Securing Health Care Information Systems using Visualisation Techniques

Abstract

Health care information systems form the backbone of health care infrastructures and are increasingly reliant on medical devices to capture and transmit data. These devices, however, are vulnerable to attacks from the digital domain. The number of differing medical devices and information systems interacting with one another in new and increasingly less secure and disparate ways creates new challenges in information systems security. This work-in-progress paper presents a system design and methodology for modelling data interactions and data flow within the health care infrastructure. The system will increase situational awareness for users of information systems and promote stronger cyber security best practices and policies within this rapidly evolving landscape.

***Keywords**: Cyber-Security, Healthcare, Medical Devices, Visualisation*

1. Introduction

Critical information infrastructures lay the foundation for an advanced society. The safety, security and comfort of ordinary people rely on critical infrastructures every day. Food & water distribution, power supply, finance, military defence, manufacturing, transport, government services and healthcare (Merabti et al. 2011), are all notable examples of goods and services provided. These information infrastructures have become increasingly dependent on Information and Communication Technologies (ICT) to facilitate communication and automate services (Eusgeld & Nan 2009). However, as with any other network, the interconnected critical infrastructures are now more vulnerable to cyber-attackers. An attack on one infrastructure can have a direct impact on multiple others (Board 1998).

Critical infrastructures operate, and are increasingly being dispersed, over large geographic areas (Macdermott et al. 2013). The result is an increased vulnerability on critical infrastructures to cyber-attacks from external sources (Walker et al. 2011).

Healthcare is an essential part of the national critical infrastructure network (Chalmers et al. 2015). Of the four critical infrastructures (safety, mission, business and security), hospital infrastructures are a mission-critical infrastructure. Damage to network communications and the loss of patient data would have a detrimental impact on the health provision, potentially resulting in patient death or theft of sensitive data (Sawand et al. 2014). Additionally, many lifesaving medical devices, used by health care infrastructures, such as the NHS, are vulnerable to attacks from the digital domain. Pacemakers for example, are calibrated wirelessly and have none or very little security in place. Medical devices are often limited in their computational and

communication capabilities; with many being battery powered and tend to be used as sensors or actuators (Arney et al. 2011). Such devices are not built to accommodate computationally exhaustive operations (Riazul Islam et al. 2015). Similarly, most medical devices have low on-device memory, leading to the challenge that they are not able to execute complicated security protocols (Riazul Islam et al. 2015). Wireless links and open connections, present on medical devices, can also be compromised by attackers. Adversaries can then manipulate the data transmitted and received by the device, alter dosages, and even turn devices off, potentially putting patients' lives at risk. However, a notable concern is that a successful attack on a medical device, presents an opportunity for an attacker to gain backdoor access into a healthcare infrastructure. This essentially allows attackers to bypass the network authentication infrastructure required to access systems containing sensitive personal data.

Attacks on medical devices have been steadily increasing over the past 6-12 months; these attacks so far appear to be 'Proof of Concept' attacks. Their aim is to allow an attacker to gain more insight to the security in place on the infrastructure network, enabling a more precise and severe attack to be carried out at a later time. These attacks are often a challenge to identify, even after the attacks have happened, as there is very little monitoring or security available on these devices which track this information.

To address the lack of information about the rise in cyber-attacks on medical devices, this research investigates the growing concern of cyber-security for the critical health care infrastructure. The project examines the recent increase in attacks on the NHS network in particular; and proposes a methodology for visualising real-world network data in order to better understand cyber-attacks on healthcare networks.

In this concept paper, we present a system design and novel methodology to explore the use of visualisation techniques in addressing the need for enhanced cyber-security measures on healthcare devices. These devices are a known risk for the NHS network. The system will also identify how pattern recognition techniques can be used to analyse big data sets and find trends in patterns for cyber-attack visualisation purposes within the network.

The remainder of this paper is as follows. Section 2 presents a literature review of health care information systems security and medical device security visualisations.

Section 3 outlines the approach that will be used on the project, including the aims and its novel contributions. Section 4 presents the methodology of the project, the four stages of the project, the system design and a discussion of the expected challenges. Section 5 is a conclusion of the work in the paper and suggests ways in which the project will continue with future work.

