TALLINN UNIVERSITY OF TECHNOLOGY
Faculty of Information Technology
Department of Computer Science
TUT Center for Digital Forensics and Cyber Security

ITC70LT

Mobolarinwa Taofeek Balogun IVCM156308

A COMPARATIVE ANALYSIS OF HEALTHCARE SYSTEM IOT AND INDUSTRIAL SCADA IOT FOR CYBERTERRORISM

Master thesis

Supervisor: Hayredtin Bahsi
PhD
Senior Research Scientist

Tallinn 2017

Author’s declaration of originality

Author’s declaration of originality is an essential and compulsory part of every thesis. It always follows the title page. The statement of author’s declaration of originality is presented as follows:

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: [Mobolarinwa T Balogun]

[18.05.17]

Abstract

We aim to compare a cyber-attack towards a Healthcare system that can create a physical result with an Industrial SCADA system and then find out if the same level of sophistication is required for the attack. We used an attack tree to access the required sophistication levels of threat actors for integrity attacks against two IoT Infrastructures: The Healthcare IoT and the Industrial SCADA IoT. We can see that there is a similarity between them in terms of technology and attack surface. While several cybersecurity researches on cyber-attacks and their analysis have been made regarding Industrial SCADA systems, there have only been a few security reports about Healthcare IoT infrastructure. The STUXNET attack have proven that it is possible for attacker to create a physical result via an attack on an Industrial system. Nick Depaula and Sanjay Goel in their paper regarding cyber incident sophistication index, listed the attack as one with the highest sophistication index i.e. 5 out of 5. We adopted the MITRE's cyber prep methodology which helps us to describe the capabilities of the adversaries more granularly. We also adopted Nick Depaula and Sanjay Goel's methodology to generate a sophistical index for our attack scenarios.

This thesis is written in English and is 78 pages long, including 6 chapters, 8 figures and 16 tables.

Keywords: SCADA, Internet of things, Cyber terrorism, Attack Trees, Attack sophistication.

Annotatsioon

Meie eesmärgiks on võrrelda tervishoiusüsteemile suunatud küberrünnakut, mis võib tuua kaasa füüsilisi tagajärgi, tööstusliku SCADA ehk järelevalve ja andmete kogumise süsteemiga ning selle tulemusel teada saada, kas rünnak peab olema sama keerulisel tasemel. Me kasutasime ründepuud, et luua ligipääs kahe värkvõrksüsteemi – tervishoiu värkvõrgu ja tööstusliku SCADA värkvõrgu – terviklikkuse ründamiseks vajalike ohustajate keerukuse tasemele. Me võime näha, et seal on seos tehnoloogia ja ründepinna vahel. Kuigi mitmed küberkaitse uurimustööd küberrünnete ning nende analüüsid on tehtud tööstuslike SCADA süsteemide kohta, siis ainult üksikuid uurimistöö tulemusi võib leida tervishoiu värkvõrgu taristu kohta. STUXNET rünnak tõestas, et ründajal on võimalik tööstusliku süsteemi rünnates teha füüsilist kahju. Nick Depaula ja Sanjay Goel´i uurimustöös küber intsidentide keerukuse tasemete kohta märkisid nad antud ründe kõrgeimaks keerukusastmeks ehk 5-st 5. Kohaldasime Mitre Cyper prep metodoloogiat, mis aitab kirjeldada vastase võimeid granulaarsemalt. Samuti kohaldasime Nick Depaula ja Sanjay Goel metodoloogiat, et genereerida keerukuse loend meie ründestsenaariumidele.

Lõputöö on kirjutatud Inglise keeles ning sisaldab teksti 78 leheküljel, 6 peatükki, 8 joonist, 16 tabelit.

Võtmesõnad: SCADA, värkvõrk, küberterrorism, ründepuud, ründe keerukus

Table of abbreviations and terms

DDOS – Distributed Denial of Service

DICOM – Digital Imaging and Communication in Medicine

ECG / EKG – Electrocardiogram

EHR – Electronic Health Record

FCC – Federal Communication Commission

HIS – Health Information Service

HMI – Human Machine Interface

LINAC – Linear Accelerator

MRI – Magnetic Resonance Imaging

PLC – Programmable Logic Controller

SCADA – Supervisory Control and Data Acquisition

SI – Sophistication Index

Table of Contents

List of Figures

List of tables

1. Introduction

The unending developments in technology have undoubtedly improved the efficiency and effectiveness of industrial processes and the delivery of health services. Jobs which would have taken longer time and effortful workforce have now been taken over by devices that are networked together to achieve the same goal and even do them better. People in the healthcare now rely on IT systems including mobile devices (Implantable or external) to make monitoring of patients easier, and delivery of services are now more automated. These connected devices called the Internet of Things (IoT) have increased significantly when it comes to importance, numbers and value over the years [1].

Despite the huge benefits of these systems, there is a possibility that these devices can be used by malicious cyber agents as a tool to endanger the system itself and the human existence. A highly motivated individual or group of people with cyberterrorism goal will endanger human lives and property by disrupting services offered by critical infrastructures e.g. Health IoT Infrastructure. By endangering human life, we mean causing panic, bodily injury, health risk, or death. Satisfaction for these set of people comes from using connected computing infrastructure to cause a physical impact on the environment.

Although different cyber-attacks have already been aimed towards the healthcare IOT Infrastructure, for this research we will like to make sure that an attack which will result in a physical impact will be studied. Drug infusion pumps have been known to be very reliable and helpful for clinicians and patients as it provides safe and accurate administration of medications and fluids [2]. Suppose the motive of an attacker were to change from financial gains to modifying the infusion rate of an infusion pump, modifying the device configuration, sending malicious commands or just interfering with the device communication. The attacker can also decide to gain physical or remote access to an electronic health record (EHR) server to modify the patient's records such as blood type, dosage type, therapy session, etc. All these can be lead to disastrous events and can as well cause panic within a society especially if the event is unexpected or proper control measures are not in place.

An alternative industry relevant for this comparative study is one that operates the industrial SCADA system. Rigorous security research was not done when SCADA systems were earlier

implemented [3]. This has resulted in many security issues faced today. The physical impact that was a result of STUXNET in 2010 was unexpected by the industry. In fact, after this event, politicians and security analysts became more concerned regarding the sophistication of attacks [4].

To compare both IoT infrastructures, we adopt the use of attack tree modeling which helps us to understand an attack from the attacker perspective [5]. Case scenarios were created from documentations and reports regarding cyber-attacks that could cause a physical result to industrial SCADA infrastructure and the Healthcare IoT infrastructure. We assigned values to the indictors related to attack sophistication that are described in [6] and use it to categorize the adversary capabilities. We also used a sophistication index categorization as applied in [7] to measure the attack sophistication level of different attack scenarios.

1.1. Motivation

Many of the current analysis regarding cyberterrorism has been on Industrial Control Systems and critical infrastructures. The report in [8] discusses the use of the cyberspace to conduct an attack on a critical infrastructure to generate a physical impact by focusing on the STUXNET attack in 2010. There is also an analysis on some known attacks that could be categorized as being organized by a well-motivated cyberterrorist group [9]. According to [10], cyberterrorism is not a near threat due to the sophistication that is needed to carry out the attack. Also, terrorist organizations do not have the required capability, attacks are expensive to coordinate, easy to neutralize and less desirable for terrorist organizations [10].

The past few years have seen an uphill in the number of cyber-attacks towards the healthcare industry. There is a fear that should the motive of the cyber attacker change into perpetuating an attack to cause a physical result; the consequences can be calamitous. We may just be a few years away from this, so it is important to analyze the feasibility of the attack, the threat capabilities and the sophistication of a possible cyber-attack. There have already been signs of an impending attack. An Islamic group related to ISIS defaced the United Kingdom NHS website earlier this year to express their dissatisfaction towards the unrest in the middle east [11]. There has also been an

increase in ransomware attacks, with the healthcare industry experiencing 88% of the attacks alone [12] [13].

1.2. Scope

Apart from a ransomware attack being a source of extortion to attackers, personal health records are also valuable, and denial of medical service to inward and outward patients can be worrisome. We are aware that terrorists organisations can have relevant capabilities to carry out this attack but dealing with this is another issue. We do not consider denial of service or confidentiality attacks in our analysis but focus mainly on integrity attacks that create a physical result. However, the result of this thesis can be an input for the relevance of terrorist's threat. We understand that cyber-attacks are also suitable to create chaos but we do not deal with this fact in our thesis as this is another discussion. Although a terrorist can combine a cyber-attack with physical attack to increase the chaos. For this thesis, our aim is to analyse the sophistication of an attack to an IoT infrastructure and so we do not consider the use of insider in our analysis. This thesis does not aim to point out if the terrorist organization have the relevant strength against attack on IoT applications but emphasizes on the required sophistication necessary to carry out attacks that can generate physical results.

1.3. Research Questions

This thesis aim to answer the following questions:

i. What level of sophistication is required to compromise a healthcare IOT infrastructure and cause a physical result to the system, its environment or the entities using the system?
ii. Do cyber-attacks that can cause a physical result on healthcare IOT Infrastructure require less sophistication than cyber-attacks with the same intent on an industrial SCADA infrastructure?

1.4. Research Contribution

This outcome of this thesis can be used as an inference that yes, critical infrastructures may require a higher level of attack sophistication. Meanwhile, IoT applications like health monitoring systems can also be a target of cyber terrorists if the required sophistication level to use them for physical damage is low and it can be affordable by terrorist organisations. This result of this research can be used to understand further the capabilities posed by threats to health IOT infrastructure and an industrial IOT infrastructure. At the end of this thesis, an attack tree for a Healthcare IoT infrastructure was created. This can be further used to build defences based on the different threat levels that we considered in this paper.

1.5. Limitations and Challenges

Although this research has several limitations, we did our best to maximise the resources we could lay our hands on. We developed an attack tree showing an attack on a Healthcare IoT Infrastructure and then compared it with an attack tree showing an attack on an Industrial SCADA Infrastructure. Although both attacks show that the attackers goal was to cause a physical result, there was a challenge of having similar comparison constraints. This is because an Industrial SCADA infrastructure can be attacked through the SCADA master or through the PLC connected to the field devices. we needed to look for a separate attack tree based on a SCADA system attack. Adding an attack scenario where there is a remote attack on the field devices via the PLC will be a more viable comparison. This is because PLCs are connected to the field devices like sensors and actuators just as a drug infusion pump is connected to the sensor connected human body. Meanwhile, there is a limited research on attacks to the SCADA system through the PLC. This would be a separate research on its own. Another major challenge of this thesis is assigning values to the nodes of each leaf of the attack tree. Since, we were unable to get an expert knowledge using a questionnaire, we did our best to use references from viable online sources that provided details of the attack type. Sources like MITRE's Common Attack Pattern Enumeration and Classification (CAPEC) and Common Weakness Enumeration (CWE) helped to identify the values of some of the indicators.

1.6. Thesis Structure

This thesis report is organized as follows. Chapter 2 discusses the background knowledge of this work including a study of potential adversaries, architecture of SCADA and healthcare IoT Infrastructure, reported attacks to the healthcare system and security issues of SCADA and healthcare IoT Infrastructure. In chapter 3, we discussed a selected literature that is related to the research. Chapter 4 discusses about how we solved the research problem. We started off by trying to describe the system and threat model as well as explaining the attack scenarios. We also introduced the securlTree which was the tool used in creating and analysing the attack tree. In chapter 5, we generated and analysed the data which is a combination of the attack indicators and the corresponding values of the leaves of the attack tree. We also compared the results of both systems to reach a conclusion. Chapter 6 shows our conclusions.

2. Background

2.1. Healthcare IoT Infrastructure Architecture

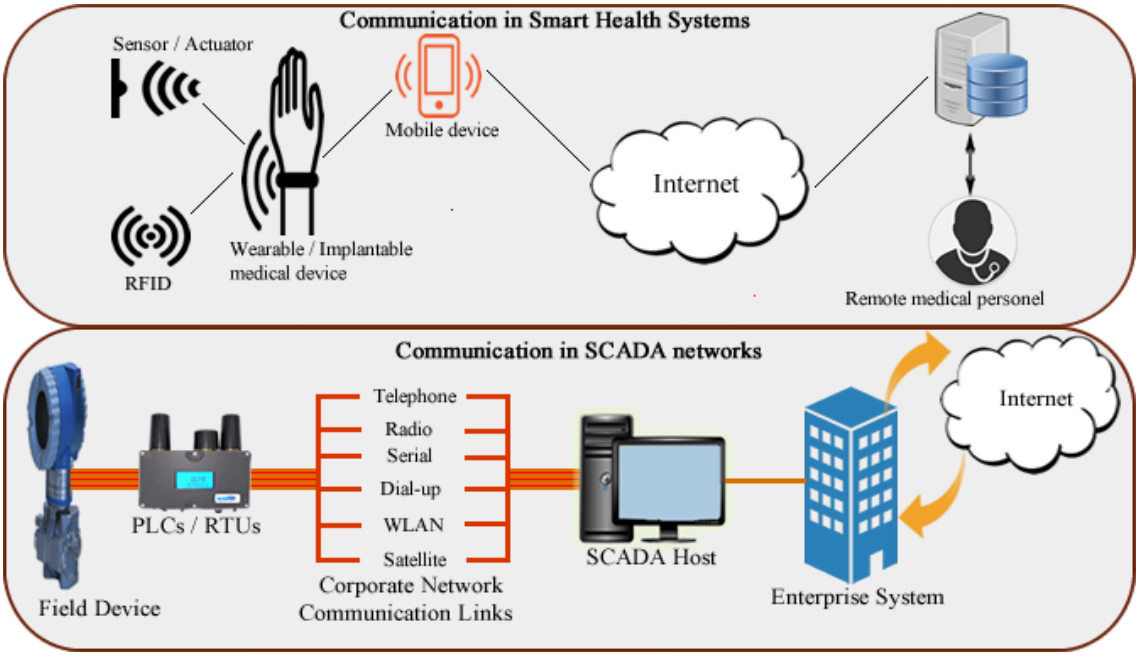


Figure 1 Diagrammatical comparison of Smart Health Systems and SCADA Networks (Healthcare IoT image adopted from m-health technology network architecture [14] and SCADA network architecture adapted from [15])

The components of the healthcare IoT consists of an Information perception layer that is responsible for collecting physiological parametric data such as temperature, blood pressure, oxygen saturation, heartbeat rate, etc. of patients. The data collection is by sensors or actuators that are connected to medical wearables or implantable devices fixed into the human body. This collected data is transmitted via wireless sensor network technologies like infrared, Bluetooth, NFC, etc. to a dedicated device such as a mobile phone, dedicated monitor or home computer that is then used to aggregate the data. Once the data is collected and aggregated, it is transferred to the network transmission layer that is responsible for carrying the data to the application layer that includes a remote healthcare information system (HIS) service [16]. Conventional internet technologies such as data networks, wired or wireless connection are used in transmitting the data. The collected information is then processed at the application layer and sent back via the same communication channel to the patient.

We see from the described communication flow that every layer of the architecture has a potential to be exploited because they all serve as entry points into the system. If incorrect data is sent to the application layer and if appropriate data correlation techniques are not implemented and erroneous data gets undetected, then there is a possibility that a patient's life can be in danger. Also, if the functioning of a health information system (server) that returns a processed data to the client is tampered with, the patient still gets exposed to danger. The communication channel that transmits data from the patient to the remote HIS can also be an entry point to intercept the data that is being communicated. An attacker may gain remote or physical access to the HIS to modify the data that is being sent or better servers can be affected by a denial of service attack or even ransomware attacks which have been a common trend in healthcare IoT industry within the last two years.

2.2. Industrial SCADA IoT infrastructure Architecture

The components of a SCADA system consist of sensors and actuators which are responsible for collecting physical parametric data from field devices. These signals are usually stored in an analogue format and are converted using a Remote Terminal Unit, Programmable Logic Controllers or Intelligent electronic device (IED) [17]. Once the data is converted, they are transmitted via a communication channel to the SCADA presentation and control unit where the collected data is processed, and operations are transmitted back to the devices on the field.

The SCADA control uses a Human Machine Interface (HMI) that is responsible for presenting the collected data to the operator in a human readable form. However, there is a further expansion of the architecture in situations where we have an operator outside the industrial network area who is trying to control the devices from remote locations. Communication between the field devices and the SCADA host can be via dial-up, satellite, serial, radio, telephone, or WLAN [17]. Also, specialised communication protocols like DNP, DNP3, ICCP, MODBUS, and ProfiBus etc. are adopted within the SCADA network [18]. Because some of these protocols existed over 20 years ago when security was not much of a problem, the focus was on efficient operation and not security [3].

With up to 4 layers (collection, conversion, communication and control) within the SCADA system, we see that any of the layers can be used as an attack entry point into the system [18]. A

physical attack where the field devices are adjusted by an attacker or a malicious insider changes the data that is sent to the HMI. Some of the popular protocols that are still used till date do not include authenticity and encryption during their development, and these shortcomings can be exploited in intercepting the data that is transferred between the devices. Operational errors from insiders or lack of proper access management can leave the HMI vulnerable and malicious attacker can exploit HMI vulnerabilities to interfere with industrial processes.

2.3. Healthcare IoT Threat Actors

2.3.1. Script Kiddies / Hobbyist

These group of adversaries are known to be the most underrated set of cyber attackers. This is due to the nonchalant way they go about carrying out their operations. The intensity of their attacks is usually low and their attacks lack a strategic objective with little or no financial or political motivation. This does not mean that the effect of their attacks cannot result in catastrophic results. Script kiddies rely on tools and malware that has been prepared by other attackers, and they lack the underlying cyber knowledge and understanding of how the tool is created [19].

Due to the increase in availability of connected IOT devices, script kiddies now have a broader attack surface to carry out their operations. A script kiddy can try to exploit a healthcare system if the target system fails to patch known vulnerabilities or if the attacker possesses a zero-day exploit [19]. Script kiddies are motivated by curiosity, and wanting to know how things work. They want to try new things but eventually do not usually aim to cause an attack that can create a physical result. However, if they can intrude a system they may not be aware of the extent of damage that can be caused. For example, a script kiddie can learn that bringing a magnetic field close to an implantable medical device can cause a distortion of the communication link between the IMD like a pacemaker or an implantable cardiac defibrillator and its controller [20]. This can possibly lead to a denial of service attack to the IMD device [20]. This though sounds simple; a curious script kiddie might place one close to his sick grandmother just for the sake of knowing how a magnetic interference can be possible.

2.3.2. Disgruntled Employee / Malicious Insiders

These group of adversaries tend to pose the largest threat to a system. This is due to their vast knowledge of how the system works and their unsuspecting and unrestricted access to the system. The do not need to possess vast cyber knowledge or technical skills to carry out an attack but may carry out an attack based on an unintentional or intentional motive.

2.3.3. Hacktivist

These set of attackers are more politically motivated. They aim to carry out attacks against individual and governmental organisations who are opposing views to their political agenda. As part of their political agenda, if necessary, they may also conduct cyber terrorism attacks [19]. The results of their attack are enough to express their political propaganda via the resulting media attention and possible political backlash [19]. A hacktivist group could consist of a set of script kiddies and other more experienced black hats hackers. To express their political propaganda, hacktivists can coordinate a denial of service attack against a health care system or they may decide to steal health data of high profile individuals in the government and in turn, reveal them to the public. One of the current high-profile hacktivist group is called Anonymous.

