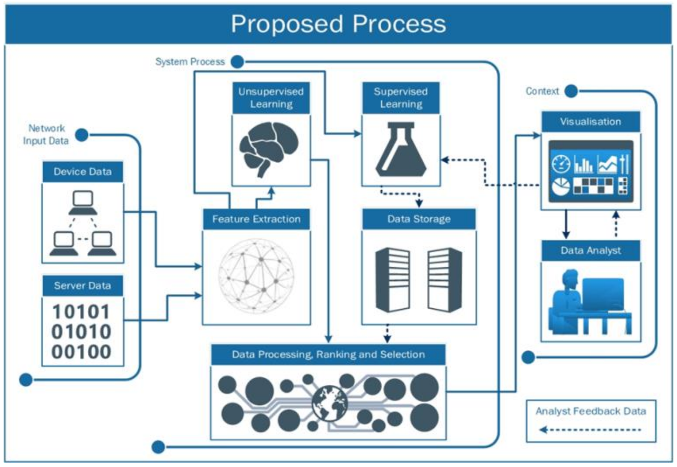


Figure 1: System Overview

Our system is a cyber-security machine learning system, which improves its accuracy over time through feedback from security analysts. The novelty of the system proposed in this paper, is the addition of visualisation techniques to aid the analyst to understand and explore the data. There is also a specific focus on healthcare infrastructures, which differ from other enterprise infrastructures due to their reliance on insecure medical devices, legacy systems, and bespoke software. The main challenge of the work involves big data analytics to process datasets generated by healthcare infrastructures. As such, in the following section, the data pre-processing aspect of the system is presented, using hospital data.

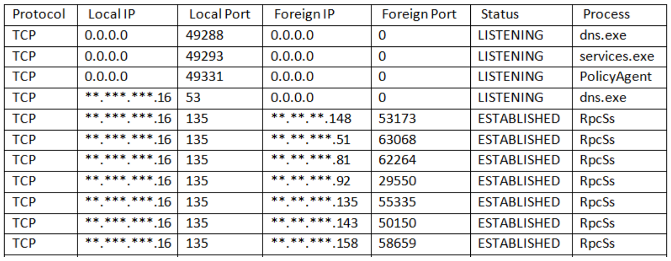
3.2 Data Collection

The dataset presented in this paper is comprised of real world data from a UK-based hospital, captured off three servers, which provide critical functionality to the hospital. The dataset is then prepared and subsequently visualised to capture a baseline assessment of the server port mappings. Finally, the data is prepared by removing low-risk data, such as typical port mappings. This data is then visualised so that only potentially malicious port communications remain. The data is captured by executing a netstat command, which displays network connections on a server. Additionally, the netstat command is executed with the parameters –abn. The netstat–a command displays all active connections of the TCP and UDP ports, on which the computer is listening. The netstat–b command displays the executable program name associated with the creation of the connection or listening port. The netstat–n command displays active TCP connections numerically and no attempt is made to determine names, in order to facilitate the dataset analysis. Specifically, the netstat command is executed on the following servers:

1. The Active Directory (AD) server, which manages directory based services for the hospital.
2. The Patient Administration System (PAS) server, which manages core functionality, such as patient administration, across the hospital.
3. Finally the Electronic Prescribing (EP) server, which generates, transmits and files prescriptions across the hospital.

An example of a typical selection of established port in the dataset can be found in Table 1.

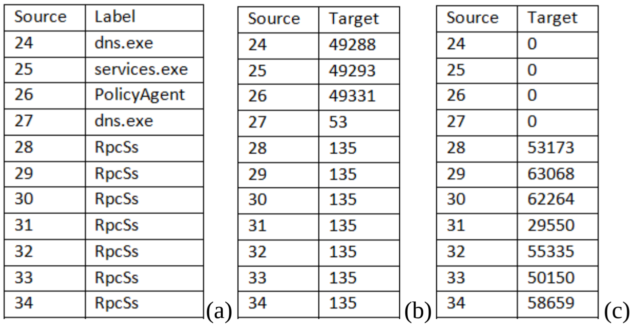
Table 1: Active Directory Dataset Sample