2. Background Research

Infrastructures are relying increasingly on cyber-physical architectures (Halperin et al. 2008). The healthcare infrastructure, in particular, is taking advantage of the benefits brought through interconnected cyber networks. As such, the interest in medical device section has grown in recent years. Medical devices are now essential for modern medicine; they allow for automated patient monitoring and management functions (Arney et al. 2011)(Health and Social Care Information Centre n.d.). Additionally, medical devices are available for continuous use by patients and not restricted to within clinical settings. Their interconnectedness is increasing both directly and wirelessly to external entities. These factors have the potential to make healthcare accessible to everyone and to reduce costs. However, it also provides another opportunity for attackers to exploit externally secure networks.

2.1 The Problem

Wireless communications and sensor technologies are intrinsically vulnerable. Attackers are able to exploit weaknesses, in order to launch attacks. Medical devices, which have wireless technology as a core component, need to be secured and private otherwise patients would be reluctant to use them. Health-care devices experience frequent and unexpected interactions between devices and systems that could potentially contain malware (Arney et al. 2011). As these medical devices often have no safeguards, they are susceptible to cyber-attacks and buffer overflows. In November 2015 the Department of Health commissioned the Health and Social Care Information Centre (HSCIC) to develop a Care Computer Emergency Response Team (CareCERT) in order to combat this rising risk of cyber threats on health care (Health and Social Care Information Centre n.d.). Several devices have been proven to be affected in this way, such as Mechanical Ventilators, which have been victims of total switch-off and changes in ventilation rates. Other examples include Syringe Pumps, which have been completely stopped, External Pacemakers, which have

malfunctioned, and Renal Replacement Devices, which have also completely stopped all due to targeted cyber-attacks (van der Togt et al. 2008).

Device monitoring systems are highly automated; reducing user involvement in deployment, operation and management (Sawand et al. 2014). As such, security is crucial for the long term viability of networked medical devices (Arney et al. 2011), which have the potential to be tampered with, reprogrammed by unauthorized users or subject to device-specific attacks. Devices can be targeted though their firmware upgrades or through connections to the network interface when connected through remote attacks in addition to local attacks. For example, telemetry data of an implantable cardiac defibrillator can be reprogrammed remotely (Halperin et al. 2008).

There are obvious direct physical hazards for an attack on a healthcare device. However, privacy issues and backdoor access to a larger secure network are also significant concerns. Techniques such as '*eavesdropping*' on the communication links make use of medical devices to inject forged data into an externally secure network. Additionally, exploiting software vulnerabilities on the medical device monitoring system may open the door for attackers and compromise the whole system. Patient data can be compromised.

Similarly, infrastructural systems are transitioning from physical components using networked controllers to complete cyber-physical systems (CPS) (Venkitasubramaniam et al. 2015). The CPSs rely on the seamless integration of both modern communication and modern computation infrastructures with existing physical ones. The purpose of which is to far exceed present systems in capability, adaptability, durability and efficiency. And CPSs are rapidly approaching the point where they are the norm; with nearly 50 million networked as of July 2014 (Venkitasubramaniam et al. 2015). However the high transfer rate of data exposes these systems to security vulnerabilities in cyber communication. These cyber vulnerabilities are both critical, yet unfamiliar and rely on the interface between cyber and physical architectures (Venkitasubramaniam et al. 2015). The increasing reliance on wireless networks is an increasing reliance on a system which is less protected and has primitive defences.

Intrusion Detection Systems (IDSs) techniques for Medical Cyber Physical Systems (MCPSs) are still in their infancy (Mitchell & Chen 2015). Attacks are detected through recording state information for both local nodes and peers. This information is then updated to a state machine, which models the subject device. This state machine generates a detection when state information becomes malicious (Mitchell & Chen 2015). In practice, this means that if a heart rate component is reporting normal cardiac function, but the Cardiac Device (CD) is in defibrillator mode, then the IDS should report a detection instead. Wireless communication security is handled by contemporary secret key technology (such as PKI). This provides authentication, which prevents man-in-the-middle attacks.

Figure 1 presents an overview of a typical network infrastructure which enables remote access for hospital users. This approach allows doctors, clinicians and support staff to provide on-call work remotely. It also demonstrates, how security is external facing, has little focus on insider threats.