In April 2014, a DDOS attack against the Boston's children hospital was attributed to the Anonymous group, although there was no evidence available to ascertain the claim [19] [21] [22]. It was further revealed in [22] [21] that the cause of the attack was related to a Massachusetts protective service child custody case that involves a 15-year-old with a complex diagnosis. Although no casualty arose because of the attack, it was a wake-up call to the healthcare infrastructure as per what could have been if the goal of the attackers were to be more catastrophic.

2.3.4. Cyber Criminal

These set of attackers are financially motivated. Their goal of their attacks is to make money either by threatening to disclose confidential information or by selling stolen data. They consist of script kiddies and more experienced black hat hackers. Contrary to the other threat actors, cybercriminals get their money from buying and selling of intellectual property and confidential information, and extortion due to data hostage via a ransomware attack [19].

One of the high-profile cyber-attacks to the critical healthcare infrastructure was one involving the Hollywood Presbyterian Medical Center where the attackers after encrypting hospital data with a ransomware demanded 3.4 million dollars in Bitcoins to decrypt the data [23]. The hospital had reverted to fax machines, pen and paper which slowed down the usual operations of the hospital. Eventually, 17,000 USD was paid to the cyber criminals to get the data back [24]. Apart from health data servers, critical health assets like ECG, MRI, etc. and mHealth devices can also be prone to ransomware attacks [19].

2.3.5. Cyber Terrorist

This group of attackers are intent on using the dependencies of critical infrastructures on information technology and connected devices to cause physical or psychological harm [25]. Cyber terrorists are not motivated by financial gains but by the rate of havoc that they can cause to human lives and property [26]. Compared to other adversaries, cyber terrorists are mainly concerned with conducting attacks that create physical results.

Recently, it was reported that there was a cyber-attack on the United Kingdom's National Health Service (NHS) website by a group of Islamic hackers linked to ISIS [27] [11]. The attack although exposed the security flaws in the website, the attackers only manage to post graphic images of their intent on the site's homepage [11]. The NHS website contains a vast content of health data which was declared vulnerable during the attack. Although no harm or lives were lost because of the attack, security experts have likened the attack to a physical act of terrorism because it is psychologically more serious than the known commercial threats [11]. However, after the ISIS – linked NHS website attack, industry experts have pointed out that future attacks may follow with an intention to create havoc or cause harm to patients [27].

2.3.6. Nation State Actor

Nation state actors are known to be the most advanced set of adversaries in terms of how they carry out sophisticated attacks, their stealthiness, and use of advanced malware [28] [19]. Their popularity arose after the STUXNET operations and project aurora in 2010 [19]. In December 2015, there was cyber-attack on the Ukrainian electric power grid that left about 230,000 residents in the dark [29]. Although there was no proof as per the source of the attack, a nation state actor

was suspected [29] [30]. There have not been many attacks against healthcare infrastructures by nation states, although in the future they may be targeted for a few reasons. The electronic health record database or payroll system of a healthcare facility can be useful to nation states for gathering an employee database for example or for espionage purposes [19]. Hacking into another nation's healthcare system may also be for learning how the healthcare system of the other nation works so that some of their methods can be copied [19]. The most worrisome analysis in [19] is a situation where a nation state accompanies a physical attack with the hampering of critical healthcare cyber infrastructure. This will be very damaging.

2.4. Security Issues of Healthcare IoT Infrastructure

2.4.1. Wireless Sensor Network Attacks

The data collection layer in healthcare IoT is exploited such that the data that is sent to the neighbouring devices is intercepted and manipulated causing non-integrity, or non-confidentiality of data. This layer consists of RFIDs, sensors, and actuators. Attacks can come in the form of the following:

2.4.1.1. Sensor Jamming

This can be used to deny communication between two devices. With this, an attacker can prevent a device from communicating with another device and then connect a rogue device in the process in what can be a man in the middle attack as explained in [31]. The paper further describes how a Bluetooth enabled mobile device was jammed so that a rogue device can then communicate with the healthcare IoT implantable device to stage a replay attack.

2.4.1.2. Eavesdropping

An attacker can intercept communication between devices by sniffing the packets and using the data collected to the advancement of another attack. In the attack illustrated in [31], there was a need to capture the packets to know the packet size and what and what needs to the manipulated

2.4.1.3. Spoofing

An attacker can use manipulate a device to think that it is communicating with another authenticated pair by broadcasting a rogue device as the original device. In [31], the researchers showed a simulation of an attack on a selected health IoT application by spoofing a device to establish a Bluetooth connection. Masquerading like an original device also makes the attack difficult to detect as the communicating device thinks it is communicating with an authenticated device. An attacker would have used other methods to generate the authentication credentials.

2.4.2. Data Aggregators Vulnerabilities

The data aggregators are classified with sensor-enabled devices as part of the Body Area Networks Area Networks (BANs) [32]. Mobile smartphones, dedicated health mobile devices, and desktop health monitors etc. all fall into this category and is a threat to the healthcare IoT system. These devices come with dedicated software applications that are pre-configured to match the operation of a sensor device. Misconfiguration can lead to a device being exploited for an attack. The software can also be exposed to malware attacks since these devices are connected to the internet. If physical security is breached, a malicious user can physically send erroneous data through the device. Also since patients will use these devices, the usability of rigorous security mechanisms may not be convenient.

2.4.3. Social Engineering

Social engineering techniques can be used to gain access physically or remotely into the system. An attacker can disguise as a sick patient to gain access into a hospital and then use rogue means to discover how a hospital IT system is being set-up. He can also use shoulder surfing technique to discover the access credentials of the system. Although this may not be very realistic, a motivated and well-coordinated attack might be successful. Spear-phishing techniques can be used to trick a hospital staff to install a malicious file into the

system to create a backdoor. If improper network-configuration allows a hospital's HIS be accessed outside of the network perimeter, then an attacker may even be able to include malicious links in the web server.

2.5. Security Issues of Industrial SCADA IoT Infrastructure

2.5.1. HMI Vulnerabilities

An attacker can exploit the industrial SCADA system by exploiting the inherent vulnerabilities that exists in the HMI of the system.

2.5.1.1. Hardcoded Credentials

A hijack of the HMI component can allow a remote attacker to control the field devices. Inherent vulnerabilities that can be exploited includes embedded username and password code in plain text within the Java code used in designing Web HMIs. This can leave authentication insecurities as a remote attacker can infiltrate into the system and decompile the codes [33]. The usernames and password can then be used to access the SCADA system through a web interface.

2.5.1.2. Poor Input Field Validation

Also, improper coding techniques can allow an attacker to run queries via the input field of a web HMI resulting in SQL injection attacks [34]. This is due to a lack of proper validation techniques in the input field of the web interface. An attacker can, therefore, run queries such as INSERT, SELECT, UPDATE, DELETE that are sent directly to manipulate the database.

2.5.1.3. Poor Authentication and Authorization

Poor authentication techniques are a loophole in the system. For example, lack of a two-factor authentication system in a critical infrastructure leave the attacker with an opportunity to access a system without many efforts.

2.5.1.4. Zero Day Exploits

Unidentified vulnerabilities by the system software manufacturers is one of the most common threats exploited by SCADA network attackers. Due to the nature of the vulnerability, attackers

can infiltrate into a system performing reconnaissance and scanning and entry without being detected. Zero days in SCADA HMI can be used to exploit vulnerabilities such as memory corruption, buffer overflow, critical credential managements, injections, insecure defaults, etc. [33].

2.5.2. PLC Vulnerabilities

The PLC, sensors and actuators serve as data aggregators on the industrial field. It is possible that an attacker assumes the control of a PLC by exploiting their inherent vulnerabilities and then directly or indirectly interfering with the industrial processes [35]. The exploitation of the PLC firmware vulnerabilities by an attacker can provide direct access to the sensors and actuators on the field. The PLC firmware works as the operating system acting as an intermediary between the hardware and its programmable layer [35]. Because of this, an attacker can directly change the readings of the field devices and then send an incorrect data to the SCADA master. Although the attack on the SCADA system via the PLC is not common, technically there is a possibility [35].

2.5.3. Social Engineering

Cyber attackers can leverage social engineering techniques to infiltrate into a network. Checking IoT databases like shodan.io for device default username and passwords is one method of learning about the network. Email spear phishing methods can also be adopted as an entry point into the corporate network if an attacker's intent is to inject malware over a network. Tricking an insider to physically connect a device (e.g. USB, disk drive) to spread a malware is also possible.

2.5.4. Inadequate Physical Security

The field devices themselves are responsible for the operation of the industrial process and improper physical security procedures can allow an unauthorised attacker to gain physical access to the devices. The consequence of this is that even though the SCADA monitor generates an alarm due to the inappropriate data received, it will be difficult to correct the situation except by physical means.

2.5.5. SCADA Protocol Vulnerabilities

Most of the common protocols used within the SCADA networks are designed for operational efficiency and effectiveness and not security [36]. They do not include authentication mechanisms common in traditional IT systems used to verify the identity of the sender or receiver of the data thereby enabling attackers to compromise the integrity and confidentiality of sensor reading values [37].

2.5.6. Connection with Corporate network

Earlier SCADA systems rely on point to point networks [38]. To adjust the scale of SCADA networks to fit into the current organisational needs, SCADA systems are being connected to the corporate network via secure gateways [39]. Corporate networks run as the same as general IT networks and with the same attack surface, they are susceptible to attacks like SQL injection, cross-site-scripting, phishing, spear phishing, and other vulnerability exploitations [38]. Now it is possible to exploit the vulnerabilities present in the outside network to gain access into the internal industrial network. According to [40], part of the events of the Ukrainian power plant attack in December 2015 was that the attackers tried to gain control of the Ukrainian power plant first via the internal network by coordinating a spear phishing attack first to the internal staff to spread malware. The attackers eventually found their way into the system and then stole access credentials that were used in other stages of the attack. This was an effort to gain access to the HMI and control it from a command and control server.

2.6. Reported Healthcare IOT Infrastructure Cyber Incidents / Scenarios

2.6.1. The Dick Cheney Scare

In 2007, Dick Cheney requested that his Implantable Cardioverter Defibrillator (ICD) to be modified after he feared that it might be under attack from cyber terrorists. Dick Cheney being the vice president of the United States as at 2007, an important and politically influential figure, feared that there could be an attack via his ICD, where the attacker could try to send a signal to the device and shocking him to a cardiac arrest in the process [41]. He feared that an attacker who could be in the next hotel room or downstairs may try to hack the implantable medical device [42]. The

heart defibrillator's wireless function was later disabled to prevent the suspected attack [43]. Security specialists later discovered that if an attacker is close to the device, it is possible to switch the device therapy on and off and also modify its configuration. Since then, we are still yet to discover an active attack on a medical device that can possible cause harm or eventual death to humans.

2.6.2. MedJack 2.0 - The attack against a PACS, X-Ray and a Blood gas analyser [44]

In May 2015, TrapX, a security research group released a document that showed the analysis of a targeted attack on three different hospitals [44]. The focus of the forensics was to see what medical devices connected to the hospital's network infrastructure have already been compromised. Using a specialised deception technology that was installed within the internal network, the researchers can detect compromised medical devices.

In the first hospital, a radiation oncology system, a LINAC gating system and a fluoroscopy workstation were detected to have been compromised. The attackers had used a shellcode execution technique to install a malware into the deception tool. At the end of the research, they discovered that the attacker had target systems running on Windows XP operating system. Furthermore, the system compromise leaves a potential for the attacker to manipulate device configurations or reading [44]. Although, as at when the forensics was conducted, the perceived intention of the attacker was to steal patient data.

In the second hospital, using the same deception technology, the researchers found out that the picture archive and communication system (PACS) has also been compromised [44]. This system is responsible for medical digital imaging, providing access and storage to imaging data. DICOM, the communication protocol used in the PACS enables an integration with other systems within the hospital network such as scanners, printers, workstations, network hardware and servers [44]. This means that an attack on the PACS system can provide a black hole into other integrated systems. The analysts had discovered that the attackers had injected malware into the PACS. They found out that the source of the attack was another device on a separate network segment. At the time the analysis was made, the attackers were about to perform a pass-the-hash attack that can allow a remote authentication of a server [44]. Although, the attack was unsuccessful.

In the third hospital, upon installation of the trap device in the hospital's internal network, a malware that was moving laterally within the network was discovered. Further analysis found out that there the X-ray equipment had a backdoor that running an application based on Windows NT 4.0 [44].

2.6.3. Ransomware attacks

Of all industries in the United States, 88% of the healthcare are affected by ransomware attacks [12] [13]. This is due to the quality of data and the urgency needs to make data available always so that patient's care is not delayed. Healthcare centres in several cities like Los Angeles, California, Ottawa, Wanganui, Indiana, Henderson, Madison, Baltimore and Southern California have all experienced ransomware attacks, but the most interesting case is that of the Hollywood Presbyterian Hospital in Los Angeles [45]. While many of the hospitals were reported to restoring the encrypted data from their backup drives and not paying the ransom, the Hollywood Presbyterian hospital paid attackers a ransom of 17,000 USD in bitcoins [23] [24] [45]. Apart from paying the ransom, the hospital experienced about 10 days of downtime and a reversion to fax machines and paper works [13]. The disruption caused was bad such that there was an inability to perform major daily operations such as CT scans and in severe cases, some patients were transferred to nearby medical centres for treatment [24].

2.6.4. NHS website attack

In January 2017, the British NHS website was targeted by a group of cyber attackers. The NHS website which was only one of the 6 different websites compromised by a Tunisian Islamic group whose intent was to send a message to the West regarding the unsettlement in the middle east [11]. The primary aim of the attackers was to target something that would affect every member of the public [11]. The NHS website was a perfect target for them as it hosts millions of sensitive data of private and public individuals. In November 2016, there was also a report of a cyber-attack that was followed by the management of the NHS trust shutting down the operations of 3 different hospitals [46] [47]. Although there was no in depth detail of the attack, it was believed that a delivered malware caused the cyber-attack. Following the attack, major medical operations were halted while diagnostic procedures and outpatient appointments were cancelled. Major trauma patients and Women in Labor were also transferred to nearby hospital. Although the NHS website

in England was involved in both incidents, we were unable to find any link between the reported attacks.

2.7. Classification of Healthcare Medical Devices

Medical devices are classified by how much risk they pose to patients, their intended use and whether their potential to cause injury as well as their dependency on human life [48]. In the classification below, we see that the medical infusion pump which is analysed in this thesis falls into the category of a class II device.

2.7.1. CLASS I

This set of medical devices do not pose any risk to humans and do not have a potential to result to injury or unreasonable risk to the patient. They are neither life supporting nor life-sustaining [49]. These devices have general controls enough for the assurance of their safety and effectiveness [49]. They thereby fall under the category of low-risk medical devices and are exempted from FDA clearance, and pre-market approval before they are put out for sale [48]. Examples are tongue depressors, crutches and scalpels, etc. [50].

2.7.2. CLASS II

For these set of devices, general controls are not enough to provide the assurance of their safety and effectiveness [49]. If the device is to provide a life-supporting or sustaining functionality, they shall be examined for special controls and how these controls provide safety assurance to human lives. They thereby fall under the category of medium-risk medical devices and must go through the FDA clearance and pre-market approval before they reach the market [48]. Examples are drug infusion pumps, heart-rate monitors and X-ray systems [50].

2.7.3. CLASS III

For these devices, general controls are not enough to provide the assurance of their safety and effectiveness [49]. They are examined for special controls that provide efficiency and safety assurance to human lives. They also go through rigorous FDA clearance, pre-market approval processes as well as post-market surveillance activities before they reach the market [48]. This is

because they are life-sustaining or supporting devices or they are used to prevent the impairment of human lives or "they present an unreasonable risk of illness or injury" [49]. They fall into the category of high-risk medical [48]. Examples are Pacemakers, Heart valves and any IMD devices, etc. [50].

Summary

This chapter discusses the architecture of the healthcare IoT Infrastructure and the Industrial SCADA IoT Infrastructure. This helps us to understand the attack surfaces of both infrastructures. We looked at the potential adversaries to the healthcare IoT citing a few events that has occurred over the past 3 years in the industry. This chapter also discusses about the security issues affecting both infrastructures. Chapter 2 also discusses about some reported events, real life and simulated scenarios within the healthcare industry that are relevant for this thesis. We conclude the chapter with a background study of the classification of medical devices.

3. Literature Review

Several literatures were reviewed to help us to better understand the problem at hand and the cyber security issues related to both industrial SCADA systems and Health IoT infrastructures. Since we wanted to base our comparison on investigating if an attacker can use a Healthcare IoT infrastructure to conduct an attack that can result in a physical impact just as it can be done with Industrial SCADA systems. We tried to put more emphasis on researches that explain cyber threat capability metrics, attack sophistication, attack trees, medical devices IoT and their security issues, SCADA system attacks etc. Some of the other studies made are already included in the background study section of this thesis. The content of this chapter represents the opinion of the writers referenced beforehand. Although, several other papers were reviewed, in this chapter we have only listed a few of them.

3.1. A Sophistication Index for Evaluating Security breaches (Nick and Goel, 2016) [7].

This paper measures the sophistication level of several publicized and documented security breaches over the past 10 years. It highlights that though there is no specific definition for a sophisticated attack due to the ambiguity of the context, and no specific metric for sophistication measurement per se. To reach their goal, they investigated the specific features of these security breaches that may be considered in the measurement of sophistication. Although many features types were considered, the use of elements of social engineering, APT, remote administration, zero-day vulnerability, and stealth were listed to be sophisticated based on the output of their survey. Other features such as use of insiders, standard tools, brute force, little or no technical knowledge etc. were considered as less sophisticated. The result of their report is shown in Appendix B.

3.2. The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems (Byres, 2004) [36].

Although this paper focuses on SCADA protocol security, it is one of the earliest document that provided an insight on the analysis of SCADA systems using attack tree modelling. The evaluation

of the attack trees part of this paper helps us to understand the analysis of attack on SCADA system from the attacker's perspective. The risk indicators focused on in the attack tree risk analysis were the technical difficulty of the attack, stealth and the attack cost. We also considered using the attack tree generated from this paper for our work but we were discouraged by two factors. Firstly, the attack tree was generated about 13 years ago when the paper was written and the tree focused on malicious insider attacks, physical compromise, MODBUS protocol vulnerabilities and not a real-life scenario per se.

3.3. A Taxonomy of Cyber Attacks on SCADA Systems (Bonnie Zhu et al, 2011) [34].

This paper prepares us to understand the potential dangers of cyber threats against SCADA systems. An interesting part of this paper is their comparison of cyber-attacks on standard IT systems versus cyber-attacks of SCADA systems. The paper explains how each part of the SCADA system architecture can be a potential attack point to adversaries. The hardware, software and the communication stack all have their own vulnerabilities which can be exploited by attackers. This paper further highlights that the exploitation of protocol vulnerabilities, MITM attacks, database attacks and cyber-attacks on field devices can lead to devastating consequences like compromising the link between the sensor and the controller to input bogus data to the controller. In fact, an attack of a similar nature is highlighted in one of our case scenarios of an attack on a drug infusion pump.