Protocol	Local IP	Local Port	Foreign IP	Foreign Port	Status	Process
TCP	0.0.0.0	49288	0.0.0.0	0	LISTENING	dns.exe
TCP	0.0.0.0	49293	0.0.0.0	0	LISTENING	services.exe
TCP	0.0.0.0	49331	0.0.0.0	0	LISTENING	PolicyAgent
TCP	**.***.***.16	53	0.0.0.0	0	LISTENING	dns.exe
TCP	**.***.***.16	135	**.**.**.148	53173	ESTABLISHED	RpcSs
TCP	**.***.***.16	135	**.**.***.51	63068	ESTABLISHED	RpcSs
TCP	**.***.***.16	135	**.**.***.81	62264	ESTABLISHED	RpcSs
TCP	**.***.***.16	135	**.**.***.92	29550	ESTABLISHED	RpcSs
TCP	**.***.***.16	135	**.**.***.135	55335	ESTABLISHED	RpcSs
TCP	**.***.***.16	135	**.**.***.143	50150	ESTABLISHED	RpcSs
TCP	**.***.***.16	135	**.**.***.158	58659	ESTABLISHED	RpcSs

3.3 Data Preparation

In order to provide an appropriate visualisation, the dataset undertakes a pre-processing phase. To do this, node and edge data are extracted and isolated into individual datasets. Three datasets are then produced for each data capture procedure. Examples of the node dataset and the two edge datasets are found in Figure 2.



Source	Label
24	dns.exe
25	services.exe
26	PolicyAgent
27	dns.exe
28	RpcSs
29	RpcSs
30	RpcSs
31	RpcSs
32	RpcSs
33	RpcSs
34	RpcSs

(a)

Source	Target
24	49288
25	49293
26	49331
27	53
28	135
29	135
30	135
31	135
32	135
33	135
34	135

(b)

Source	Target
24	0
25	0
26	0
27	0
28	53173
29	63068
30	62264
31	29550
32	55335
33	50150
34	58659

(c)

Figure 2: Active Directory Data Preparation – (a) Port Process – (b) Local Port – (c) Foreign Port

In Figure 2, the Source column refers to a common ID number indicating the Transmission Control Protocol (TCP) connection or listening port. Figure 2 (a) contains the port process running on the IP connection. Figure 2 (b) contains the local port number and Figure 2 (c) contains the foreign port number. In order to provide a proof of concept, the data is manually cleansed of low-risk data. Unknown port processes, or processes running on unfamiliar ports, are left in the dataset, whilst common processes, running on secure and known port mappings are removed.

4 VISUALISATION AND EVALUATION

To undertake the visualisation process, a case study of different visualisation algorithms is presented. Firstly, Yifan Hu, which is a force-directed graph drawing algorithm, is used to model the network data through a system of *bodies*, with forces acting between them [18]. It uses a multilevel approach to find global optimal layouts, and the Barnes-Hut octree technique, to approximate short and long range forces [18]. It is the first algorithm to combine both techniques for large scale graph drawing. Typically, this multilevel approach has three phases:

1. Coarsening: In this phase, a series of graphs are generated, with the aim of encapsulating the information of its parent, while containing fewer vertices and edges. The process continues until the coarsest graph layout is determined.
2. Coarsest graph layout: In this stage, the graph is then presented using an algorithmic technique that combines an adaptive step length control scheme.
3. Prolongation and Refinement: The layout on the coarsest graphs are then prolonged recursively to the finer graphs. Once this has been carried out, the layout is then refined again using the algorithm used in phase 2. This is an iterative process.

This overall process is defined as follows [18]:

```
Coarsest Graph Layout:
if $(n^{i+1} < MinSize \ or \frac{n^{i+1}}{n^i} > p)\{$
* $x^i := random\ initial\ layout$
* $x^i = ForceDirectedAlgorithm(G^i, x^i, tol)$
* $return\ x^i$
}

The Coarsening Phase:
$set\ up\ the\ n^i \times n^{i+1} prolongation\ matrix\ P^i$
$G^{i+1} = P^{i^T} G^i P^i$
$x^{i+1} = MultilevelLayout(G^{i+1}, tol)$

The Prolongation and Refinement Phase:
$prolongate\ to\ get\ initial\ layout: x\^{}i = P\^{}i\ x\^{}(i+1)$
$refinement: x^i = ForceDirectedAlgorithm(G^i, x^i, tol)$
$return\ x^i$
```
(1)

In Figure 3 the Active Directory Port Mapping is visualised. The Port to Port mappings are represented by circles, which are connected by lines. The processes associated with the creation of the connection are labelled. If an attacker attempts a privilege escalation attack, in order to extract confidential data (or perform a ransomware attack), they would comprise the Active Directory server. In Figure 4, the same Active Directory dataset is visualised, but the dataset has been processed to remove low-risk port mappings. In this case, there still remains a significant cluster of data present, which has been marked as of medium risk due to the process having been identified by the netstat command as Unknown. The Unknown cluster of dataset is due to a large number of IP addresses established on local port 445 to various foreign ports. As port 445 is within the 0-1023 range of 'Well known Ports', it is likely benign, but until the Process can be verified by a member of the hospital security team, the port mapping should be regarded as a potentially risk.