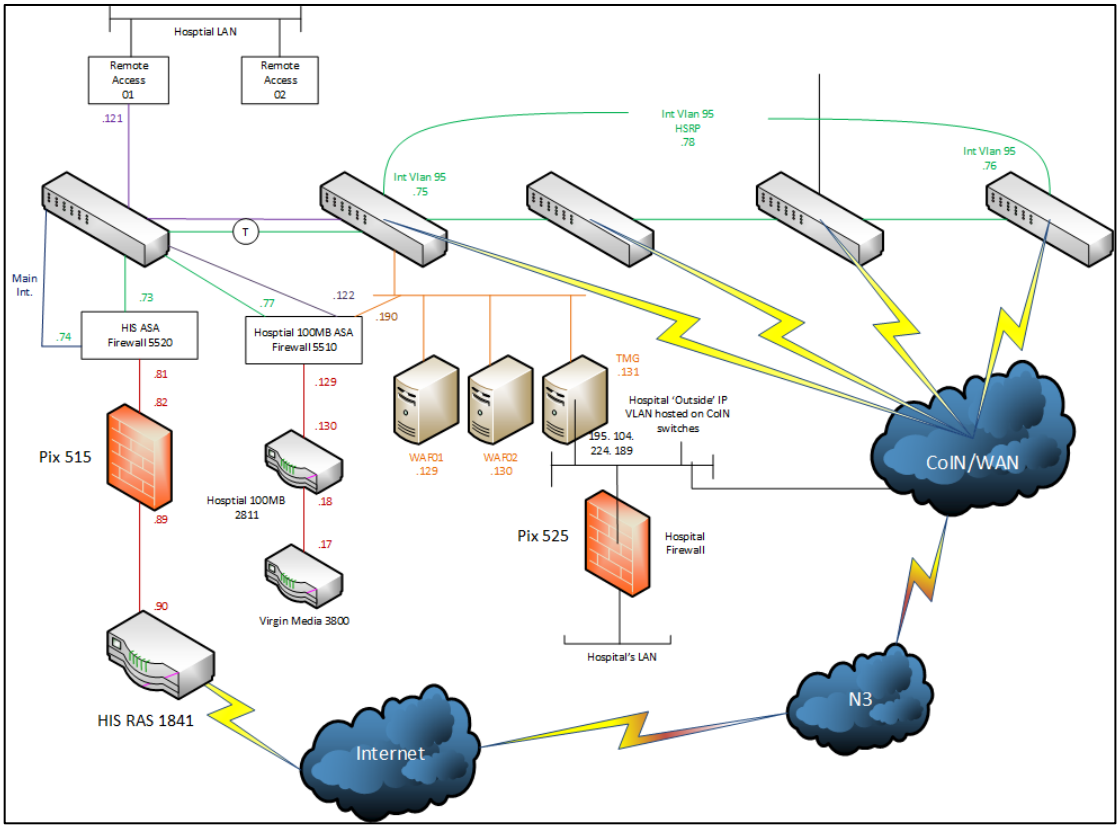

Figure 1. Remote Access

Novel vulnerabilities and threats will continue to be introduced due to the dynamic nature of the IoT and eHealth devices (Sawand et al. 2014). Cryptography based techniques (data encryption or cryptographic protocols) are commonly used to protect

medical data. However, this is often costly for health care providers (Sawand et al. 2014). More specifically, Figure 2. Critical Interface Diagram is the data infrastructure of a Hospital, showing the data flow process currently in place within the network.