3.4. A methodology for Systematic Attack Trees Generation for Interoperable Medical Devices (Jian Xu et al, 2016) [51].

The aim of this paper is to generate a general methodology that can be used to create attack trees for Interoperable Medical devices. This paper was carefully studied as it provides more details regarding medical devices and especially infusion pumps. Although, the perspective through which the writer of the paper looked at the attacks was different from ours, the relevance of this paper cannot be overemphasized. The writer did not focus on how the attack can be performed, but what parts of the device if modified can lead to an erroneous infusion. This attack perspective cannot help us to understand the capability of an attacker. However, the paper also agrees that the modification of an infusion pump to cause over infusion can be extremely harmful and even lead

to possible death. Attack sub goals such as an adversary compromising the EHR and the compromise of the pump controller were also discussed in this paper.

3.5. Threat Metrics (Mark Mateski et al, 2012) [6].

This report was studied to understand the qualitative measurement of threats. Since the thesis focused on measuring the required level of sophistication required to perform an attack, we find the cyber threat metric report quite valuable. This paper describes the general threat matrix in detail; a vital study is relevant towards the outcome of this thesis. Another important part of this paper is the description of the expected relationship between threat attributes and incident information categories. Threat attributes serves as indicators in our paper and attack sophistication serves as the incident information category we are investigating. The 4 indicators we focused on i.e. technical ability, stealth, access and time were all generated from this paper. This report also highlights the importance of using attack trees for threat analysis.

	Attribute						
	Commitment			Resources			
					Knowledge		
Criteria	Intensity	Stealth	Time	Technical personnel	Cyber	Kinetic	Access
Incident				✓	✓		
Target system				✓	✓		✓
Timeline	✓	✓	✓				
Covert activity		✓			✓		✓
Attack vector		✓	✓		✓		✓
Sophistication		✓	✓		✓		✓
AV Signature				✓	✓		
Physical interaction				✓		✓	✓
Obfuscation		✓		✓	✓		
Data compromise	✓	✓	✓		✓		✓
Attribution	✓	✓		✓	✓		

Figure 2 The relationship between threat attributes and incident information categories [6]

3.6. Securing Legacy Mobile Devices (Vahab et al, 2013) [31]

This literature shows a simulated attack against a Healthcare IoT application, a pulse oximeter. The main goal of the attack is to intercept a Bluetooth communication between a pulse oximeter and a data aggregator access point (controller). For a successful attack on a medical device of this nature, the writers drew out some assumptions. It is assumed that the attacker is within the proximity of the device such that uninterrupted transmission is possible. They also assumed that an attacker already knows the name, type and model of the pulse oximeter. Another assumption is that the attacker can reverse engineer the packet format of the medical device such that he can modify the appropriate data that can cause harm to the victim. The last assumption drawn out from the literature is that the communication between the pulse oximeter and controller is unencrypted. The detailed analysis of this paper helps us to generate the attack scenario against a drug infusion pump. Other literatures like [52] and [53] also made as hint of this kind of attack. This paper also helps us to understand that an attack against such device is not out of reach of a motivated attacker.

3.7. Attack-Graph Threat Modeling Assessment of Ambulatory Medical Devices (Patrick et al, 2017) [54]

This paper provides an understanding of connectivity of Information systems with medical devices. The paper highlights that this provides a broader attack surface for malicious attacks against the Healthcare IoT infrastructure. The major aim of this paper is to present a vulnerability assessment and mitigation strategy that can be used when designing ambulatory medical devices. Ambulatory medical devices are wearables themselves but are used to monitor blood glucose levels, EKG data, and blood oxygen saturation in real time. This paper also shares the notion with this thesis that communication between a medical device and a remote information system facility such as an EHR can be intercepted if the medical device provider has implement improper security in the communication links. We were also able to learn from this paper that communication in IMDs/AMDs are defined by three levels of security. The first is an unsecured communication channel transmitting unsecured frames. Confidentiality, integrity, authenticity and privacy of data cannot be guaranteed. The second is a communication link where the data is authenticated not encrypted. The last communication channel is one that provides authentication and encryption.

The communication link in an IMD/AMD fall into any one of these categories. Mitigation strategies to Bluetooth attack and android attacks were further highlighted in this literature.

3.8. Threat Modelling for Electronic Health Records (Ahmad Almulhem, 2011) [55].

This literature focuses on the threat modelling for EHR using attack trees. Since we consider an attack scenario in our study, where the attacker tries to modify the patient's record in the EHR, the review of this paper is important to understand the opinion of the writer regarding the scenario. The attack tree analysis is against a proposed client – server model of an EHR system. This paper highlights that an attacker can decide to attack the client system such as the doctor's PC, the EHR server as well as the network link. Although, the paper emphasizes on the physical aspect of the attack such as the use of a malicious insider, our work does not focus on this aspect.

3.9. Awareness of the potential threat of Cyberterrorism to the National Security (Abdulrahman Alqahtani, 2014) [56].

This paper uses the views of cybersecurity experts and security personnel in critical infrastructure to analyse the potential threat of cyberterrorism to National security. The interesting aspect of this paper is in its literature review where several definitions of cyberterrorism were analysed. Having reviewed the definitions from other writers, the writer of this paper concludes that cyberterrorism "involves a surprise attack from a group of individuals or sub-state terrorist organisations using computing infrastructure including networks to cause a disruption of electronic and physical infrastructure of a state". The paper further highlights that a cyber-attack against an IMD can result in death and should also be considered as a cyberterrorist attack.

3.10. Attack Tree-based Threat Risk Analysis (Terrance R, 2013) [5].

The documentation was a follow up to the securlTree attack tree tool designed by Amenaza Technologies. The paper explains the concept of attack tree modelling, their applications as well as some sample scenarios that can help to better understand how to use the tool. Figure 3 shows an image of a goal oriented tree. The attack tree consists of OR nodes, AND nodes and leaf nodes. The topmost node is the root node that shows the overall goal of the adversary. The topmost node

decomposes into several sub goals which consists of other nodes and leaves. The “OR” nodes indicates that the attack can be accomplished by executing 1 or more sub-goals. For example, Intermediate “OR” goal #1 can be accomplish by either subgoal #1a or subgoal #1b. The “AND” node indicates that the attack can be accomplished by executing all the sub-goals. For example, Intermediate “AND” goal #2 can be accomplished by executing subgoal #2a and subgoal #2b.

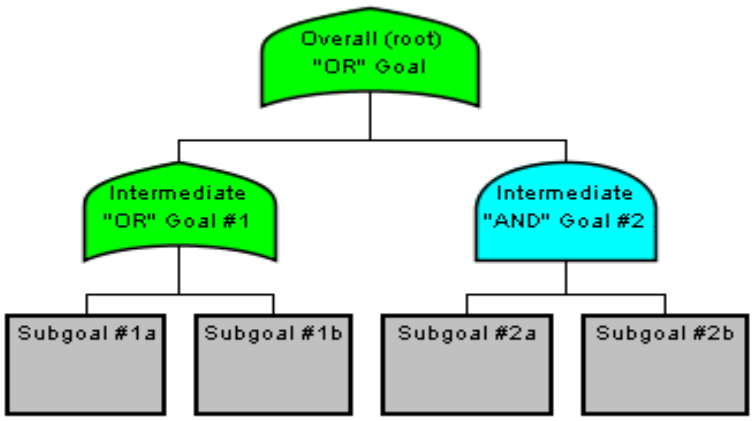


Figure 3 A goal oriented tree [5].

The paper also further explains the pruning technique which is used to eliminate unlikely scenarios in an attack. This technique was also adopted in our work to categorize each attack scenarios into their attack sophistication levels.

Summary

This chapter summarizes some of the literatures that we studied while writing this thesis. These studies help us to understand better the research problem, and how to find a solution to it.

4. Methodology

A diagrammatical overview of the attack tree generation methodology and workflow description from the adoption of a system model to the categorization of threat level capabilities is shown in Fig 4. First, we think in the abstraction of the healthcare IoT environment and we tried to describe the setting which is to be threatened by an attacker. We then modelled the attacker describing the aim, which is to cause a physical result to a user or group of users within the healthcare IoT environment. To proceed with the attack scenarios, we searched for real life scenarios, research documentations, documentations of attack simulations against medical devices, articles, journals and online media related to healthcare industry attacks. To avoid complacency, we focused our research on attacks on medical infusion pumps. For the server side of our system model, we searched for documents describing attacks on electronic health record servers as well as web servers in general. We then converted the reports and documentations to cyber-attack scenarios which was later used to generate an attack tree. The securlTree modelling tool from Amenaza Technologies Ltd. was used in developing the attack tree.

The next thing to do was to assign indicators and their respective values to leaves of the generated attack tree. We used the MITRE cyber prep methodology to select indicators that relates to attack sophistication [6]. The document showed that the cyber knowledge of an attacker, stealth, access and time taken to conduct an attack are important indicators related to attack sophistication. To assign values to each leaf and their corresponding indicator, we search for credible references and documents to ensure that an abnormal value is not assigned to the indicators.

As we need to compare our findings with an attack towards a SCADA system, we tried to find a credible resource showing a SCADA system attack. We tried as much as possible to look for a resource with an already generated attack tree. In 2011, Jason R. Nielsen prepared a thesis on an Air Force SCADA system [57]. In that paper, an attack tree was generated. We then adjusted their attack tree to suit the purpose of our research.

In addition, we adopted the methodology in [7] to generate a sophistication index for our attack scenarios. The paper in [7] was written in 2016 and focused on the sophistication index for evaluating security breaches.

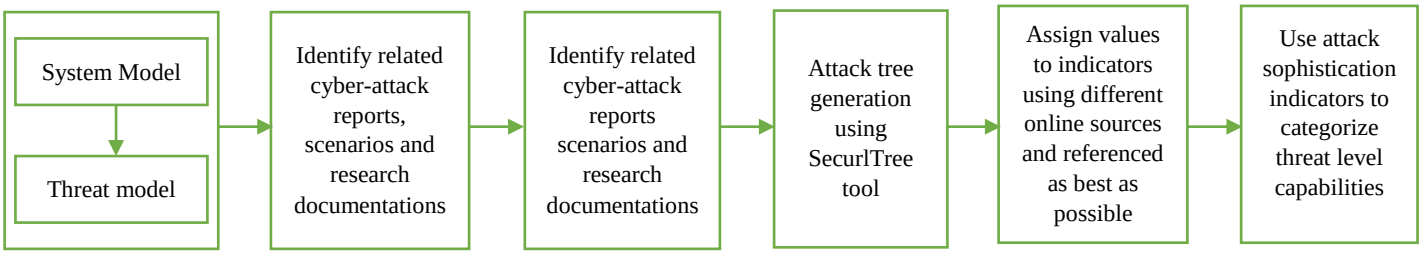


Figure 4 Attack tree generation methodology and workflow description

4.1. System Model

As identified by the ECRI Institute top 10 health hazards in 2017, Infusion pump errors tops the list of devices that are identified as a potential source of danger [58]. Drug infusion pumps being a class III medical device are the most widely used connected medical devices [59] and if tampered with can harmful or result in a possible death. To ensure an understanding of the attack environment, we describe the entire system model as well as the characteristics of the attacker. The system includes sensors, an IMD application such as a drug infusion pump, a smartphone, PDA or home installed health monitoring system, networks, and Electronic health records server. The human components include an attacker, a patient, a caregiver and a remote clinician. A home caregiver is a trusted relative, friend, or someone who is paid to assist the patient if the patient needs to operate the controller but they are unable to do so.

IMDs use sensors for collecting patient's physiological parametric data and monitoring patient's health status. In an Insulin delivery pump, a sensor functions to gather the level of glucose in the bloodstream and then uses this data to determine what therapy the patient needs [60]. To control the pump, an external device such as a mobile smartphone [61], PDA or a dedicated home monitor must communicate with the pump to control the pump function via recommended settings [62]. Communication standards that are used by IMDs include ANT, Bluetooth low energy, Bluetooth, and Medical Implantable Communication Service [60]. In our scenario, the drug infusion pump communicates with the smartphone via Bluetooth. The smartphone is also running a clinical software application which connects to the drug infusion pump via Bluetooth. The function of the

software is to store data, change the device settings, and control the switch of the device. The device settings may include the drug type and dosage, therapy timers, infusion rates, alarm settings and battery status [59]. The controller collects this data and then send it over an IP network via a wired or wireless connection to a dedicated server that hosts the EHR (electronic health record) [63]. The remote clinician can access this data on the clinician website via a firewall protected network or virtual private network to make necessary changes if required. Patients and visiting guests are however able to connect to the hospital's communication link via the guest network, although they are unable to access services such as the EHR server and other critical information systems. [64] [63]

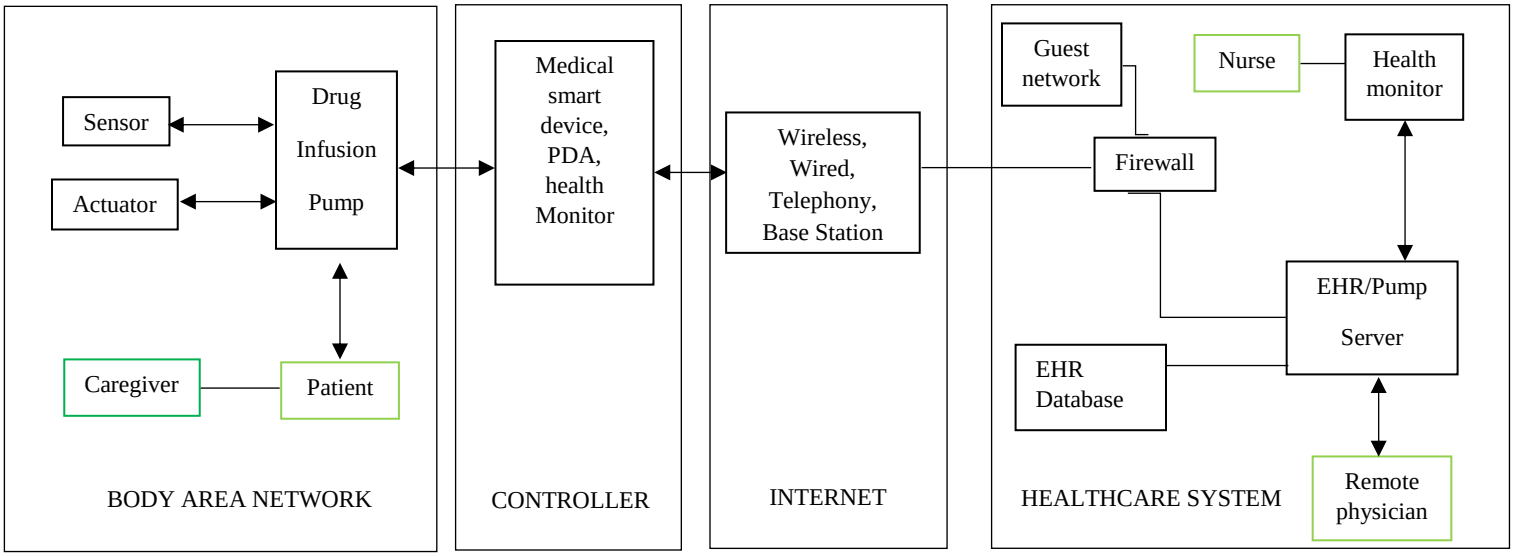


Figure 5 System Model for A Healthcare IOT Infrastructure Setup. Adapted from [65]

4.2. Threat Model

Having discussed the several types of cyber adversaries, our major focus in this research is an attacker whose aim is to cause a physical impact to a device or harm to a target or untargeted individual or a group of persons. The attacker's means is by using cyber exploitation techniques which include social engineering, computing infrastructure vulnerability exploitations, remote administration. DOS attacks on medical devices are not considered in this thesis. This is because we expect a user within the system to consider alternatives that can overcome physical outcomes.

The perceived attack scenario is one where the device is working but not as specified due to the attack. One of the adversary's aim is to disrupt the operation of a drug infusion pump by forcing it to send erroneous instructions clinician. For a successful attack, an attacker needs to be knowledgeable about how to reverse engineer the data coming from the device [66] [52]. For the attack on the drug infusion pump, the attacker needs to be within the range to connect with the device to carry out the attack.

For this research, the threat we will like to consider is one that could lead to physical harm to a patient or death. The greatest threat that fits in this model is that caused by the manipulation of data as they move through the system, i.e. manipulation the data at any point in time as it moves from the sensors on the human body to the remote physician and vice-versa. The modification of data should be such that it results into an erroneous infusion of drug which is the highest priority threat [64] that could be harmful to humans or lead to potential death.

4.3. Possible Cyber Attack Scenarios.

For this research, we will like to make sure that the attacker's goal results into a physical impact. The major goal considered in this case is an attacker who is aiming to cause an erroneous infusion of drugs to a patient or patients thereby leading to physical harm or potential death. We consider three possible attack cases as follows:

4.3.1. CASE 1. Manipulate the Drug Infusion Pump

The drug infusion pump is responsible for directly infusing drug proportions into the human body. If an attacker were to intercept and modify the data that is transferred between the pump and a controller such as a mobile device, then an overdose is possible. Here an attacker's aim is to rogue a wireless relay point while data is transferred between a patient connected to a drug infusion pump and a remote hospital server [53] [31]. The attacker needs to possess the passcode that allows the Bluetooth connection between the drug infusion pump and the mobile device. Once the passcode is known, the attacker who is within the range of connection uses a rogue device to jam the connection between the authentic mobile device and the drug infusion pump. The attacker then connects the rogue device with the drug infusion pump. At this point, the drug infusion pump thinks it is communicating with the original mobile device as the rogue device now has the same

properties such as model type, name and MAC address as the original device [31]. An attacker who must have reverse engineered the drug infusion pump to know how the packets are being stored and may decide to modify the data that is sent or send the same data repeatedly [66] [52]. These options are available to the attacker because the communication between the drug infusion pump and the mobile device is this case is unencrypted [31]. The effect of the modification or replay attack is that the server will return data to the drug infusion pump based on the data received and this could lead to an erroneous injection of the patient [53]. This kind of attack if carried out successfully can lead to a possible patient death [67].

Another way to manipulate the drug infusion pump is to remotely modify the configuration from the device controller by sending malicious code to the device. The medical device controller is responsible for managing the drug infusion pump as well processing the data collected by the drug infusion pump and sending it to the electronic health server. Such device if modified can also lead to an erroneous infusion. It is also possible for an attacker to exploit Bluetooth and wireless transmission vulnerabilities affected from using mobile devices in the healthcare [67]. An attacker can remotely send malicious commands for lethal doses on a drug infusion pump [67]. The aim of the attack launched can range from instructing the pump to stop infusion totally or within a period without the patient knowing. If the drug infusion has stopped, a remote command may be launched to resume the infusion or even so infuse a lethal amount of drug into the patient's body [52].

4.3.2. CASE 2. Modify the Electronic health record to increase the infusion rate of an infusion pump.

The use of electronic records in the healthcare infrastructure was not only to make patient data processing more effective and efficient, but it was also seen as a way of reducing medication errors [68]. This also means that if the system in place to ensure a smooth running of medical operations were to be breached, it can result in a catastrophe. Although most health record breaches that have been reported has been mainly related to privacy issues and financial gain [24] [22], a scenario where an attacker decides to modify stored data will result in confusion in drug administration for example. The drug infusion pump in our scenario connects to the EHR and vice-versa [2]. Here, we are looking at an attacker whose aim is to modify the data that is related to the drug administered by the infusion pump. If an attacker gains full access to the records and decides to swap the patients

names in the record, for example, this will in-turn result in the wrong drug type or infusion rate administered to the patient. An attacker can as well change the drug type that is associated with a patient or simply increase the infusion rate that will be returned to the drug infusion pump.