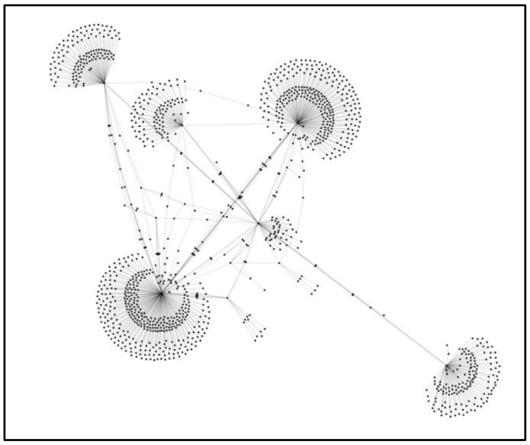


Figure 3: Active Directory Server Port Mapping

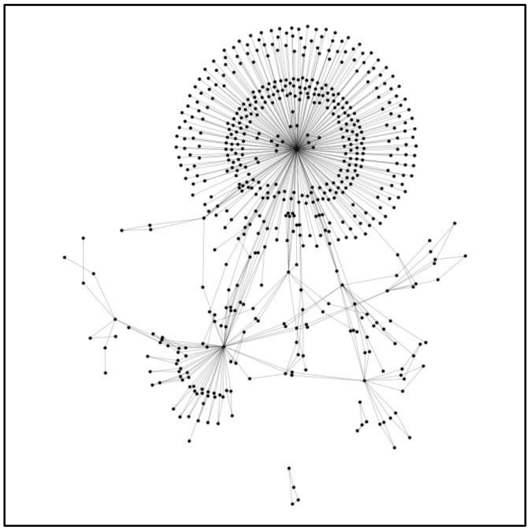


Figure 4: Processed Active Directory Server Port Mapping

In Figure 5 the Electronic Prescribing dataset is visualised. This dataset has far fewer connections than the Active Directory dataset and has more nuanced processes running on the ports. Whilst it is likely that the port mappings are legitimate or low risk, only a few rows of data have been manually removed between Figure 5 and Figure 6. If an adversary wanted to remotely alter a patient prescription in order to cause them physical harm, they would need to compromise the Electronic Prescribing server. In Figure 6 only a small number of port mappings have been removed from the visualisation. Many more can likely be removed but the expertise of the IT admin staff within the hospital would need to be leveraged and combined with machine learning algorithms in order to fully realise the benefits of the preparation and cleansing of the data.