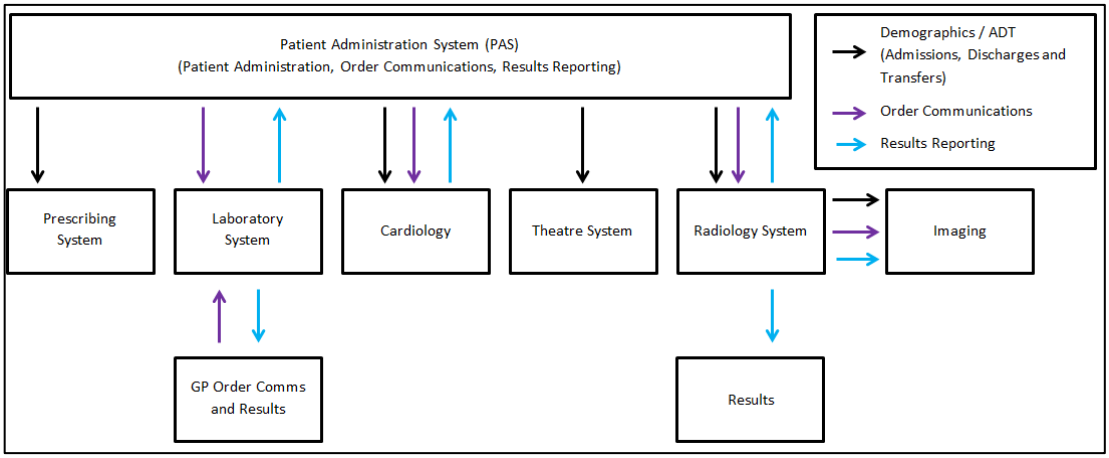

Figure 2. Critical Interface Diagram

2.2 Medical Technology

In addition to in-body medical devices, patient monitoring systems have cyber-vulnerabilities of their own. Draeger systems, for example, are medical devices for use in patient bedside care, which operate using a custom OS Shell running Windows XP/7. The system is currently installed in a number of hospitals throughout the UK (Draeger. 2016). This custom Windows shell is known as the Infinity Explorer (Draeger. 2016). For system security, the Draeger Omega system (see Figure 3. Draeger Technology (Draeger n.d. 2016)) uses Infinity Explorer Security, which is both Virus and Intrusion Protection, in addition to a Firewall. At present the majority of their systems are outward facing, meaning that they are resistant to external attack sources, yet vulnerable to insider attacks.

Draeger medical devices, including the Omega system, employ the use of a touch screen interface and customisable user interface for designed patient/diagnosis specific layouts. The intention of Draeger devices, as with most medical devices, is to provide the highest quality of patient care, by providing Data Accessibility, Integrity and Security. The Draeger ‘Omega’ system runs Windows XP, which is inherently vulnerable since it is no longer supported by Microsoft and its vulnerabilities are well known to attackers.

Figure 3. Draeger Technology (Draeger n.d. 2016)

Draeger Infinity Explorer is secured using the following approach:

- Firstly, the 'Software Firewall' mechanism is a security method which prevents intrusion and damage to the device and healthcare infrastructure which might be introduced through network services. Firewalls are a defence that aims to be proactive to damage and virus mitigation. They prevent damage from infection and intrusion rather than recover from it after an attack.
- Secondly, applying Microsoft Hotfixes, also known as QFE's (Quick Fix Engineering) is a mandatory security mechanism for the Infinity Explorer Security concept. These patches are analysed when released for applicability to the workstation. This is done as Draeger systems are mission-critical software systems. However, this does significantly delay their rollout to the devices, as they are incorporated into a new release, verified and validated before the customer is notified.
- Thirdly, Draeger Systems have the capability to accept removable media (in the case of the Omega system, this is in the form of USB Memory Sticks). The access to this file system can be restricted to the administrative user. However access to applications, fixed disks and removable disks is restricted to regular windows user rights by default, with certain user groups not having the permissions to add or delete files on disk. Similarly, booting from removable media can be disabled to prevent malicious code being executed on system boot which could potentially corrupt the workstation, however this feature needs to be enabled and is not enabled by default.

- Finally, the overall runtime system (the Draeger Watchdog) is a program that operates in an environment with regular windows user's rights with restrictions on file system access. The intension of the watchdog is that malicious code introduced by an intruder would not be executable under privileged rights. Applications available to the watchdog can be included by the administrator to be executed.

As the Infinity Explorer acts as a patient monitor and deals with real-time data it does not use antivirus. This is because, the antivirus software would take up resources needed by the Draeger Watchdog component. In response, the anti-virus would perceive the Watchdog as a virus trying to stop the service, and would subsequently attempt to shut down the Watchdog.