A remote attacker can use port scanning tools to identify open and unsecured ports and then exploit server vulnerabilities. For a web server, an attacker may decide to inject malicious queries remotely via the input field and then update the content of the database with incorrect data. An attacker can also gain physical access to the server facility and then directly make changes to the system. Once a direct access is accomplished, the attacker will use the login credentials that have been gotten by devious means to gain access to the network. An attacker can also exploit network communication vulnerabilities to perform a man in the middle attack. Once the attacker is connected to the network, he sniffs the packet as they move to or from a host or network. Once this is done, the attacker will modify the packet as they move in real time before forwarding it to the client. In the description in [69], the communication between the client and the server is encrypted, meanwhile, the attacker creates a fake security certificate to send the modified packets successfully. The described scenario was successful because of a browser vulnerability.

4.3.3. Case 3. SCADA System Attack Scenario

The SCADA attack tree model analysed in this section was developed and presented by [57]. The attack tree was modelled like the STUXNET attack and was based on the Wright-Patterson Air Force Base (WPAFB) fuels operation [57]. The goal of the attack was to degrade the fuels operations. Upon a successful attack, an attacker can be able to alter the fuels manager defence (FMD) database data, alter the FMD real-time HMI data, cause the FMD hard drive to crash, transmit a false report to the fuels enterprise system and disrupt FMD communication [57]. For simplicity, the attack tree generated by [57] was reduced to suit the purpose of this thesis. We only considered the incidents with the highest impact per the impact ratings generated by the paper. Altering the FMD database data and altering the FMD real-time HMI data were presented in the paper to have the highest impact [57]. To carry out the attack, the attacker must exploit a vulnerability within the network device and a system related vulnerability [57]. A full attack tree showing different possibilities to carry out this attack is in [57].

4.4. The SecurlTree Attack-tree Tool

We used the securlTree to generate our attack trees. SecurlTree is a graphic attack tree modeling tool developed in Java by Amenaza Technologies. The tool helps in capability based attack tree modelling which eases the creation and understanding of an attack from the attacker's perspective [70]. The securlTree provides a 'pruning tree' function which was maximized for use in this thesis. Pruning helps us to reduce an attack tree based on the resources available to an attacker [71]. Attacks that are beyond the capability of a threat level are removed from the tree effectively. Even though the securlTree is an automated tool, it works based on the information the analyst has inputted regarding the system, the adversaries, and the resources in their disposal. First, we analyse our data using metrics like high, medium and low and then we assigned values to each metric. For example, high = 3, medium = 2 and low = 1 etc. Qualitative analysis metrics were applied in the attack sophistication measurement in [6] and the securlTree is suitable for the analysis of such metrics.

4.5. Attack Sophistication

There is yet to be an accepted standard that can be used to measure the sophistication of an attack. The term sophistication became important as an indicator after the STUXNET attack to help in attributing an attack to a nation state, other cyber-criminal groups or individual [4].

For an attack sophistication analyses based on an attack on a healthcare IOT infrastructure where the attacker's goal is to cause a physical impact, we aim to investigate the following incident details.

i. The relationship between the incident details (attack sophistication) and the threat attributes as provided by [6].
ii. The combination of different attack features (Zero-day, Use of APTs etc.) that can be used to classify the sophistication level of the attack scenario [7] [6].

4.6. Indicators

To carry out an attack, an attacker needs a variety of resources. To limit the resources considered for this research, we will use the indicators provide in [6] that relates to the attack sophistication category. Four different indicators are considered

i. ACCESS: The accessibility is measured by how easily the attacker can gain access to a restricted system [6]. In our research, we will consider the attacker's accessibility to the attack tools as well. We will also consider how much an attacker needs to be close to the device or victim for the attack to be successful [6]. For example, an attack that requires the attacker to be close to the victim or victim's device is given a higher score than an attack that does not consider the proximity to the device.

Table 1 Scoring standard for access

ACCESS [72]		
Name	**Description**	**Value**
Low	The threat has no access to the restricted system or attack tools	1
Moderate	The threat has an indirect or limited access to the restricted system or attack tools	2
High	The threat has a direct or unlimited access to the restricted system or attack tools	3

ii. STEALTH: Stealth is the measure of how much an attacker can carry out an attack without being noticed. The stealth measurement comes from the secrecy of the attack from the planning stage to reconnaissance until the attack is eventually carried out successfully [6]. The stealth score ranges from 1 – 5 which means from very high level of secrecy of attack to low level of secrecy of attack [73].

Table 2 Scoring standard for stealth

STEALTH [73]		
Name	**Description**	**Value**
Very High	It is unlikely that the threat is noticed in pursuance of the goal	1
High	An elevated level of secrecy can be maintained in pursuit of the goal	2
Moderate	A moderate level of secrecy can be maintained in pursuit of the goal	3
Low	It is hard to maintain secrecy during pursuit of the goal	4
Very Low	It is unlikely that the goal is pursued without being noticed	5

iii. TECHNICAL ABILITY: Technical ability is the measure of how easy it is to carry out an attack step. This is related to the cyber knowledge level of the attacker, the level of expertise and specialty which are all put into consideration when determining the technical ability of the attacker. The technical ability score ranges from 1 – 5 which indicates a range from a quite simple attack to a quite difficult attack [6]. For example, an attack that can be carried out by an attacker with software hacking and hardware hacking skills, reverse engineering as well as electrical engineering skill is considered to have a technical ability score of 5.

Table 3 Scoring standard for technical ability

TECHNICAL ABILITY [73] [36]		
Name	**Description**	**Value**
Very Low	Little or no technical ability is required to carry out the attack	1
Low	A minimal level cyber knowledge and technical ability is required to carry out the attack	2
Moderate	An average Cyber hacking skill and Technical Knowledge is required to carry out the attack	3
High	The attack is difficult and requires the expertise of a highly skilled attacker	4
Very High	The attack is quite difficult and requires the expertise of diverse cyber knowledge and technical abilities	5

iv. TIME: Time is a measure of how much period an attacker is willing to invest in coordinating, strategizing, planning until the final implementation of the attack. Due to the variability of time, for this paper the measurement of time will range from Days – Weeks to Years - Decades [6].

Table 4 Scoring standard for time

TIME [6]		
Name	**Description**	**Value**
Days	Planning, strategizing and implementing the attack can be achieved in hours or a few days	1
Days - Weeks	Planning, strategizing and implementing the attack can go on for several days to several weeks	2
Weeks - Months	Planning, strategizing and implementing the attack can go on for several weeks to several months	3
Months - Years	Planning, strategizing and implementing the attack can go on for several months to several years	4
Years - Decades	Planning, strategizing and implementing the attack can go on for several years to decades	5

4.7. Leaf-Node Selection Process

The attack tree builds up from the leaf to the sub-nodes until the attacker reaches its goal which is the root node. Table 5 shows how each leaf-nodes of the attack tree were selected and how the "OR" and "AND" nodes were computed. For the "OR" nodes, all the leaves are considered in the attack. This means that the number of leaves attached to the "OR" nodes affects the number of attack scenarios generated. To compute the indicator values that makes up the root node, the value of each node is combined starting from the bottommost leaf to the root node. The computation of the "AND" nodes vary depending on the type of indicator. For some indicators, the least node value is selected and for others the highest node value is selected to go up the tree. For example, an attack node ("AND") that consists of two leaves one of which has a low technical ability and the other a medium technical ability. The indicator value for the attack node will be medium because for technical ability, we select the value of the most difficult node as this needs to be achieved for the attack to be successful. This process is followed until we get to the root node. Rather than manually go through this process, the securlTree helps us to automatically derive the value of the indicators according to the attack scenarios. In the end, different root node indictors are derived depending on the structure of the attack scenario considered.

Table 5 Leaf-node selection process table

Indicator Name	**OR**	**AND**	**Range**
Access	Minimum of Vertices: The tree selects and considers any of the nodes for each of the attack scenarios.	Minimum of Vertices: The value of the leaf with the highest restriction to access the system is selected to move towards the root node. For example, in an attack that consists of a high access node (unlimited access) and a moderate access (limited access) node, the moderate node value goes up the tree being the more difficult node.	1-3
Stealth (Noticeability)	Minimum of Vertices: The tree selects and considers any of the nodes for each of the attack scenarios.	Minimum of Vertices: The value of the leaf with the stealthiest attack is selected to move towards the root node. This is because the lower the value the leaf the higher the stealth of the attack.	1-5
Technical Ability	Minimum of Vertices: The tree selects and considers any of the nodes for each of the attack scenarios.	Maximum of Vertices: The value of the leaf with the highest technical ability is selected to move towards the root node. This is because the higher the score the higher the technical ability required to carry out the attack. If one of the attack leaf in a combination of attacks is very difficult then the attack node is very difficult as well.	1-5
Time	Minimum of Vertices: The tree selects and considers any of the	Maximum of vertices: The value of the leaf with the highest	1-5

	nodes for each of the attack scenarios.	amount of time in carrying out the attack is selected to move up towards the root node.	

4.8. Threat Level profile

Table 6 Threat level matrix

Threat Level	**Technical Ability**	**Access**	**Stealth**	**Time**	
1	H	H	H	Years - Decades	Most Sophisticated Level
2	M	M	H	Years - Decades	
3	H	M	H	Months - Years	
4	H	M	H	Weeks - Months	
5	M	M	M	Weeks – Months	
6	M	L	M	Weeks – Months	
7	L	L	M	Months – Years	
8	L	L	L	Days - Weeks	Least Sophisticated Level

The threat level matrix in Table 5 was generated according to the generic threat matrix in [6]. In our analysis, the threat level is proportional to the required sophistication level of the attack. That is, the higher the threat level, the higher the attack sophistication. The threat levels shown in table 5 illustrates a decreasing level of threat capability with threat level 1 possessing the highest attack sophistication level and threat level 8 possessing the least attack sophistication level. From the table, we can infer that an organization with a threat level 1 have the required technical ability to carry out any type of attack. They have unlimited access to a restricted system as well as the attack tools required to carry out the attack. The attacks they carry out are well coordinated such that the stealthiness of their attacks from the planning stage to implementation stage is almost undetectable. They can also go as far as conducting an attack for years until they reach their goal. The lowest threat level is threat level 8. Attacks that fall under this category have low technical capability and do not have access to a restricted system. They do not have the capability to perform stealthy attacks and the dedicated time they can put into conducting at attack is a few days to few weeks.

4.9. Using Sophistication Index to measure the attack scenarios

Nick DePaula and Sanjay Goel in their methodology measured the sophistication of an attack based on five different feature types [7]. Having gone through a security survey, the result of their research was that an attack with all five feature types is regarded as the most sophisticated. This means that for an attack to be regarded as the most sophisticated, the attacker will use elements of social engineering, APT, remote administration, zero-day vulnerability exploit and stealth. For every cyber-attack incident, each feature type is given a score of 1. For example, an attack that rootkit, zero-day and spear-phishing is given a score of 3 [7]. More details regarding their result is found in Appendix B.

Summary

This chapter discusses about how we tried to solve the research problem. Measuring the capability of an attacker or the sophistication level of an attack depends on several constraints and varies for threat levels. To help us proceed, we adopted the use of attack trees which helps us to reason more like an attacker. To begin, we tried to describe the system that is at the disposal of the attacker and, we model the threat. We also describe some 3 attack scenarios. The first 2 case scenarios describe an attack to the healthcare IoT facility while the last scenario described an attack towards an Industrial SCADA facility. Each attack scenario can be carried out in several ways. For this research, we believe that all the threats have the same goal regardless of their resources or capability, which is to conduct an attack that can cause a physical result. We categorized the threat level capabilities based on some related attributes of attack sophistication that were described in [6]. This means that even a motivated attacker with without the capability or resources may not be able to carry out any of the attack scenarios. Chapter 4 also describes the values of each indicators and how they are assigned.

5. Data Analysis and Results

This section describes how the values of each leaf-node of our attack tree is generated, the analysis of this data and the results of our analysis. The full attack tree of each case scenario 1, 2 and 3 is shown in figure 6, 7 and 8 respectively. Each node in the attack tree is described and the values of each indicators of attack sophistication are generated in this section.

5.1 Case 1: Manipulate the Drug Infusion Pump

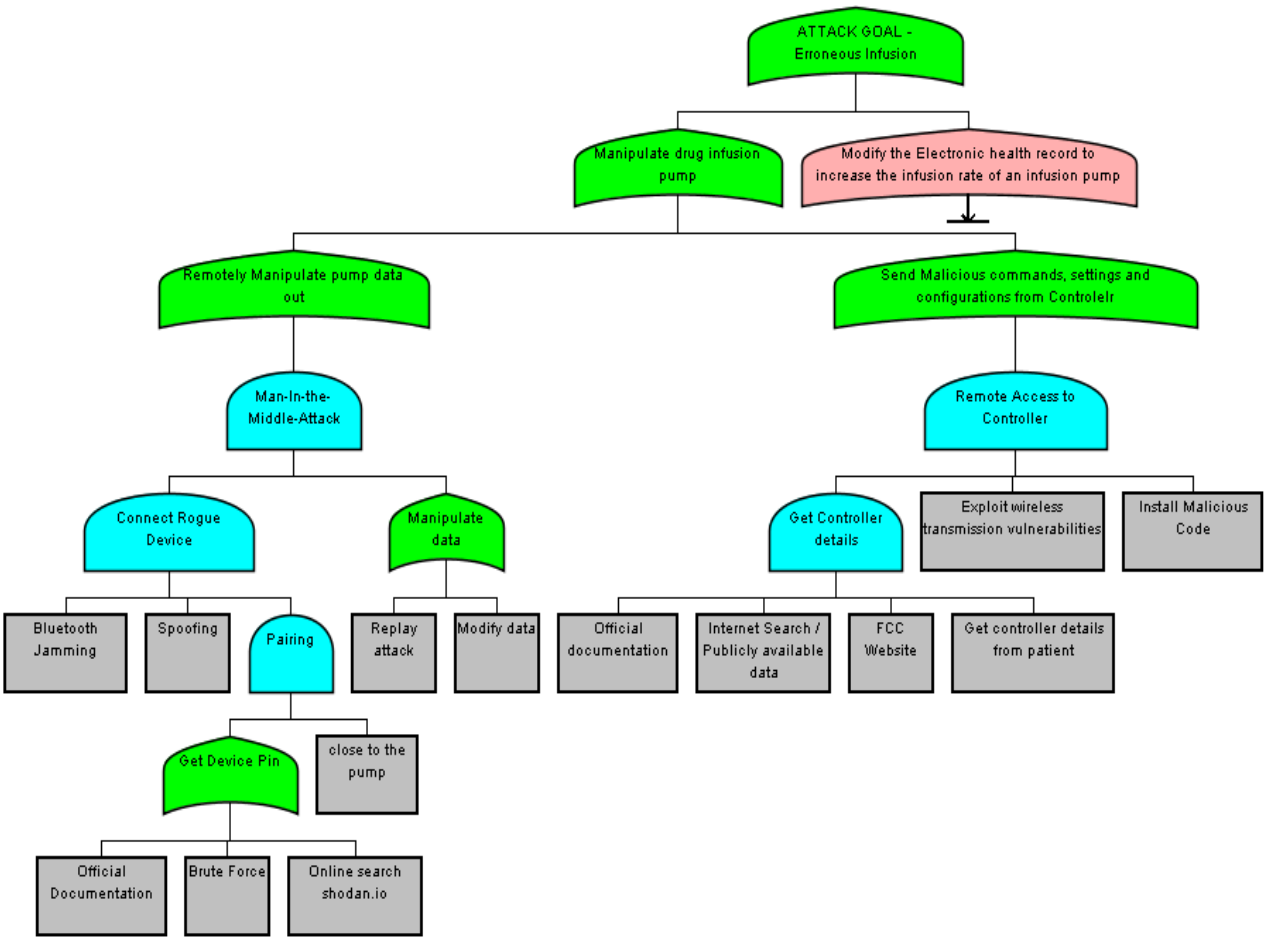


Figure 6 An attack tree of a Drug Infusion Pump

Table 7 Attack tree description for a Drug Infusion Pump

sub-goal	Sub-goal Description	Attack nodes	Tech. Abi	Access	Stealth	Time
Get Device Pin	To connect a rogue device, the attacker needs to possess the Bluetooth authentication credentials. Any one of the attack nodes can be chosen to proceed with the attack	Use Official Doc	L	H	VH	Days – Weeks
		Brute Force	M	M	H	Weeks – Months
		Online Search	L	H	VH	Days – Weeks
Connect Rouge Device	The attacker needs a rogue device that behaves like the original controller and then he tries to connect this device in between the communication between the drug infusion pump and the controller.	Jamming	M	M	H	Days – Weeks
		Spoofing	H	M	H	Weeks – Months
		Pairing	L	M	H	Days – Weeks
Man-in-the-Middle	Once the attacker can intercept the data between the drug infusion pump and the controller, he then decides to either send the same data to the pump or modify the data.	Modify Data	H	M	M	Weeks – Months
		Replay Attack	M	M	M	Weeks – Months
Remote access to Controller	The attacker aims to remote access the mobile device controller in order to change the data and configuration on the device.	Exploit wireless transmission	VH	M	H	Weeks – Months
		Install Malicious code	H	M	H	Weeks – Months
Get Controller details	The attacker needs every information possible regarding the victim's device to be able to gather the appropriate tools to further the attack.	Official doc	L	H	VH	Days – Weeks
		Internet Search	L	H	VH	Days – Weeks
		FCC Website	L	H	VH	Days – Weeks
		Get details from patient	L	M	H	Days – Weeks

- Get Device Pin: The connection between the drug infusion pump and the mobile device controller is via Bluetooth. In a Bluetooth authentication process, a pin code is required to pair the devices for a connection to be established. To proceed with the attack, the attacker needs to get the device pin.

- Official Documentation: The attacker can get the pin of the device via the official documentation or instruction manual that comes along with the product upon its purchase [31]. The attacker could easily find such documentations on the internet or simply by asking someone who owns a drug infusion pump to provide its instruction manual for reading purpose. For this reason, little technical capability and a high score for its accessibility.

- Brute Force: The attacker can use brute force technique to input several guesses of pin codes using automated software until the correct pin is generated [74]. An attacker with a moderate technical skill will be able to perform this attack and the accessibility to the attack tool is given a moderate score as well. A high stealth score is estimated for this attack [75]. Typically, the time needed to perform a brute force attack cannot be precisely determined since it is dependent on the complexity of password itself as well as the processing speed of the brute force tool [76] [77].

- Online Search: The attacker can get the pin of the device by conducting a thorough online search once the device type and model number of the device are known. Since the attacker will be on the internet, it will be very difficult for him to be noticed. It may take days – weeks for the attacker to find the required data. An attacker with average skills good enough to use anonymous websites should be able to carry out this search.

- Connect Rogue Device: The attacker needs to connect a fake or rogue device with the drug infusion pump such that the drug infusion pump thinks that it is communicating directly with the original mobile device controller. To do this, the attacker needs to combine Bluetooth jamming techniques with spoofing before eventually pairing the rogue device with the drug infusion pump.