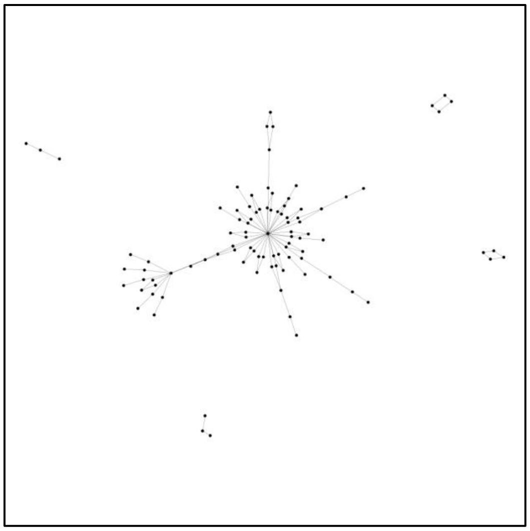


Figure 5: Electronic Prescribing Server Port Mapping

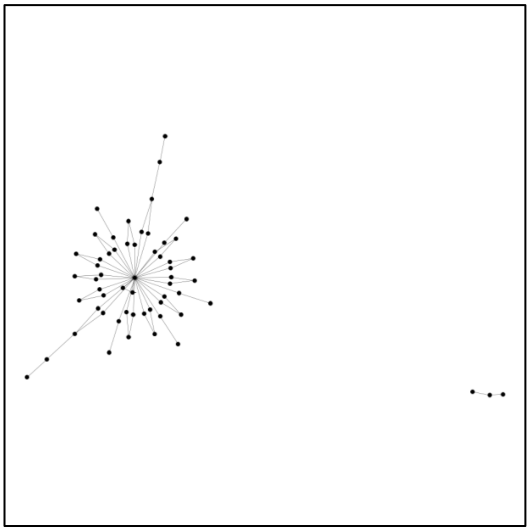


Figure 6: Processed Electronic Prescribing Server Port Mapping

The Patient Administration System (PAS) dataset is visualised in Figure 7. The PAS solution hosts all patient record demographics and information. For many hospitals (including the hospital profiled in this paper) the PAS also interfaces with a number of other key hospital systems, such as allowing accessing to Electronic CaseNotes (ECN) of a patient and other critical healthcare information. If an adversary targets a hospital, in order to illegally extract patient data and patient records, either out of curiosity or with the intent to blackmail the patient or the hospital, they would very likely start with the PAS server. Specific healthcare infrastructures have unique systems hosted on their own servers, within the same infrastructure. However, compromising the PAS server would be an effective way to leverage an attack on another server. It would provide access to the patients NHS number or hospital number, which links to every other system.

In Figure 8 the PAS system port mapping data has been processed by our system to remove low risk data. In this case, the visualisation clearly highlights the three small collections of ports mapped to one another in isolation, running an Unknown process.

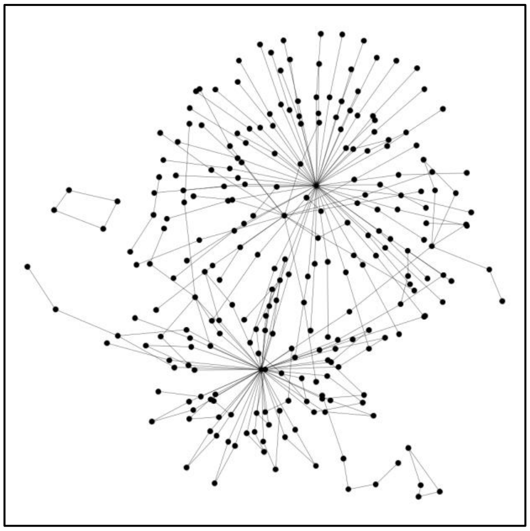


Figure 7: Patient Administration System Server Port Mapping

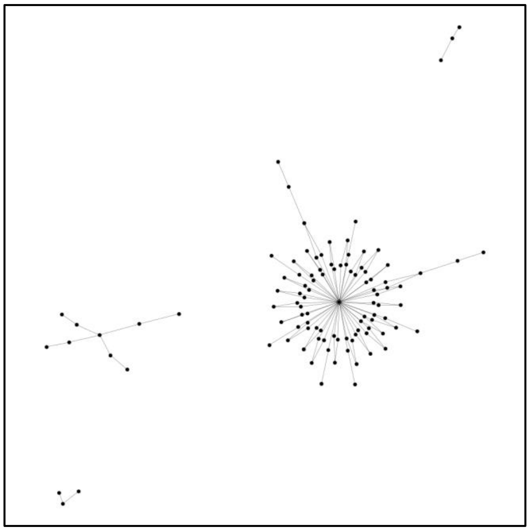


Figure 8: Processed Patient Administration System Server Port Mapping

This data should be investigated as a priority in order to understand which processes are running on these ports on the server.

5 CONCLUSION AND FUTURE WORK

The three datasets presented in this paper are identified as being the most valuable to a potential attacker. Depending on the attackers' intentions, compromising the Active Directory server would allow the adversary access to the core of the organisational infrastructure, including all user accounts, passwords and security groups. Compromising the Electronic Prescribing server would allow an attack to alter prescriptions and doses administered to a patient. And finally, compromising the PAS server would allow an attacker access to view and modify patient data. Port mapping servers is of crucial importance on hospital networks. Actively monitoring the ports for unusual activity is a huge task, but preparing and cleansing the data first highlights anomalous data activity to a cyber security analyst to mitigate the threat. With the assistance of machine learning algorithms leveraging the expertise on in-house knowledge can assist the IT department of hospitals to find the 'needle in a haystack' of a potential cyber-attack within their vast data infrastructure.

Future work will involve using datasets captured over a longer period of time. The dataset used in this paper represents a snapshot of data on three critical hospital servers. Future work will involve visualising data captured at select intervals, and cross reference the data across the various servers. In this way, the data can not only be profiled for malicious port mappings, suggesting that there is a potential attacker or malware on the hospital servers, but the system can also profile user behaviour, and flag unusual user behaviour to the IT Department. For example, if a user typically only logs into their account on weekdays, then if the account is logged in on a weekend, it may be an indication that the users' username and password has been compromised by an attacker. The attacker could either be illegally accessing hospital records, or searching for further vulnerabilities within the network in order to perform a privilege escalation attack.