2.3 Related Research

A similar tool which uses visualisations to increase situational awareness of cyber-attacks and vulnerabilities is IPMatrix. IPMatrix is a visualization program that can find trends in IP Addresses in order to show patterns to allow administrators to predict attacks and prevent them (Ohno et al. 2005)(Koike et al. 2005). It's a simple visualization of Attacker IP Addresses, allowing the User to predict potentially vulnerable addresses at both site-level and at local level. Additionally IPMatrix3D is a piece of software in preliminary development that shows potential in expanding the Visualization capabilities of the tool (Koike et al. 2005). The main advantages of IPMatrix are that it visualizes IP addresses economically and allows the user to intuitively predict the proximity of an attack. However, the tool is limited due to the fact that there are unused IP Addresses on the visualization (Ohno et al. 2005). The Paper was published over 10 years ago, making its relevance to current work and Visualization techniques questionable.

Virtual Hospitals are occupying an emerging role in eHealth (Ahmed & Akhtar Raja 2013). Mobile Adhoc Networks (MANETs) in live monitoring and healthcare are becoming increasingly important in developing countries. Knowledge Based Systems (KBS) for E-Healthcare can enable huge amounts of information to be interacted with through the use of intelligent tools (Ahmed & Akhtar Raja 2013). Virtual Hospitals reduce the stress of going to a hospital for aged, indisposed or ailing patients. Additionally, they allow for ambulance workers to receive guidance from the hospital whilst a patient is being brought in for urgent treatment and make it possible for

hospital staff to make informed and appropriate advanced arrangements for the patient (Ahmed & Akhtar Raja 2013). Outsourcing Cloud Services to major providers such as Google and Amazon also relieves hospitals of the burden of major infrastructure and maintenance investments (Ahmed & Akhtar Raja 2013). The benefits of Cloud Healthcare are outlined in the context of Disaster Response Management (DRM) initiatives, allowing rescue workers to communicate with doctors and upload medical data for both parties to make informed decisions (Ahmed & Akhtar Raja 2013). The emergence of virtual hospitals, along with the increasing reliance on networked healthcare solutions, demonstrate that there is a clear need for further cyber security solutions to defend against cyber-attacks. Datasets become more valuable and enticing to attackers the larger they become and the more that healthcare infrastructures depend on them.

3. Approach

This project focusses on addressing the issues identified in the background section which highlights specific weaknesses within health care information systems and devices.

3.1 Aims

As such, the aim of this project is to address the cyber-vulnerabilities of medical devices, particularly within the NHS critical infrastructure network. The proposed research project will develop a system which analyses the data sets from various medical devices and employs data analysis and visualisation techniques to identify threats and vulnerabilities within healthcare networks. Specifically, the following aims for the proposed system are considered.

- Develop a system which analyses patterns and trends of data within healthcare networks.
- Employ the system to ascertain likely points of entry for attackers.
- Detecting vulnerabilities within medical devices.
- Detect compromised medical devices that are behaving erratically and a potential threat to the infrastructure as a whole through visualisation techniques.

The benefits of a system that analyses and visualises trends of medical data within the Critical Infrastructure are numerous. The system will provide valuable information as to where vulnerabilities are within the infrastructure so that solutions can be developed to patch them. The system will also allow the developers of medical devices to make more informed decisions about the design of their devices in order to make them less vulnerable to cyber-attacks.

The key objective of this research project is to develop a system which concerns the use of visualisation techniques to communicate complex health-care networks, exchange data and converse attack movement.

3.2 Project Novelties

The proposed research project will have the following novel contributions:

- The development of a system which is able to automatically analyse medical device data and present it as a visualisation will be novel. The system will allow the operator valuable insight into the flow of data within the critical infrastructure network and allow patterns and trends to be discerned and potential vulnerabilities predicted. The visualization will aid the operator in their situational awareness; allowing them to foresee potential cyber vulnerabilities and security risks through improved recognition and response to evolving events. From our research to-date, no system is able to analyse and visualise healthcare networks in real-time for the detection of cyber-threats in medical devices.
- The system will involve the implementation and development of new algorithms in order for the system to identify these complex patterns and readings. In addition, the system will make use of a novel application of existing machine learning techniques by applying the approach to a healthcare visualisation setting.
- The system will provide personalised feedback to individual healthcare infrastructures networks, meaning the system will be generic and adaptable to different healthcare infrastructure environments.

4.0 Methodology

In this section, the project methodology is presented. This will include the four stages of the project, the proposed system design, and a discussion of the potential challenges the project may face.