- Bluetooth Jamming: The attacker needs to prevent the original mobile device controller from communication with the drug infusion pump. He does this by jamming the signal so that he can introduce the rogue device [31]. There is a reducing cost of Jammers as and sources showing how an adversary with a medium level technical ability can carry out a Bluetooth jamming operation are publicly available online [78]. We conclude that a moderate technical ability is needed to carry out the attack. A moderate score is given for accessibility to attack tool. The device owner is

unaware that an attack is going on so a difficult noticeability score is given for this attack [79]. We assume that since the attacker needs to be within a connecting distance with the device the attacker may take between days to weeks to find a comfortable attack zone without detection.

- Spoofing: Once the attacker can perform the Bluetooth jamming attack, he needs to ensure that traceability and noticeability of the attack are difficult by matching the device serial number, Bluetooth connection name, model number etc. with that of the original device [31]. With this, the drug infusion pump thinks it is in communication with an actual controller. A similar attack is described in a paper analysing an automotive attack surface [80] and was rated as a medium cost attack. According to [81], an attack of this nature needs the use of a sophisticated equipment as well as a specialised technical expertise. For this, we will assign a difficult technical ability score to this attack. For an attack that requires specialised technical expert and sophisticated equipment, this will take weeks to months to accomplish.

- Pairing: Once the Bluetooth jamming and spoofing attacks have been completed, the attacker needs to pair the rogue device with the drug infusion pump using the generated Bluetooth pin. The pairing process requires little or no technical knowledge but is given an accessibility rating of high. This is because for the pairing to be successful, the attacker needs to be within the proximity of the device as well as the human that is to be attacked. A moderate access score has been assigned to this part of the attack since the attacker has a limited access to the victim. In fact, in [66], it was iterated that although getting physically close to the victim is not impossible, it only reduces the possibility of the attack. Once other stages are done pairing can be achieved within a day or even less depending on the attacker's strategy.

- Man-in-the-Middle: To ensure that an erroneous data is sent from the drug infusion pump to the controller, the aim of the attacker is to intercept the data during the communication between the devices in real time. Once the interception is achieved, the aim of the attacker is to confuse the drug infusion pump to think that it is communicating with the authentic medical controller and vice-versa. Once this is done the attacker has a choice to either send repeated data or modify the data during transmission.

- Replay Attack: Upon interception of the communication between the drug infusion pump and the controller, the attacker can choose to keep resending the same packets that have been outdated to

the infusion pump [52] [31]. When a replay attack is performed, it may not be necessary to examine the format of the transmitted packet. This reduces the technical ability needed to carry out the attack. For this reason, a moderate technical ability score is given to carry out the attack. It is also possible to maintain a moderate level of secrecy when planning and carrying out the attack. A moderate access score is given to this attack because the attacker needs to be within the proximity (about 5 – 7 meters) of the victim [52].

- Modify data: Upon interception of the communication between the drug infusion pump and the controller, the attacker can choose to change the content of the packet during transmission to cause an erroneous infusion [31]. For such attack, it is necessary for the attacker to examine the format of the transmitted packet to know what field can be modified. A difficult technical ability score is assigned to this attack. We also gave a moderate score for stealth and a moderate accessibility.

- Remote Access to Controller: The attacker can access the mobile device controller without being in direct contact with the device itself. The major aim of the attacker is to change the configuration of the device such as infusion rate, infusion intervals, alarm notifications, pre-configured wireless commands etc. [2] [82]

- Exploit Wireless Transmission: The attacker can exploit the wireless capabilities of the mobile device controller to remotely control the device using another device that works like the original controller. The technical ability that is needed to perform the attack is very high as well. Software security hacking skills, as well as hardware hacking skills, are requirements necessary to be able to carry out an attack of this nature [66]. Accessibility to the attacking tools is given a difficult score. The attacker needs to learn of the model of the device which usually needs physical access to the device and needs to search at different stores as well as organisational websites like that of the Federal Communication Commission (FCC) to get more details necessary for this type of attack [66]. Carrying out this attack will take weeks to months to achieve because it involves an extensive research and planning [66].

- Install Malicious code: The attacker needs to accompany the wireless transmission exploit by reprogramming the device. He does this by installing a malicious code into the device. In [66], it was explained that some of the command codes are freely available on multiple sites via google

even though the information have not been provided by the manufacturers directly. Even though there is a moderate level of access to these codes, only an attacker who can understand how the code works and can also reprogram the code to carry out its intended function can carry out this attack. A moderate technical skill is given to this attack and the attack may take weeks to months to be eventually carried out.

Table 8 Indicator values for an attack on a Drug Infusion pump

Attack Nodes	**Tech. Ability**	**Access**	**Stealth**	**Time**
Use Official Document	2	3	1	2
Brute Force	3	2	2	3
Online Search	3	3	1	2
Jamming	3	2	2	2
Spoofing	4	2	2	3
Pairing	2	2	2	2
Modify Data	4	2	3	3
Replay Attack	3	2	3	3
Exploit Wireless Transmission	5	2	2	3
Install Malicious Code	4	2	2	3
Official doc	2	3	1	2
Internet Search	2	3	1	2
FCC Website	2	3	1	2
Get details from patient	1	2	2	2

5.2. Case 2: Modify the Electronic Health Record to increase the infusion rate of an infusion pump.

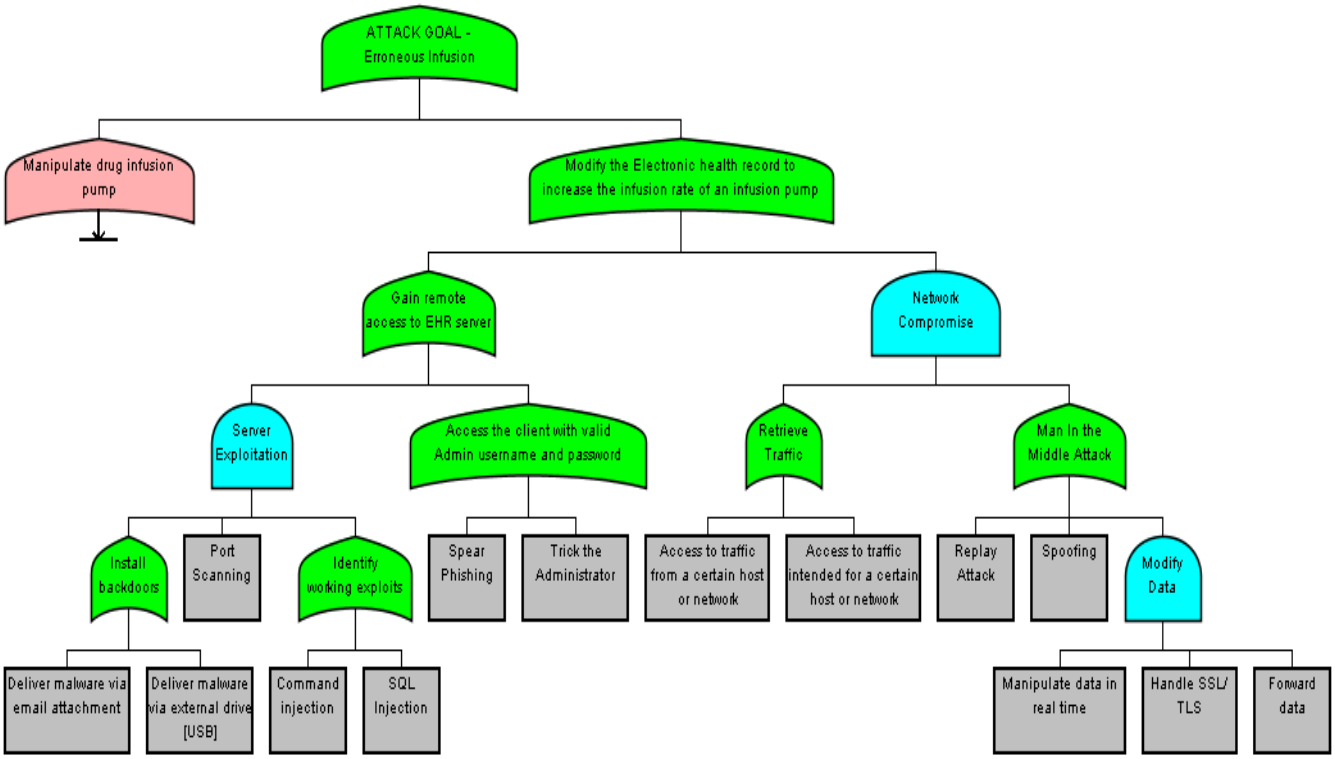


Figure 7 An attack tree of an Electronic Health Record

Table 9 Attack tree description table for Electronic Health Record attack

sub-goal	Sub-goal Description	Attack nodes	Tech. Abi	Access	Stealth	Time
Install Backdoors	The attacker aim to find a point of entry into the system by installing backdoor programs on an EHR server computer	Deliver Malware via Email	M	H	H	Weeks – Months
		Deliver Malware via USB	M	M	H	Weeks – Months
		Port Scanning	L	M	H	Days – Weeks
Identify Working Exploits	The attacker will exploit several vulnerabilities in the EHR server until an exploit that suits the attacker's goal is discovered.	Command Injection	H	M	M	Weeks – Months
		SQL Injection	M	M	M	Days – Weeks

Access with admin Username and Password	The attacker upon gaining access to the hospital network can try to login with the admin username and password	Spear Phishing	M	H	H	Weeks – Months
		Trick the Admin	L	H	H	Days – Weeks
Retrieve Traffic	The attacker needs to find means to get access to the traffic to or from the network	Access to traffic from a host	M	M	M	Weeks - Months
		Access to traffic to a host	M	M	M	Weeks - Months
MITM Attack	The attacker aims to intercept the data as they move from the client to the EHR server. Replay attack and packet modification is considered here.	Replay Attack	M	M	M	Weeks - Months
Modify packets	During data transmission the attacker and upon interception of the data, the attacker needs to modify the data such that the modified data result to a physical injury to the patient.	Manipulate data in real time	H	M	H	Weeks - Months
		Forward data	L	H	H	Days - Weeks
		Handle TLS / SSL	VH	L	H	Years - Decades

- Install Backdoors: The need to install a backdoor is to enable the attackers to repeatedly access the system and the intranet sites whenever they want by bypassing normal security controls [83]. During this time, the attacker is finding other loopholes in the system that can be exploited to carry out the intended goal. The methods that can be used to deliver malware into the system in our attack scenario is either by an email attachment or by a USB drive.

- Deliver Malware via Email attachment: An attacker can send an infected file via an email attachment to an individual or group of individuals in the hospital. Once the file is opened on a computer within the hospital's network, a backdoor can be created that enables an attacker to connect to that computer from a remote location. We give a moderate score for the technical difficulty needed to carry out this attack as we also considered the attacker's skill to create or modify the backdoor. A high score is given for stealth as the attack can go one for a very long time without it being noticed. Also, an easy score is given for accessibility as the emails are sent over the internet and there are no restrictions. Even though the malware is not likely to be delivered directly by the attacker, a hospital staff with access privileges can be tricked into performing the attack. It is estimated that an attack of this nature may between several weeks – months.

- Deliver Malware via an External drive (USB): The attacker can deliver malware to the target EHR server via a USB drive. Means such as the distribution of free USB devices to hospital employees or tricking a doctor to share a file from the physician's computer system into a USB drive can be an alternative way. A low technical skill is needed to carry out this attack. We also give a moderate accessibility score to this attack. An attacker will choose an unsuspecting way to deliver the malware, so we rate the stealth of this attack as high. From planning to delivery of the malware, this attack can take days – weeks.

- Port Scanning: Upon successful access into the hospital's network, an attacker will scan for open ports within the network that can be used to begin an exploitation. A very low technical skill is required to carry out this attack as there are numerous tutorials explaining how this can be done online [84]. We also give a medium score for accessibility as there is an unlimited access to tools necessary to carry out the attack. We assume that the attacker is performing a stealth port scanning which is harder to detect than conventional port scanning [85]. We estimate that this attack could be carried out from a day to weeks.

- Identify Working Exploits: Once the attacker has established persistence in the system, the next aim of the attack is to find the vulnerabilities in the system. He can try different exploits until one is found that can accomplish the attacker's goal.

- SQL Injection: The aim of the attacker is to execute database queries that can result in the modification of electronic health records in the database [86]. A medium technical ability is required to carry out this attack and we have also given a moderate score for the stealth of this attack [87] [88]. We have given a moderate score for access and the attack could also take days to weeks to accomplish.

- Command Injection: Upon entrance into the hospital's network the attacker can decide to execute arbitrary operating system commands via a discovered vulnerable application [89]. A high technical ability score is assigned to this attack because this attack is more difficult to perform than SQL injection as the attacker needs knowledge of operating system shell commands and the operating system itself [90] [91]. We have given a high score for access because details regarding command injection are scarce even in forums, books and websites related to hacking [91]. We also

assign a moderate score for stealth and this attack could also take weeks to months to accomplish [88].

- Access the client with valid admin username and password: An attacker that can gain root access to the server can try to use different combinations of admin username and passwords to gain access to the system. The attacker might have tried several social engineering techniques to get the access credentials of the system. A low technical ability score and low stealth are given for this attack [92]. A moderate score is given for access and this attack can be achieved within days to weeks.

- Retrieve traffic: To compromise a network the attacker needs to eavesdrop the traffic as it flows between the client and the server. The attacker has an option to retrieve the traffic as data is transferred from the EHR server to the patients or vice versa from the patients to the EHR server.

- Retrieve data Intended for a network: An attacker can try to retrieve the data that is intended for the hospital's network [69]. A moderate technical skill is needed to carry out this kind of attack [93]. We give a moderate score for the accessibility of the attack as the attacker might need some level of physical and network access to begin sniffing. A high score is given for the stealth of this attack as it is difficult for notice or trace [94]. We estimate that this attack can be carried out within days to weeks.

- Retrieve traffic from a network: An attacker can try to retrieve the data that is coming from a hospital's network [69]. The indicator score for this attack is the same as to retrieve data intended for a network or host.

- Replay attack: An attacker can decide to maliciously forward an already captured data so that the EHR server so that it is receiving an authentic data in real time. If successful, this will result in an erroneous health record transfer since the original data is not the same as the repeated data. This attack path can be chosen if the attacker decides to bypass authentication [95]. A medium technical skill is needed to achieve this attack [96]. The attack could take weeks to months to be achieved.

- Manipulate Data in Real-time: The attacker needs to sniff and modify the incoming packets during transmission in real time to capture the SSL stream [69]. A high technical skill is needed to carry out this attack. The events in the attack include creating a secure socket that listens on the same

port as the original data recipient [69]. An advanced programming skill is also needed to tweak the already available program libraries used in the attack [69]. A moderate score is given for accessibility of this attack and the attack is also difficult to notice [94]. An estimated time to carry out the attack is between weeks to months.

- Forward Data: Forwarding the data is the least worry of the attacker. The attacker can only try to implement additional techniques to ensure that the attack is stealthy enough upon transmission of modified data [69]. A medium technical skill is estimated for this attack. A high score is given for stealth and low score is given for access. An estimated time to achieve this attack node is between days to weeks.

- Handle TLS / SSL: A very high technical skill score is given to this attack node as a high level of the understanding of the underlying principles of encryption is needed to begin the attack [97]. An attacker needs to have access to the data in real time to gather the SSL stream [97]. This increases the accessibility score of the attack so we estimate a high score for this. We also estimate that it may take between months – years to be able to carry out this attack.

Table 10 Indicator values for an attack on an EHR

Attack Nodes	**Tech. Ability**	**Access**	**Stealth**	**Time**
Deliver Malware via Email	3	3	2	3
Deliver Malware Via USB	2	2	2	3
Port Scanning	2	3	2	2
Command Injection	4	2	3	3
SQL Injection	2	2	3	2
Use Admin Username and Password	2	3	4	1
Access to traffic from a host	3	2	3	3
Access to traffic to a host	3	2	3	3
Replay Attack	3	2	3	3
Manipulate Data in Real Time	4	2	2	3
Forward Data	2	3	2	2
Handle strong TLS / SSL	5	1	2	5

5.3. Industrial SCADA System Attack Scenario

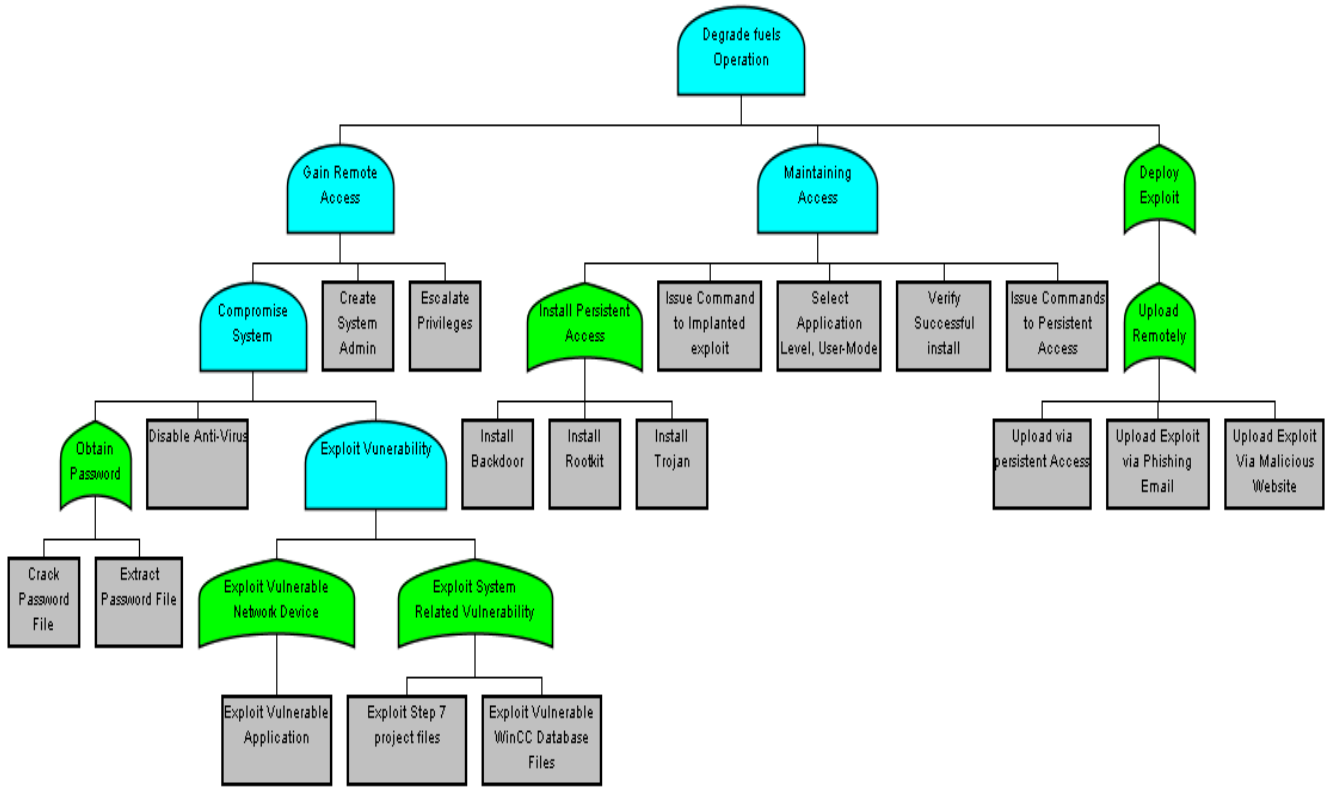


Figure 8 An attack tree of a Wright-Patterson Air Force Base (WPAFB) fuels operation [57]

5.3.1. Assigning Values to the nodes.

The technical ability value for each of the nodes was given in the original paper that discussed the SCADA attack to a WPAFB fuels operation. In the paper, the probability of attack success equals the technical difficulty of the attack node [57] which is proportional to the technical ability needed to carry out the attack. We also gathered that the technical difficulty of an attack is the most important indicator needed to measure the probability of success of an attack. Since this paper provides a similar metric for technical difficulty, we decided to proceed to use it for our comparison. We then generated a score for the other indicators of the attack nodes using the same definition as in access, stealth and time.