Additionally, machine learning algorithms will be tested in order to automate the process once it has been refined. This will allow the process outlined in this paper to be performed on all 274 of the hospital's servers, and at regular intervals, in order to alert cyber security analysts of unusual port mappings shortly after they occur. Over time, the analyst will be order to provide feedback to the system through the use of supervised machine learning algorithms, and the algorithms will be refined and tailored to the unique threat landscape and infrastructure of the hospital.

REFERENCES

[1] R. Vargheese, Dynamic Protection for Critical Health Care Systems Using Cisco CWS: Unleashing the Power of Big Data Analytics, in *2014 Fifth International Conference on Computing for Geospatial Research and Application*, pp. 77–81, 2014.

[2] P. S. Mathew and A. S. Pillai, Big Data solutions in Healthcare: Problems and perspectives, in *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, pp. 1–6, 2015.

[3] S. M. Riazul Islam, M. Humaun Kabir, and M. Hossain, The Internet of Things for Health Care: A Comprehensive Survey, *IEEE Access*, vol. 3, pp. 678–708, 2015.

[4] W. Hurst and C. Dobbins, Guest Editorial Special Issue on: Big Data Analytics in Intelligent Systems, *J. Comput. Sci. Appl. Vol. 3, 2015, Pages 1-9*, vol. 3, no. 3A, pp. 1–9, 2015.

[5] D. Arney, K. K. Venkatasubramanian, O. Sokolsky, and I. Lee, Biomedical devices and systems security., *Conf. Proc. ... Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. IEEE Eng. Med. Biol. Soc. Annu. Conf.*, vol. 2011, pp. 2376–9, Jan. 2011.

[6] J. J. Walker, T. Jones, and R. Blount, Visualization, modeling and predictive analysis of cyber security attacks against cyber infrastructure-oriented systems, in *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, pp. 81–85, 2011.

[7] D. Jackson, A direct path to dependable software, *Commun. ACM*, vol. 52, no. 4, p. 78, Apr. 2009.

[8] R. van der Togt, E. J. van Lieshout, R. Hensbroek, E. Beinat, J. M. Binnekade, and P. J. M. Bakker, Electromagnetic interference from radio frequency identification inducing potentially hazardous incidents in critical care medical equipment., *JAMA*, vol. 299, no. 24, pp. 2884–90, Jun. 2008.

[9] J. Kim, B. J. Lee, and S. K. Yoo, Design of real-time encryption module for secure data protection of wearable healthcare devices., *Conf. Proc. ... Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. IEEE Eng. Med. Biol. Soc. Annu. Conf.*, vol. 2013, pp. 2283–6, Jan. 2013.

[10] R. Skowyra, S. Bahargam, and A. Bestavros, Software-Defined IDS for securing embedded mobile devices, in *2013 IEEE High Performance Extreme Computing Conference (HPEC)*, 2013, pp. 1–7.

[11] A. Sawand, S. Djahel, Z. Zhang, and F. Nait-Abdesselam, Multidisciplinary approaches to achieving efficient and trustworthy eHealth monitoring systems, in *2014 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 187–192, 2014.

[12] O. Kocabas, T. Soyata, and M. K. Aktas, Emerging Security Mechanisms for Medical Cyber Physical Systems, *IEEE/ACM Trans. Comput. Biol. Bioinforma.*, vol. 13, no. 3, pp. 401–416, May 2016.

[13] R. Mitchell and I.-R. Chen, Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber Physical Systems, *IEEE Trans. Dependable Secur. Comput.*, vol. 12, no. 1, pp. 16–30, Jan. 2015.

[14] Q. Shafi, Cyber Physical Systems Security: A Brief Survey, in *2012 12th International Conference on Computational Science and Its Applications* , pp. 146–150, 2012.

[15] D. B. Kramer *et al.*, Security and privacy qualities of medical devices: an analysis of FDA postmarket surveillance., *PLoS One*, vol. 7, no. 7, p. e40200, Jan. 2012.

[16] Q. Chen and J. Lambright, Towards Realizing a Self-Protecting Healthcare Information System, in *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, pp. 687–690, 2016.

[17] A. Boddy, W. Hurst, M. MacKay, and A. El Rhalibi, A Study into Detecting Anomalous Behaviours within HealthCare Infrastructures, *9th Int. Conf. Dev. eSystems Eng.*, 2016.

[18] Y. Hu, Efficient, High-Quality Force-Directed Graph Drawing, *Math. J.*, vol. 10, no. 1, pp. 37–71, 2005.