4.1 Methodology Stages

The methodology includes, firstly, the assessment of real world big data sets collected from within a healthcare infrastructure. The analysis process has the goal of identifying how attacks perform and modelling infrastructure behaviour in high detail.

The second phase will include the engagement of data visualisation techniques to envision both, the generation and effects of cyber-attacks on a network, and the changes occurring in a system when an attack is taking place. The output will also be used to educate and create awareness between stakeholders and communicate knowledge of existing threats in order to improve health care infrastructure security. This stage will be evaluated through a target end-user group.

Thirdly, the expected outcome of the project will be a novel framework for a plug-in system capable of autonomously generating visualisations of cyber-attacks and critical infrastructure behaviours. As cyber-attacks on medical devices in the Healthcare Infrastructures have been increasing within the last six months (BBC 2015), the research is timely and directly applicable to a real-world environment. Specifically, the system will use data collected from medical devices to analyse patterns of data for points of entry from attackers, detect vulnerabilities of medical devices and detect medical devices that are behaving erratically and are therefore compromised and pose a potential threat. This approach is depicted in Figure 4.

- .

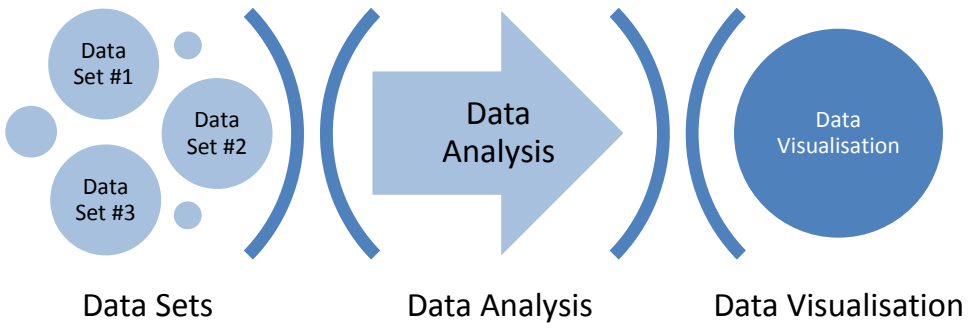

Figure 4. The Proposed Process

4.2 System Design

Figure 5 presents the framework for the proposed system. Real-time data is extracted from information systems and processed, through different stages, when it is displayed as a visualisation through a user interface.

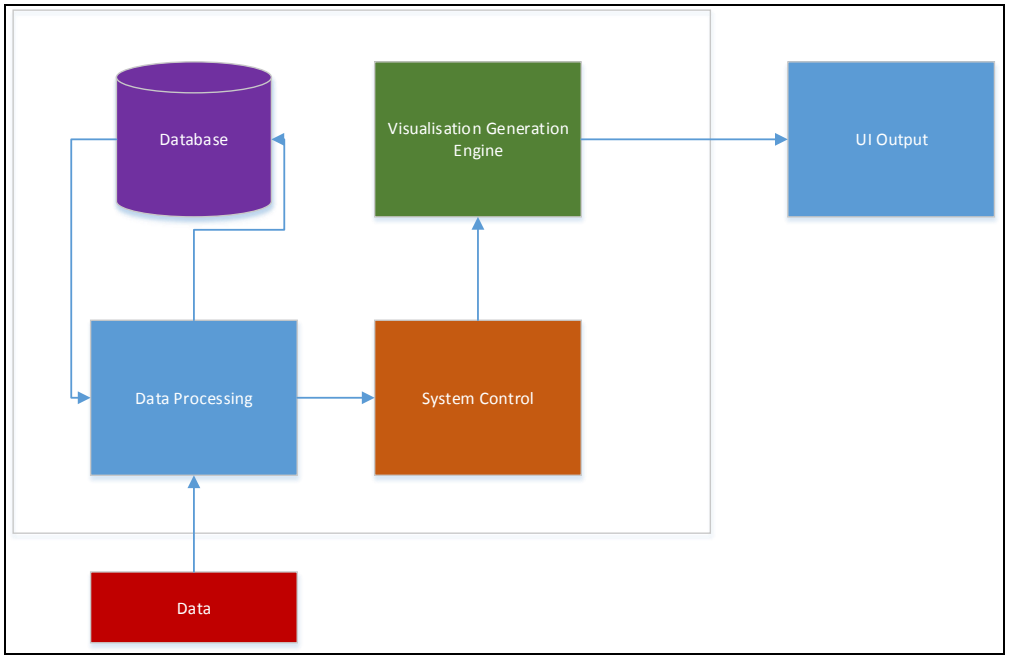

Figure 5. The Proposed Framework

Each of the components in the framework are explained as follows:

- Data: The proposed framework includes investigated methods for acquiring critical infrastructure attack data for serious game development. The data will be acquired from the newly established HSCIC Care Computer Emergency Response Team (CareCERT) (Health and Social Care Information Centre 2016). CareCERT was launched in January 2016 and is funded by the Cabinet Office National Security Programme and provides cyber security expertise to healthcare organisations in the form of providing information regarding cyber vulnerabilities, mitigating risks and advising appropriate reactions to national cyber security attacks.

- Data Processing: This component of the framework processes the data to ensure that irrelevant data is removed from the datasets. This will safeguard that only pertinent, useful data is included in the analysis stage.

- Database: The database will store the datasets when not being called on by other components of the framework. The database will also store patterns of known attack behaviours for the datasets to be compared against. This will allow the operator to recognise potentially malicious data and investigate further through manipulation of the visualisation.

- System Control: The system control regulates the operations of the visualisation and notifies the data manager to perform data processing functions. The system control is required to execute a variety of function, which include several key aspects, such as:
    - Instructing the data manager to either start or stop data collection
    - Allowing the operator to input data collection requirements
    - Allowing the operator to manipulate the visualisation of the display in order to gain additional perspectives on the data.
- Visualisation Generation Engine: This component generates visualisations as instructed by the system control. The component can accurately and effectively showcase the network of information systems and identify data relationships and patterns. The visualisation can pinpoint erratic and unusual data behaviour within the datasets to assist in cyber-attack detection.
- UI Output: This is the output shown to the operator. The output increases the operator's situational awareness of the data flow within the information systems of the health care infrastructure.

4.3 Summary

The seriousness of critical information infrastructure protection is a key issue. Their vulnerability to the growing cyber-threat enforces this further. Using the approach put forward in the paper to identify system threats within health care networks, a layer of security is added to the defence in depth approach currently in place.

Health care information systems are the most integral component of the health care critical infrastructure. Additionally, it is well known that the dangers of cyber-crime increase exponentially with the number of interconnected computers and devices. Therefore the increasing reliance on medical devices for data capture and transmission is an increasing reliance on devices vulnerable to attacks from the cyber domain.

5. Conclusion and Future Work

Health care data is an extremely attractive target for a cyber-criminal, the compromise of this data could lead to severe loss of patient privacy or the tampering and malicious falsifying of data could even lead to patient death. Therefore, unique analysis and reporting tools need to be developed to combat the increasing risk of data compromise

and a focus on cyber security innovations is required to maintain patient trust in digital health care innovations.

In this paper, a framework for a visualisation system to increase situational awareness for cyber security experts within health care infrastructures is proposed. Through creating a visualisation of data flow of the information systems used in the health care infrastructure the system will allow the operator to more accurately predict potential cyber vulnerabilities within its systems, cyber-attacks and implement a set of cyber security best practices and policies through a unique and novel data analysis and visualisation tool. The system will further knowledge and understanding of health care information systems and aim to prevent data compromise from within them.

In our future work, we will begin to design and test the visualisation framework and system with simulated data. Once the visualisation has passed initial the implementation stage the team will work with industry to ultimately use real-world data and analysing its vulnerabilities.

References

Ahmed, S. & Akhtar Raja, M.Y., 2013. Role of social networking in patient monitoring and E-healthcare. In *2013 High Capacity Optical Networks and Emerging/Enabling Technologies*. IEEE, pp. 98–103. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6729765 [Accessed December 17, 2015].

Arney, D. et al., 2011. Biomedical devices and systems security. *Conference proceedings : ... Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Annual Conference*, 2011, pp.2376–9. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6090663 [Accessed January 27, 2016].