Attack nodes 1 – 13, 16 and 17 were assigned a moderate access score. This is because the attacker has limited access to the system to carry out the attack describe in the attack nodes. We expect that

the attacker already has access to the Master SCADA system so he has fewer restrictions to verify successful installations or issue corresponding commands. We also assign a high access score for the attacker to upload the exploit via a phishing email. There is less restriction to do this as it is only up to the staff to fall for the bait.

Many of the attack nodes describe elements of an advanced persistent threat (APT) [98]. Social-engineering, spear-phishing, malware infection, mapping, privilege escalation, spreading within the network and attack execution were described in the anatomy of an APT attack [98]. APTs are designed such that it is difficult for them to be discovered within the network traffic as they move from one host to the other [98]. Trojans, rootkits and backdoors, for example, are designed in such a way that they can keep a low profile within the system [98]. For this, attack nodes 1 – 11, 13, 17 and 18 were assigned a high stealth score. We assume that uploading the exploit via persistent access may not be as stealthy as by phishing email or through a malicious website so a moderate stealth score is given.

A report on the analysis of the Ukrainian power grid cyber-attack describes that an attacker can be leveraging the vulnerabilities of an Industrial Control System to perform reconnaissance for at least 6 months [40]. We also learnt that during the STUXNET attack was executed very stealthily such that at some point the attackers separated each phase of the attacks by 27- days [99]. From this, we concluded that the planning and execution of an attack against an industrial SCADA system can take months to years. We used this ideology in assigning time indicator values to our attack nodes.

Table 11 Indicator values for an attack on Wright-Patterson Air Force Base (WPAFB) fuels operation

No	Attack Nodes	Tech. Ability [57]	Access	Stealth	Time
1	Create System Admin Account	4	2	2	3
2	Escalate Privileges	4	2	2	3
3	Crack password File	3	2	2	3
4	Extract Password File	4	2	2	3
5	Disable Antivirus	4	2	2	2
6	Exploit Vulnerable Application	4	2	2	3
7	Exploit Step 7 Project files	4	2	2	4

8	Exploit Vulnerable Win CC database files	4	2	2	4
9	Install Backdoor	3	2	2	4
10	Install Rootkit	3	2	2	4
11	Install Trojan	3	2	2	4
12	Issue Command to Implanted Exploit	2	2	3	2
13	Select App Level User-Mode or Kernel Mode	3	2	2	2
14	Verify successful Install	2	3	3	2
15	Issue Commands to Persistent Access	3	3	3	2
16	Upload via Persistent Access	2	2	4	2
17	Upload Exploit via Phishing Email	4	3	2	3
18	Upload Exploit via Malicious Website	4	2	2	3

5.4. Comparative Analysis

The securlTree software provides us with a tool that allows us to map the threat agent profiles to their defined capabilities [70]. In this research, the threat agent profiles are defined according to the indicators provided in [6] that can be related to attack sophistication. We then used the pruning tool to analyse the capabilities of the threat agent level with the attack scenarios. Table 12 shows the results of our analysis in terms of number of scenarios. The report of the attack scenarios including the attack leaf-nodes and generated indicator values is shown in appendix A, fig A.7 – A.12.

The attacks scenarios that fall within threat level 1 have the highest attack sophistication level. The attack sophistication level decreases from threat level 1 to threat level 8. While attacks that fall under threat level 1 are the most sophisticated, a threat level 5 can conduct an attack against a Healthcare IoT infrastructure, with a lesser sophistication and then causing a physical result. In the SCADA attack scenario, we can see that only attackers that fall under threat level 1 and 3 can perform the attack.

Comparing both results, it is seen threat level 4 and 5 can carry out an attack towards the Health IoT Infrastructure but not the industrial SCADA system. This means that the required sophistication necessary to carry out an attack against an IoT application such as a healthcare drug infusion pump is lesser than an industrial SCADA system while the motivation of the attacker remains as to cause a physical result.

Table 12 Tabular View of Attack Tree Scenarios by Threat Level.

Health Care Infrastructure IOT (No of Scenarios = 19)		**(WPAFB) SCADA attack (No of Scenarios = 36)**	
Threat Level	**Scenarios**	**Threat Level**	**Scenarios**
1	11	1	36
2	5	2	0
3	9	3	36
4	9	4	0
5	2	5	0
6	0	6	0
7	0	7	0
8	0	8	0

5.4.1. Analysis of CASE 1 using Sophistication Index – Manipulate the drug infusion pump

Table 13 shows the how the sophistication index of the attack to the drug infusion pump is generated. The sophistication feature types necessary to remotely manipulate the drug infusion pump are social engineering, remote administration and stealth. No zero-day vulnerability was described to be exploited while carrying out the attack and there was also no attack scenario that can be analysed as an Advanced Persistent Threat. Altogether, a sophistication index of 3 out of a possible 5 is derived for the attack.

Another way of manipulating the drug infusion pump is by sending malicious command to the pump's controller. An attacker can use social engineering methods to get the device details from public sources or from the patient.

Table 13 Sophistication Index table for an attack on the Drug Infusion Pump

Feature types	**Remotely manipulate the drug pump out**	**SI**	**Sending malicious command to the controller**	**SI**
Social Engineering	Online search, official documentation.	1	Official documentation, internet search/publicly available data, Get device details from patient	1
Remote Administration	Bluetooth jamming, spoofing, pairing, modify data, replay attack	1	Exploit wireless capabilities, install malicious code	1
Stealth	Spoofing	1	Exploit wireless capabilities, install malicious code	1
Zero-Day Vulnerability	None	0	None	0
APT	None	0	None	0
		Total = 3		Total = 3

5.4.2. Analysis of CASE 2 Using Sophistication Index - Modify the Electronic health record to increase the infusion rate of an infusion pump

The attacker can modify the electronic records by either attacking the EHR server, the EHR client or the network. To attack the server, we assume that the attacker is exploiting existing vulnerabilities. To conduct the attack, the attacker needs to combine elements of social engineering, stealth, remote administration and APT. This makes the SI score for this attack scenario 4. In the network attack scenario, our assumption is that if the attacker would compromise a server that correctly implements SSL/TLS data encryption, then a zero-day vulnerability must be exploited. This increases the sophistication of this attack to 5, otherwise we generate a SI score for an attack to the network layer to be 4. The least sophisticated attack to the EHR is an attack to the client machine. The scenario here sees an attacker remotely gaining access to the client machine after using social engineering techniques to acquire vital access information. The SI score for such attack is 2. Table 14 illustrates the attack in detail.

Table 14 Sophistication Index table for an attack on the Electronic Health Record

Feature types	**Attack Server**	**SI**	**Attack Network**	**SI**
Social Engineering	Deliver malware via email attachment, Deliver malware via USB	1	Access traffic from/to the network or host	1
Remote Administration	Command injection, SQL injection,	1	Access traffic from/to the network or host	1
Stealth	Install backdoors	1	Access traffic from/to the network or host	1
Zero-Day Vulnerability	None	0	Handle SSL/TLS – (strong encryption)	1
APT	Install backdoors	1	Access traffic from/to the network or host	1
		Total = 4		Total = 5
Feature types	**Attack Client**	**SI**	**Attack Network**	
Social Engineering	Spear phishing, Trick the administrator	1	Access traffic from/to the network or host	1
Remote Administration	Command injection, SQL injection,	1	Access traffic from/to the network or host, Replay attack	1
Stealth	None	0	Access traffic from/to the network or host	1
Zero-Day Vulnerability	None	0	None	0
APT	None	0	Access traffic from/to the network or host	1
		Total = 2		Total = 4

5.4.3. Analysis of the SCADA attack scenario Using Sophistication Index – Degrade Fuel operation of the Wright-Patterson Air Force Base

The attack to degrade the fuel operation of the WPAFB utilizes all the features of a sophisticated attack. In the analysed attack, there are elements of social engineering, APT, stealth, Remote administration and the exploitation of zero – day vulnerability. This gives the total SI score for this

attack to be 5. Which is the highest derivable SI score. Further illustration is shown in table 14 below.

Table 15 Sophistication Index table for an attack on the Wright-Patterson Air Force Base

Feature types	**Attack Nodes**	**SI**
Social Engineering	Upload with phishing email	1
Remote Administration	Install backdoor, install rootkit, issue commands, verify Install	1
Stealth	Disable antivirus, Escalate Privileges, Exploit Vulnerabilities, Install rootkit	1
Zero-Day Vulnerability	Exploit Vulnerable Win CC database files	1
APT	Install backdoor, create system admin, Install rootkit	1
		Total = 5

5.4.4. Results from the Healthcare IOT infrastructure attack tree

Using the indicators related to attack sophistication to analyse the capabilities of each threat levels, we realise that threat level 5 is the lowest threat level that can carry out an attack on a health care infrastructure. The attack can result in a physical impact such as endangering a patient life. Two attack scenarios can be achieved by threat level 5. The goal of both attacks is to successfully replay the transmitted data between the patient device and the EHR server. A replay attack would result in an incorrect data to be stored in the health data if a medical doctor sends a patient's treatment based on this data, the result can be catastrophic. This threat level has limited access to the system, a medium technical level of cyber knowledge, a medium stealth level and is ready to dedicate weeks to months to carry out the attack.

The result of our analysis also shows that threat level 1 is the highest level of threat to the healthcare IOT infrastructure. A threat level 1 is aiming to modify a strongly encrypted data during transmission. This could include swapping the names of the patients, changing the blood type of patients, and modifying the data that is used to decide the patient's infusion rate, etc.

Part of the attack nodes includes the interception of the network traffic, manipulating the data in real time, handling SSL / TLS encryption before finally forwarding the data.

For the healthcare system attack tree, five scenarios can be carried out by threat level 2. These attacks consist of a spoofing attack that is intended to deceive a doctor into inputting medical records into a fake domain, a spear phishing attack that is a precursor to getting the admin username and password for remote access to the EHR and finding a vulnerability in the server to perform a server exploitation remotely. The same attack scenarios can be carried out by threat level 3 and threat level 4. These attacks include a man in the middle attack on the drug infusion pump itself, a remote access attack on the controller and a server exploitation of the EHR server. These attacks cannot be performed by threat level 2 due to the decrease in their technical capability. We can also see at the end of the analysis that none of the attacks can be carried out by threat level 1, 2 and 3.

5.4.5. Results from the Wright-Patterson Air Force Base (WPAFB) fuels operation [57] attack tree.

The minimum threat level required to carry out an attack on an industrial SCADA infrastructure is threat level 3. Due to the AND function of the root node, for the attack to be achieved by any of the threat levels all attack paths must be achieved. Threat level 3 produced 36 scenarios which are the same as the total number of scenarios generated by the attack tree. This means that an attacker with high technical skill, limited level of access to the system, an elevated level of stealth and ready to dedicate months to years into planning and implementing the attack can carry out a successful attack. The maximum threat level required to carry out an attack on an industrial SCADA system to generate a physical result is threat level 1. The threat level 1 attacker will also be able to carry out all the 36 attack scenarios of the SCADA system attack tree and he does this with unlimited access to the system as well.

Although an attacker with threat level 3 can carry out the attack, result from the analysis shows that an attacker with threat level 2 cannot be able to perform the attack. This is because a threat agent with a threat level 2 only has a medium technical level of cyber knowledge although stealth and access indicators are high. For this reason, we can infer that the technical ability of an attacker is one of the most important indicators in analysing the capabilities of an attacker.

5.4.6. Results from the Sophistication Index analysis

Our analysis shows that directly trying to manipulate the drug infusion pump though from a remote location close enough to get a transmission has the lowest sophistication index. Remotely manipulating the data that is sent from the drug infusion pump either by modifying the packets or performing a replay attack has a SI score of 3. Also, sending the malicious commands to the controller has the same score. From our research, these attacks do not require an attacker installing an element of an APT or exploiting a zero-day vulnerability. From our result, this attack may be less sophisticated than the other attack scenarios, we learnt that the attack may require a very high level of technical know-how which is not limited to software and hardware hacking techniques alone. Attacking the EHR server generates an SI score of 4. If the EHR server data is not encrypted, or there is an improper SSL/TLS configuration, then it is possible that a motivated attacker modifies the EHR. To do this, the attacker may need element of social engineering, APT, stealth and remote administration. For our healthcare IoT infrastructure attack case scenario, the most sophisticated attack would be an attack to a properly secured EHR server. From our research, this may be possible if there exist a zero-day vulnerability in the web browser for example that allows an attacker to intercept and replay or modify an encrypted data. An attack of this nature is known to be very sophisticated with a SI score of 5.

The attack on the WPAFB to degrade fuel operation will need all the attack feature types to be successful i.e. APT, remote administration, zero-day vulnerability, stealth and social engineering. This gives it a total SI score of 5.

Table 16 Comparison table showing the differences in the attack sophistication levels

Research Questions	**Healthcare IoT Infrastructure**	**Industrial IoT Infrastructure**
What is the maximum attack sophistication required to generate a physical result using the threat levels?	Threat level 1	Threat level 1
What is the attack sophistication required to compromise the system to generate a physical result using threat levels?	Threat level 5 (lesser sophistication)	Threat level 3

What is the maximum attack sophistication required to generate a physical result using the SI?	SI score = 5	SI score = 5
What is the attack sophistication required to compromise the system to generate a physical result using SI?	SI score = 2 (lesser sophistication)	SI score = 5

Summary

This chapter describes how the value of each node of the attack tree is derived as well as the presentation of the result generated from the securlTree. analysis. For the healthcare IOT infrastructure attack tree, every node is described in detail, while for the SCADA IOT infrastructure, we relied on the data already provided by the referenced paper [57]. Although [57] provided values for the technical ability of each attach leaves, we tried as much as possible to get referenced data for the rest of the indicators such as stealth, access and time.

Once the data were correlated, we proceeded in inputting the corresponding value of each attack leaf in the securlTree tool and a threat level categorization table was generated. With this, we can know the lowest threat level of each IOT Infrastructure analysed.

We also used the methodology of [7] to generate a sophistication index for all our attack cases. With this, we can compare the sophistication level of SCADA and healthcare IOT infrastructures.

Finally, we discussed the results. In the discussion, we tried to analyse the reason for the differences based on the indicators related to each threat level. At the end, it became easier to draw an analysed conclusion rather than a thought or a mere claim. We found out that attacks can be conducted towards an IoT application such as the Healthcare IoT infrastructure with a lesser sophistication level requirements and still create a physical result. Table 15 shows a more general and conclusive result of the analysis.

6. Conclusion

The benefits of the ubiquitous connectivity in the Healthcare industry cannot be over-emphasized. In-fact it outweighs the possible attacks predicted in this thesis considering the over 2.5 million people that rely on IMDs in the United States. However, an increasing number of users comes with increased attention from manufacturers, security researchers, attackers and defenders. It is therefore important to understand some of the threats that are likely in this domain.

The outcome of our research shows that an attack does not require a high sophistication to generate a physical result. Contrary to the claims by [10] that cyberterrorism is not a near threat due to sophistication of attacks, this thesis has helped to understand clearly that there is a possibility. Terrorist organizations can opt for the less sophisticated attacks that will be less expensive to carry out and require a moderate level of technical-know how.

In the United Kingdom Cyber Security Strategy document for the year 2016 – 2021, it was highlighted that the technical capabilities of terrorists remain limited while they aim to destabilize the computer network operations in the UK, publicity and disruption remains their cyber goal [97]. The same document also emphasizes that for us to measure the success of a government in preventing terrorism, there is a need to fully understand the risk posed by cyber terrorism and the cyber threat from terrorist actors and hostile nation states [97]. This can be achieved through identification and investigation of cyber terrorism threats [97]. This thesis is a valuable input that addresses some of the concerns raised in the cyber security strategy document as it lays emphasis on attacks that create physical results which is one of the goals of a terrorist organization. The output of this thesis further proves the statement that "terrorists will likely use any cyber capability to achieve the maximum effect possible" [97]. "Thus, even a moderate increase in terrorist capability may constitute a significant threat to a state and its interest" [97].

References

[1] Ironpaper, "IronPaper," 04 Febuary 2016. [Online]. Available: http://www.ironpaper.com/webintel/articles/internet-of-things-market-statistics/. [Accessed 10 November 2016].

[2] G. O'Brien and G. Khanna, "Wireless Medical Infusion Pumps," National CyberSecurity Center of Excellence, 2014.

[3] S. Gold, "The SCADA Challenge: Securing Critical Infrastructure," 2009.

[4] C. Guitton and E. Korzak, "The Sophistication Criterion for Attribution," *The RUSI Journal,* vol. 158, no. 4, pp. 62 - 68, 2013.

[5] T. R. Ingoldsby, "Attack Tree-based Threat Risk Analysis," Amenaza Technologies Ltd., 2013.

[6] M. Mateski, C. M. Trevino, C. K. Veitch, J. Michalski, J. M. Harris, S. Maruoka and J. Frye, "Cyber Threat Metrics," Sandia National Laboratories, 2012.

[7] S. Goel and N. DePaula, "A Sophistication Index for Evaluating Security Breaches," in *11th Annual Symposium on Information Assurance Asia*, Albany, New York, 2016.

[8] T. M. Chen, "Cyberterrorism After Stuxnet," in *Strategic Studies Institute and U.S. Army War College*.

[9] B. Mitko and P. Drage, "Cyber Terrorism - Global Security Threat," *International Scientific Defence, Security and Peace Journal,* 2013.

[10] M. Conway, "Reality Check: Assessing the (Un) likelihood of Cyberterrorism," Springer, New york, 2014.

[11] K. Sengupta, "Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images," 7 Feb 2017. [Online]. Available: http://www.independent.co.uk/news/uk/crime/isis-islamist-hackers-nhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html. [Accessed 15 April 2017].

[12] A. Mulero, "Charts: Must-know healthcare cybersecurity statistics," 27 Feb 2017. [Online]. Available: http://www.healthcaredive.com/news/must-know-healthcare-cybersecurity-statistics/435983/. [Accessed 17 April 2017].

[13] E. Gershfang, "Ransomware and Healthcare," OWASP , Montreal , 2016.

[14] Wu-Zhao, L. Lei-Hong, H. Yue-shan and W. X. Ming, "A Community Health Service Architecture Based on Internet of Things on Healthcare," in *World Conference on Medical Physics and Biomedical Engineering*, 2013.

[15] A. Nicholson, S. Webber, S. Dyer, T. Patel and H. Janicke, "SCADA security in the light of Cyber-Warfare," *Computers and Security,* vol. 31, pp. 418 - 436, 2012.

[16] A. Sarwate, "SCADA Security: Why is it so hard?," 2011.

[17] ICIT - Institute for Critical Infrastructure Technology, "Hacking Healthcare IT in 2016," 2016.

[18] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno and W. H. Maisel, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," *IEEE Symposium on Security and Privacy,* 2008.

[19] S. D. Hall, "Healthcare lessons learned from 'hacktivist' attack," 1 Aug 2014. [Online]. Available: http://www.fiercehealthcare.com/it/healthcare-lessons-learned-from-hacktivist-attack. [Accessed 29 March 2017].

[20] Radware, "DDoS Case Study: DDoS Attack Mitigation Boston Children's Hospital," 21 Oct 2015. [Online]. Available: https://security.radware.com/ddos-experts-insider/ert-case-studies/boston-childrens-hospital-ddos-mitigation-case-study/. [Accessed 29 March 2017].

[21] K. Zetter, "Why Hospitals Are the Perfect Targets for Ransomware," 30 March 2016. [Online]. Available: https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/. [Accessed 29 March 2017].

[22] T. Mog, "HOLLYWOOD HOSPITAL PAYS $17,000 TO RANSOMWARE HACKERS," 18 Feb 2016. [Online]. Available: http://www.digitaltrends.com/computing/hollywood-hospital-ransomware-attack/. [Accessed 29 March 2017].

[23] D. H. a. P. M. Yellowlees, "Cyberterrorism: Is the U.S. Healthcare System Safe?," *Telemedicine and e-Health,* vol. 19, no. 1, 2014.

[24] L. Ayala, Cyber security for Hospitals and Healthcare Facilities: A guide to detection and Prevention, Virginia: aPress, 2016.

[25] FORTINET, "Four Ramifications of Cyber Attacks on Healthcare Systems," 10 March 2017. [Online]. Available: https://blog.fortinet.com/2017/03/10/four-ramifications-of-cyber-attacks-on-the-nhs-and-other-healthcare-systems. [Accessed 14 April 2017].

[26] M. Chalfant, "Cybercriminals catching up to sophisticated nations state actors, firm says," 14 Mar 2017. [Online]. Available: http://thehill.com/policy/cybersecurity/323879-cyber-criminals-catching-up-to-sophisticated-nation-state-actors-firm. [Accessed 21 April 2017].

[27] K. Zetter, "Inside cunning unprecedented hack of ukraine's power grid," 3 Mar 2016. [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. [Accessed 21 April 2017].

[28] P. Polityuk, "Ukraine to probe suspected Russian cyber attack on grid," 31 Dec 2015. [Online]. Available: http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UE0ZZ20151231. [Accessed 21 April 2017].

[29] V. Pournaghshband, M. Sarrafzadeh and P. Reiher, "Securing Legacy Mobile Medical Devices," 2011.

[30] K. Habib and W. Leister, "Threats Identification for the Smart Internet of Things in e-Health and Adaptive Security Countermeasures," 2015.

[31] B. Gorenc, "Understanding the attack surface of critical infrastructure," 8 Aug 2016. [Online]. Available: http://blog.trendmicro.com/understanding-the-attack-surface-for-critical-infrastructure/. [Accessed 18 April 2017].

[32] A. J. S. S. Bonnie Zhu, "A Taxonomy of Cyber Attacks on SCADA Systems," California, 2012.

[33] C. D. Schuett, "PROGRAMMABLE LOGIC CONTROLLER MODIFICATION ATTACKS FOR USE IN DETECTION ANALYIS," 2014.

[34] E. J. Byres, M. Franz and D. Miller, "The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems," 2004.

[35] T. H. Morris1 and W. Gao, "Industrial Control System Cyber Attacks," in *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research* , Missisipi, 2013.

[36] A. Nicholson, S. Webber, S. Dyer, T. Patel and H. Janicke, "SCADA security in the light of cyber warfare," *Computer and Security,* vol. 31, pp. 418-436, 2012.

[37] H. Kim, "Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks," *International Journal of Distributed Sensor Networks,* p. 5, 2012.

[38] Electricity Information Sharing and Analysis Center, "Analysis of the Cyber Attack on the Ukrainian Power Grid," SANS, 2016.

[39] D. Ford, "Cheney's defibrillator was modified to prevent hacking," 24 Oct 2013. [Online]. Available: http://edition.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/. [Accessed 15 April 2017].

[40] R. Luscombe, "Dick Cheney heart assasination attack," 19 Oct 2013. [Online]. Available: https://www.theguardian.com/world/2013/oct/19/dick-cheney-heart-assassination-fear. [Accessed 14 April 2017].

[41] BBC, "Dick Cheney: Heart implant attack was credible," 21 Oct 2013. [Online]. Available: http://www.bbc.com/news/technology-24608435. [Accessed 14 April 2017].

[42] TrapX Research Labs, "Anatomy of Attack: MedJack 2.0 - Hospitals Under Siege," TrapX software, 2016.

[43] United States Department of Homeland Security, "Growing Trend of Ransomware Attacks Targeting Hospitals and Healthcare," Kentucky, 2016.

[44] G. Viña, "Patients in limbo as cyber attack shuts three hospitals," 2 Nov 2016. [Online]. Available: https://www.ft.com/content/1292d25c-a12a-11e6-891e-abe238dee8e2. [Accessed 17 April 2017].

[45] M. Kumar, "Hundreds Of Operations Canceled After Malware Hacks Hospitals Systems," 3 Nov 2016. [Online]. Available: http://thehackernews.com/2016/11/hospital-cyber-attack-virus.html. [Accessed 17 April 2017].

[46] J. Madary, "Addressing cybersecurity vulnerabilitites and threats to Implantable Medical Devices," 2016.

[47] Centre for Connected Health policy, "The FDA and Mobile Medical Applications," Sacremento, california, 2015.

[48] FDA, "Medical Devices," 6 April 2014. [Online]. Available: https://www.fda.gov/MedicalDevices/ResourcesforYou/Consumers/ucm142523.htm. [Accessed 24 March 2017].

[49] J. Xu, K. K. Venkatasubramanian and V. Sfyrla, "A Methodology for Systematic Attack Trees Generation for Interoperable Medical Devices," 2016.

[50] C. Li, A. Raghunathan and N. K. Jha, "Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System," in *IEEE 13th International Conference on e-Health Networking, Applications and Services*, 2011.

[51] P. Kumar and H.-J. Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," *Sensors,* vol. 12, pp. 55-90, 2012.

[52] P. Luckett, J. T. McDonald and W. B. Glisson, "Attack-Graph Threat Modeling Assessment of Ambulatory Medical Devices," in *Proceedings of the 50th Hawaii International Conference on System Sciences | 2017*, Hawaii, 2017.

[53] A. Almulhem, "Threat Modelling for Electronic Health Records," *Journal of Medical Systems ,* vol. 36, no. 5, 2011.

[54] A. Alqahtani, "Awareness of the Potential Threat of Cyberterrorism to the National Security," *Journal of Information Security,* vol. 5, pp. 137 - 146, 2014.

[55] M. Jason R. Nielsen, "EVALUATING INFORMATION ASSURANCE CONTROL EFFECTIVENESS ON AN AIR FORCE SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEM," 2011.

[56] ECRI Institute, "Top 10 health technology hazards of 2017," 2016.

[57] S. L. Grimes, "Biomedical Devices: Could Lack of Security Harm Patients?," in *HIMSS16*, Las Vegas, 2016.

[58] J. McDonald, S. Dean, D. Nielwolny, D. Garcia, N. Chhabra and L. Chang, "Integrated Circuits for Implantable Medical Devices," Freescale , 2011.

[59] M. Rushanan, A. D. Rubin, D. F. Kune, C. M. Swanson and A. Arbor, "SoK Security and Privacy in Implantable Medical Devices and Body Area Networks," 2014.

[60] K. B. Wellington, "Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions," *Santa Clara High Technology Law Journal,* vol. 30, no. 2, 2013.

[61] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu and W. H. Maisel, "Security and privacy for Implantable Medical Devices," *IEEE CS,* 2008.

[62] J. Xu, "Systematic Vulnerability Evaluation of Interoperable Medical Device System Using Attack Trees," Worchester, 2015.

[63] Jerome(Radcliffe, "Hacking Medical Devices for Fun and Insulin Breaking the Human SCADA system," 2011.

[64] S. Z. a. R. Hasan, "The EnemyWithin: The Emerging Threats to Healthcare from Malicious Mobile Devices," Birmingham, 2012.

[65] "Roundup: Preventing Medication Errors in Health Systems," 01 July 2008. [Online]. Available: http://www.pharmacytimes.com/publications/issue/2008/2008-07/2008-07-8601. [Accessed 19 Feb 2017].

[66] M. Eriksson, "An Example of a Man-in-the-middle Attack Against Server Authenticated SSL sessions," 2002.

[67] Amenaza Technologies Ltd., "Introduction to SecurITree," 2017.

[68] Amenaza Technoogies Ltd., "Introduction to Pruning," 2017.

[69] D. P. Duggan, S. R. Thomas, C. K. K. Veitch and a. L. Woodard, "Categorizing Threat: Building and Using a Generic Threat Matrix," Sandia National Laboratories, California, 2007.

[70] H. Zhu and S. Du, "Security Assessment via Attack Tree Model," in *Securitty Assessment in Vehicukar Networks*, Springer, 2013, p. 14.

[71] W. B. Glisson, T. Andel, T. McDonald, M. Jacobs, M. Campbell and J. Mayr, "Compromising a Medical Mannequin," Alabama, 2015.

[72] Mitre - Adversary Tactics Techniques and Common Knowledge, "Brute Force," 14 June 2016. [Online]. Available: https://attack.mitre.org/wiki/Technique/T1110. [Accessed 25 March 2017].

[73] L. Ayala, "How Hackers can Gain Access to Healthcare Facility or Hospital Network," in *Cybersecurity for Hospitals and Healthcare Facilities : A Guide to Detection and Prevention*, Apress, 2016, p. 16.

[74] INFOSEC institute, "Popular Tools for Brute-force Attacks," 29 Dec 2016. [Online]. Available: http://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/. [Accessed 19 March 2017].

[75] The Institutuion of Engineering and Technology, "Jamming & radio interference: understanding the impact," Essential Engineering Intelligence for Information & Communications.

[76] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Medical Devices: Evidence and Research,* 2015.

[77] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," 2013.

[78] J. Finkle, "Technology News," REUTERS, 4 Oct 2016. [Online]. Available: http://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L. [Accessed 7 March 2017].

[79] D. G. Koenig, "Security and Privacy of Wireless Implantable Medical Devices," 2013.

[80] H. F. Tipton and M. Krause, Information System Management Handbook, Auerbach, 2004, pp. 294 - 296.

[81] T. Parker, E. Shaw, E. Stroz, M. G. Defost and M. H. Sachs, Cyber Adversary Characterization: Rating the attack - Post Incident Characterization Metrics, Syngress, 2004, p. 87.

[82] B. Claypool, "Global Information Assurance Certification Paper," SANS Institute, 2002.

[83] OWASP, "SQL Injection," 4 Oct 2016. [Online]. Available: https://www.owasp.org/index.php/SQL_Injection. [Accessed 23 March 2017].

[84] MITRE - Common Attack Patter Enumeration and Classification, "CAPEC 66 - SQL Injection," 7 Dec 2015. [Online]. Available: https://capec.mitre.org/data/definitions/7.html. [Accessed 23 March 2017].

[85] J. Panella, "Web Application Security and the OWASP Top 10," Sapient Nitro, 2011.

[86] IBM, "Injection Attacks," [Online]. Available: https://www.ibm.com/support/knowledgecenter/en/SSB2MG_4.6.0/com.ibm.ips.doc/concepts/wap_injection_attacks.htm. [Accessed 23 March 2017].

[87] MITRE - Common Attack Patter Enumeration and Classification, "CAPEC-88: OS Command Injection," 7 Dec 2015. [Online]. Available: https://capec.mitre.org/data/definitions/88.html. [Accessed 23 March 2017].

[88] A. Prakesh, "Module 3: Scanning," in *Hack the world - Ethical Hacking*, Hacking Corporation.

[89] MITRE - Common Attack Patter Enumeration and Classification, "CAPEC 70: Try Common(default) Usernames and Passwords," 7 Dec 2015. [Online]. Available: https://capec.mitre.org/data/definitions/70.html. [Accessed 23 March 2017].

[90] M. -. C. A. P. E. a. Classification, "CAPEC-94: Man in the Middle Attack," 7 Dec 2015. [Online]. Available: https://capec.mitre.org/data/definitions/94.html. [Accessed 23 March 2017].

[91] D. Ma, L. Wang, C. Lei, Z. Xu, H. Zhang and M. Li, "Thwart eavesdropping attacks on network communication based on moving target defense," Hong Kong, 2016.

[92] Mitre - Ccommon Weakness Enumeration, "CWE-294: Authentication Bypass by Capture-replay," 18 Jan 2017. [Online]. Available: http://cwe.mitre.org/data/definitions/294.html. [Accessed 23 March 2017].

[93] Mitre - Common Attack Pattern Enumeration and Classification, "CAPEC-60: Reusing Session IDs (aka Session Replay)," 07 Dec 2015. [Online]. Available: http://capec.mitre.org/data/definitions/60.html. [Accessed 23 March 2017].

[94] Mitre - Common Attack Pattern Enrumeration and Classification, "CAPEC-217: Exploiting Incorrectly Configured SSL," 07 Dec 2015. [Online]. Available: https://capec.mitre.org/data/definitions/217.html. [Accessed 23 March 2017].

[95] IMPERVA, "Advanced Persistent Threat: Are you the next target?," 2011.

[96] P. Mueller and B. Yadegari, "The STUXNET worm," 2010.

[97] HM Government, "NATIONAL CYBER SECURITY STRATEGY 2016-2021," United Kingdom, 2016.

[98] N. Paul and T. Kohno, "Security Risks, Low-tech User Interfaces, and Implantable Medical Devices: A Case Study with Insulin Pump Infusion Systems," 2011.

[99] D. Hutter, "Physical Security and Why It Is Important," SANS Institute Infosec Reading Room, 2016.

[100] Personal Connected Health Alliance, "Fundamentals of Data Exchange," 2015.

[101] C. Silcock, "Four Ramifications of Cyber Attacks on Healthcare Systems," 10 Mar 2017. [Online]. Available: https://blog.fortinet.com/2017/03/10/four-ramifications-of-cyber-attacks-on-the-nhs-and-other-healthcare-systems. [Accessed 15 April 2017].

[102] M. M. Baig, H. GholamHosseini and M. J. Connolly, "Mobile healthcare applications: system design review, critical issues and challenegs," *Australas Phys Eng Sci Med,* vol. 38, pp. 23-38, 2015.

[103] Schneider Electric, "SCADA systems - Telemetric and SCADA solutions," Schneider Electric, 2012.

[10 N. Leavitt, "Researchers Fight to Keep Implantable Medical Devices Safe from Hackers," 2010. 4]