BBC, Medical devices vulnerable to hackers - BBC News. Available at: http://www.bbc.co.uk/news/technology-34390165 [Accessed December 16, 2015].

Board, E., 1998. Critical Infrastructure Protection VIII. In J. B. jonathan. butts@afit. ed. (1) & S. S. sujeet@utulsa. ed. (2), eds. *Critical Infrastructure Protection VIII, A Survey of Critical Infrastructure Security ,8th IFIP WG 11.10 International Conference*. Liverpool, United Kingdom: Springer Berlin Heidelberg, p. 203p. Available at: http://link.springer.com/chapter/10.1007/978-3-662-45355-1_9.

Chalmers, C. et al., 2015. Smart Meter Profiling For Health Applications. In *The Internal Joint Conference on Neural Networks*. IEEE, pp. 1–7. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=7280836 [Accessed November 30, 2015].

Draeger, Infinity® Omega Solution. Available at: http://www.draeger.com/sites/en_uk/Pages/Hospital/Infinity-Omega-Solution.aspx [Accessed February 21, 2016a].

Draeger, Medical division. Available at: http://www.draeger.com/sites/en_corp/Pages/investor-relations/Medical-division.aspx [Accessed February 21, 2016b].

Eusgeld, I. & Nan, C., 2009. Creating a simulation environment for critical infrastructure interdependencies study. In *2009 IEEE International Conference on Industrial Engineering and Engineering Management*. IEEE, pp. 2104–2108. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5373155

[Accessed February 29, 2016].

Halperin, D. et al., 2008. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, pp. 129–142. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=4531149 [Accessed January 19, 2016].

Health and Social Care Information Centre, 1 Trevelyan Square, Boar Lane, Leeds, LS1 6AE, United Kingdom, Cyber Security Programme (CSP) CareCERT Project. Available at: http://www.hscic.gov.uk/carecert [Accessed February 21, 2016].

Koike, H., Ohno, K. & Koizumi, K., 2005. Visualizing cyber attacks using IP matrix. In *IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05).* IEEE, pp. 91–98. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1532070 [Accessed December 15, 2015].

Macdermott, Á. et al., 2013. Considering an elastic scaling model for cloud Security. In *2013 8th International Conference for Internet Technology and Secured Transactions, ICITST 2013*. IEEE, pp. 150–155. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6750181 [Accessed November 30, 2015].

Merabti, M., Kennedy, M. & Hurst, W., 2011. Critical infrastructure protection: A 21st century challenge. In *2011 International Conference on Communications and Information Technology (ICCIT)*. IEEE, pp. 1–6. Available at: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5762681 [Accessed November 30, 2015].

Mitchell, R. & Chen, I.-R., 2015. Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber Physical Systems. *IEEE Transactions on Dependable and Secure Computing*, 12(1), pp.16–30. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6774867 [Accessed January 12, 2016].

Ohno, K., Koike, H. & Koizumi, K., 2005. IPMatrix: An effective visualization framework for cyber threat monitoring. In *Proceedings of the International Conference on Information Visualisation*. IEEE, pp. 678–685. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=1509147 [Accessed December 15, 2015].

Riazul Islam, S.M., Humaun Kabir, M. & Hossain, M., 2015. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*, 3, pp.678–708. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7113786 [Accessed October 24, 2015].

Sawand, A. et al., 2014. Multidisciplinary approaches to achieving efficient and trustworthy eHealth monitoring systems. In *2014 IEEE/CIC International Conference on Communications in China (ICCC)*. IEEE, pp. 187–192. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=7008269 [Accessed December 15, 2015].

van der Togt, R. et al., 2008. Electromagnetic interference from radio frequency identification inducing potentially hazardous incidents in critical care medical equipment. *JAMA*, 299(24), pp.2884–90. Available at: http://jama.jamanetwork.com/article.aspx?articleid=182113 [Accessed January 27, 2016].

Venkitasubramaniam, P., Yao, J. & Pradhan, P., 2015. Information-Theoretic Security in Stochastic Control Systems. *Proceedings of the IEEE*, 103(10), pp.1914–1931. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=7270416 [Accessed January 24, 2016].

Walker, J.J., Jones, T. & Blount, R., 2011. 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)*. IEEE, pp. 81–85. Available at: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6107851 [Accessed December 15, 2015].