Appendices

Appendix A – The SecurlTree

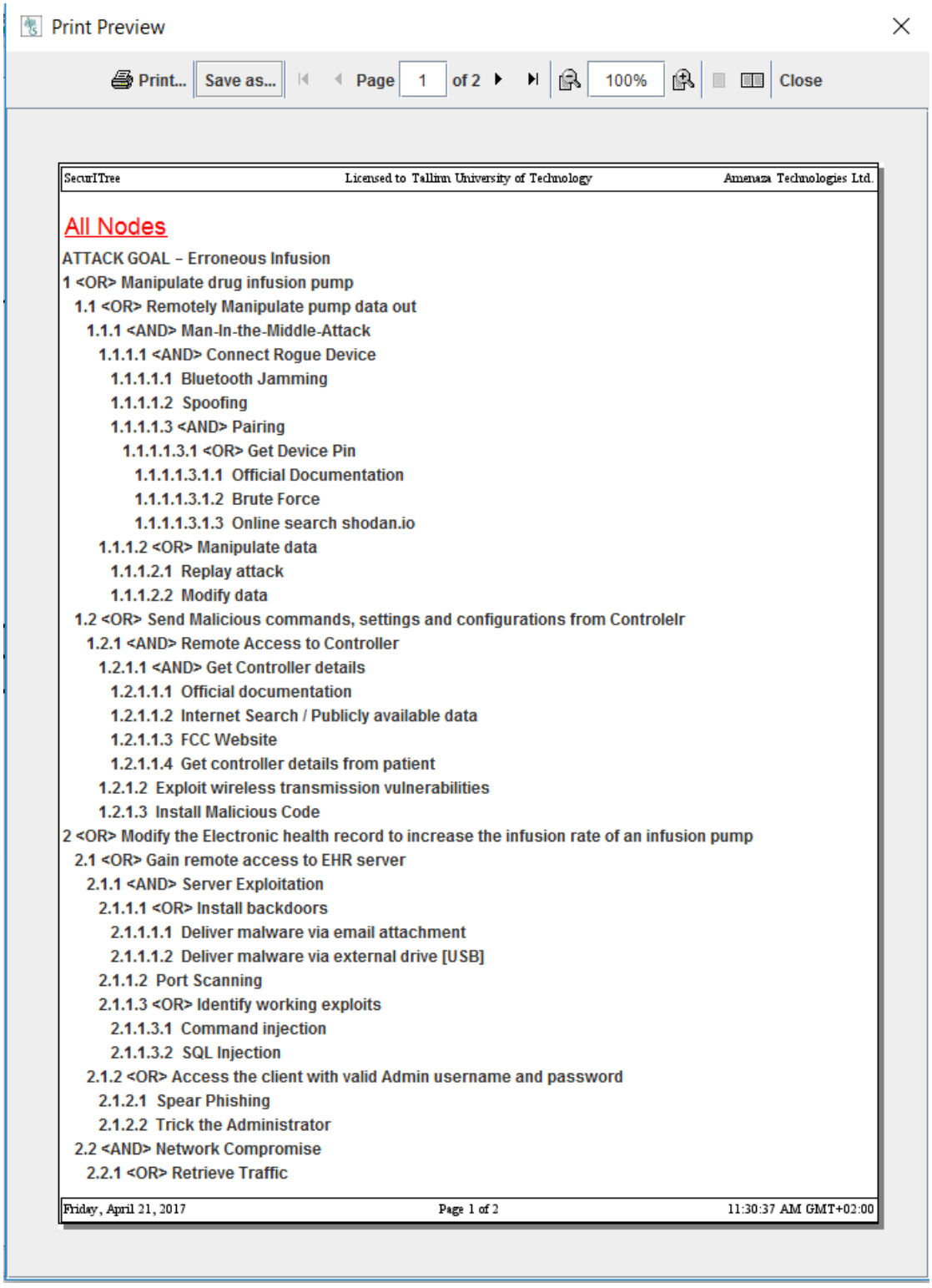


Figure A.1 An attack tree to a Healthcare IoT infrastrucure – Page 1

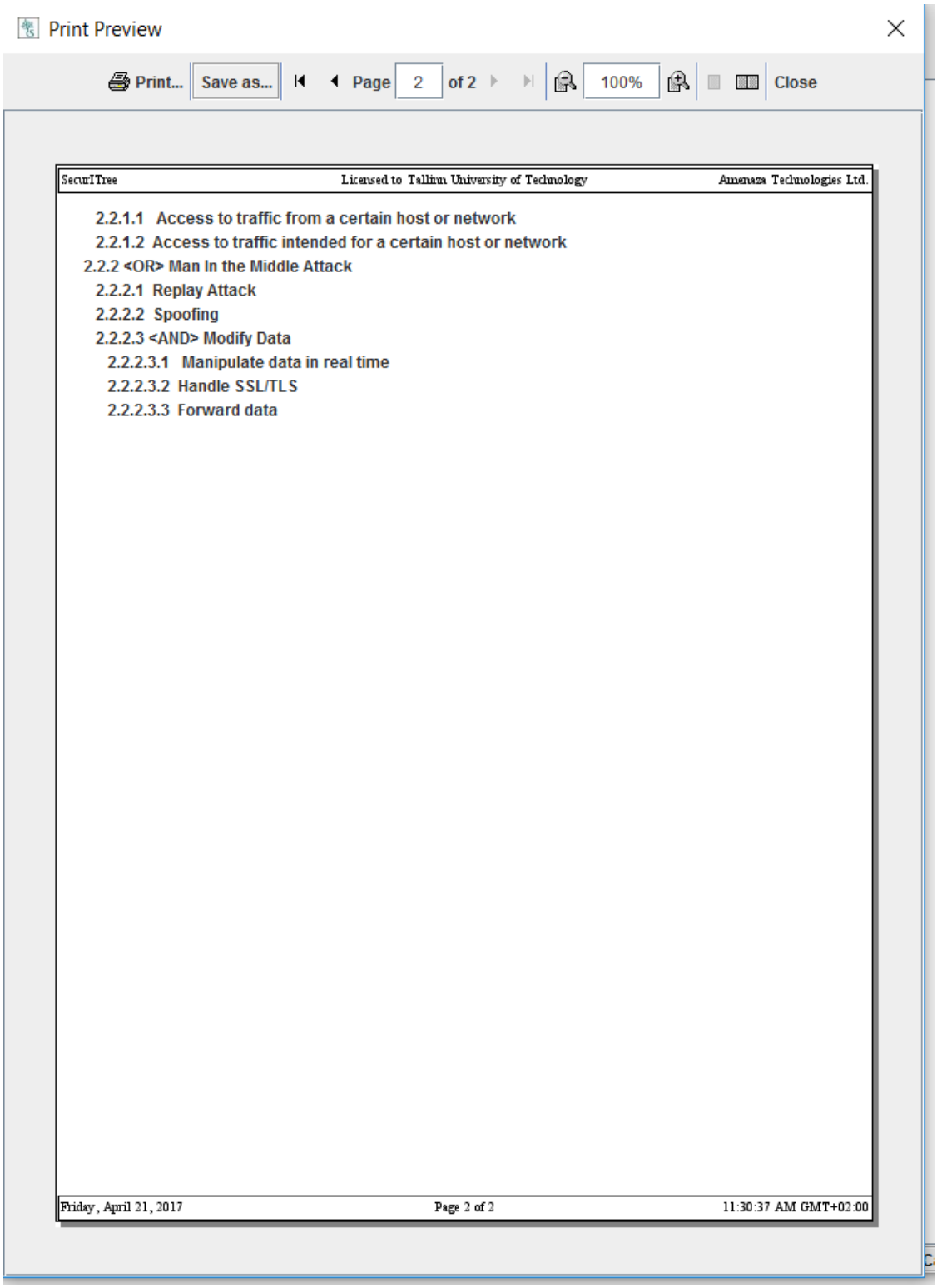


Figure A.2 An attack tree to a Healthcare IoT infrastrucure – Page 2

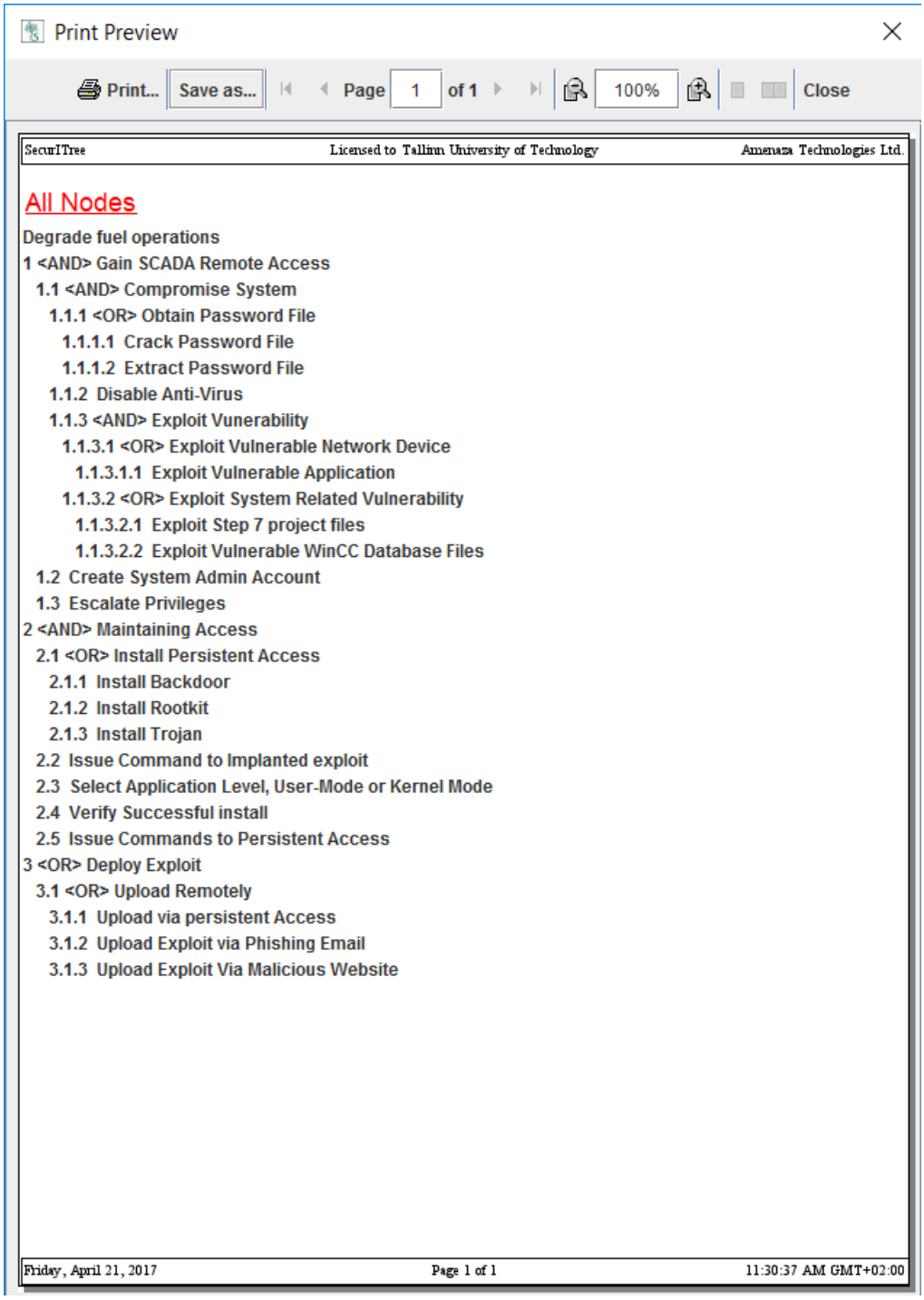


Figure A.3 An attack tree to degrade the fuel operations of the WPAFB

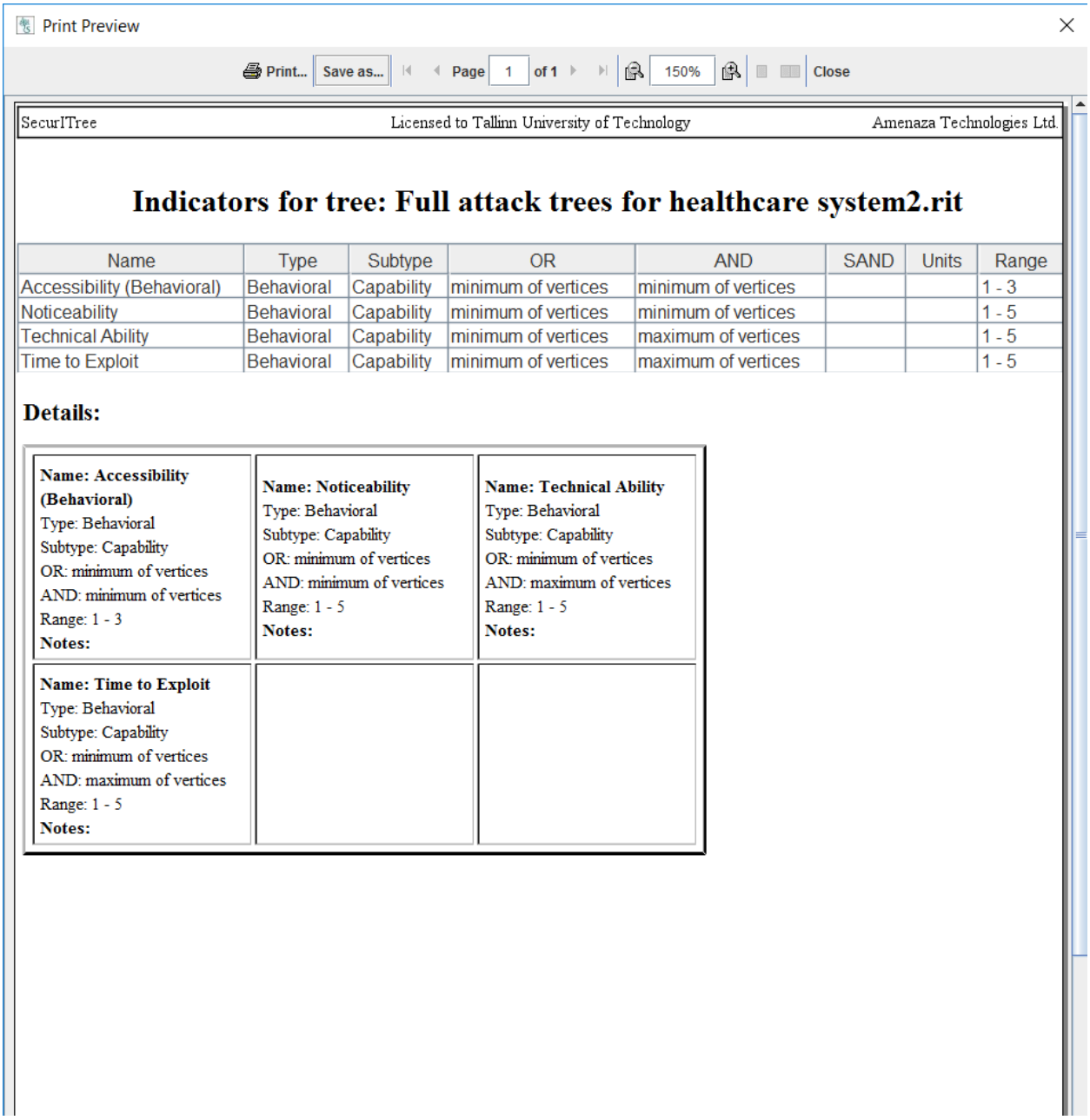
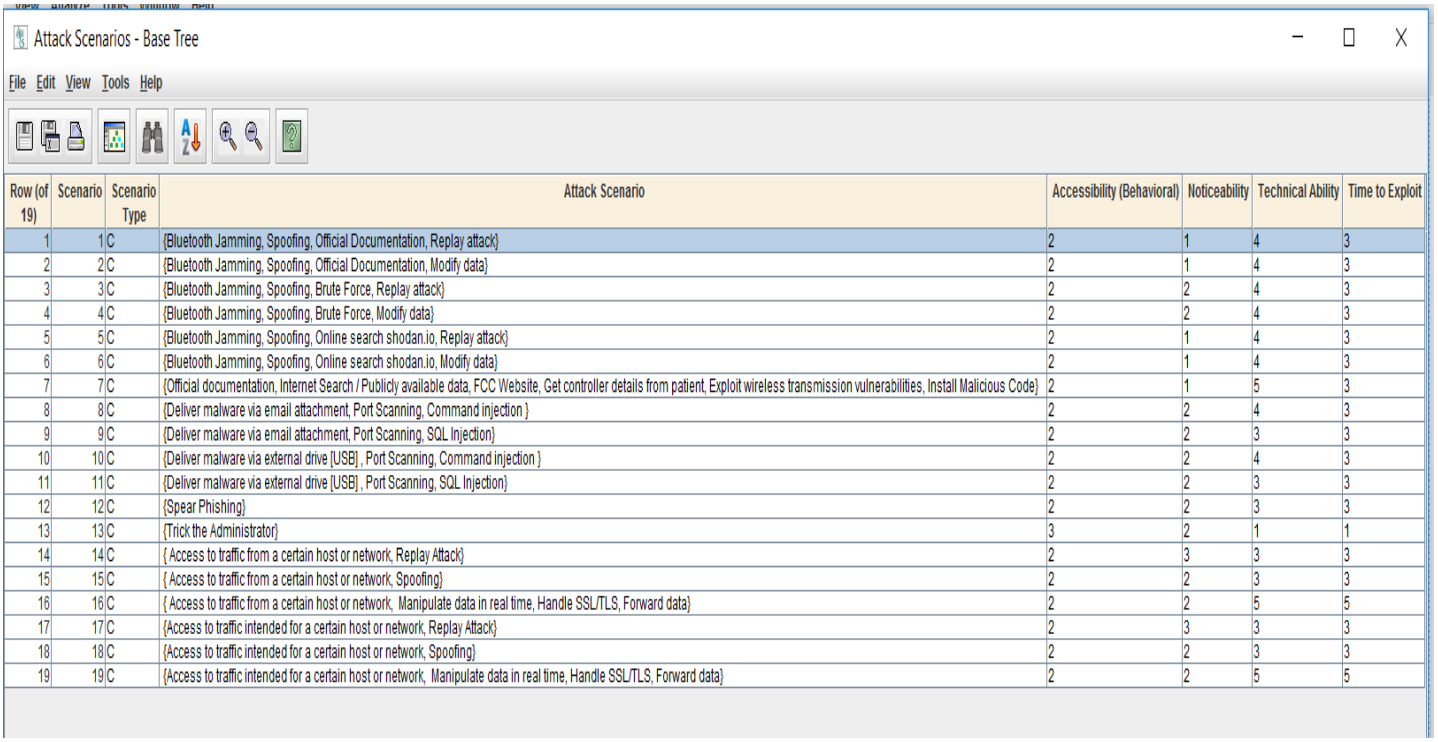
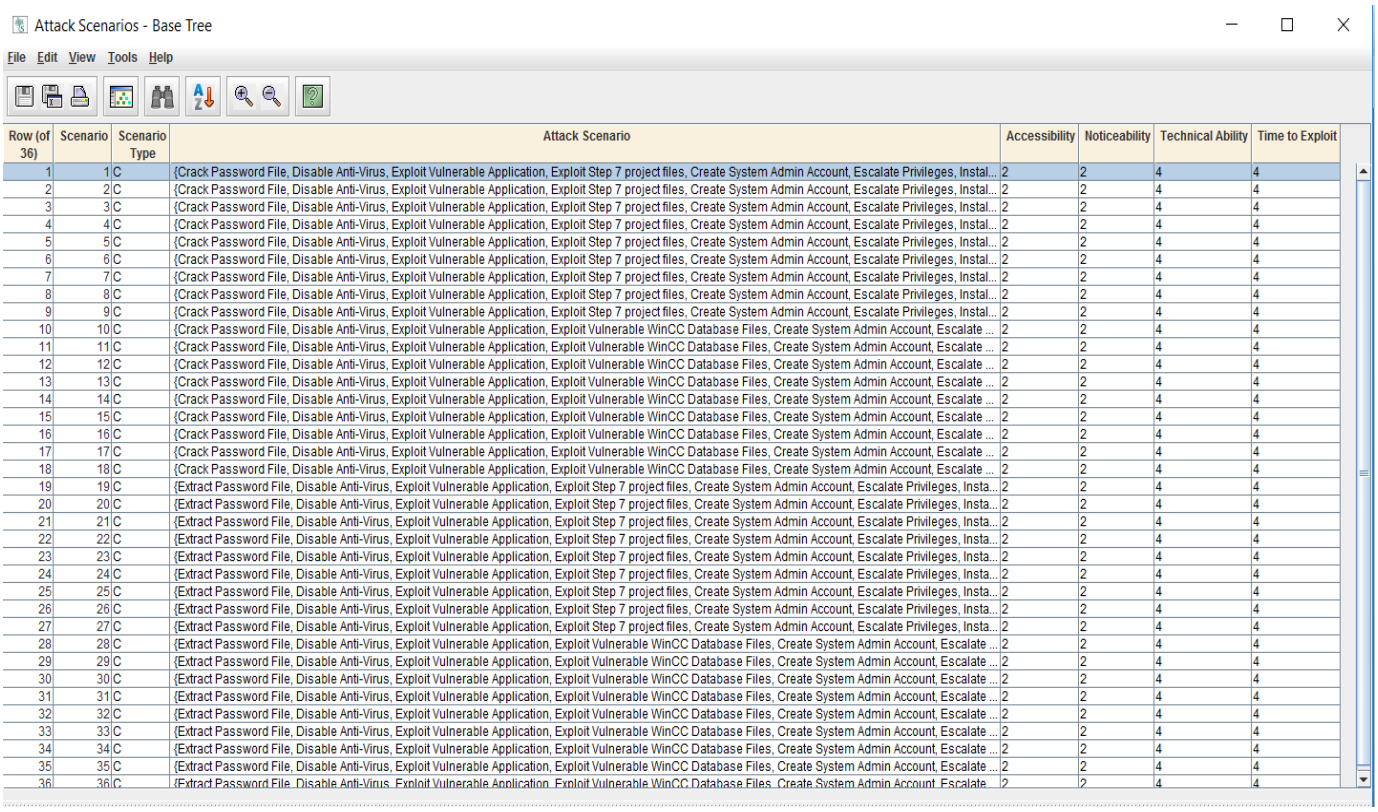


Figure A.4 Attack indicators and the capability ranges



Row (of 19)	Scenario	Scenario Type	Attack Scenario	Accessibility (Behavioral)	Noticeability	Technical Ability	Time to Exploit
1	1	C	{Bluetooth Jamming, Spoofing, Official Documentation, Replay attack}	2	1	4	3
2	2	C	{Bluetooth Jamming, Spoofing, Official Documentation, Modify data}	2	1	4	3
3	3	C	{Bluetooth Jamming, Spoofing, Brute Force, Replay attack}	2	2	4	3
4	4	C	{Bluetooth Jamming, Spoofing, Brute Force, Modify data}	2	2	4	3
5	5	C	{Bluetooth Jamming, Spoofing, Online search shodan.io, Replay attack}	2	1	4	3
6	6	C	{Bluetooth Jamming, Spoofing, Online search shodan.io, Modify data}	2	1	4	3
7	7	C	{Official documentation, Internet Search / Publicly available data, FCC Website, Get controller details from patient, Exploit wireless transmission vulnerabilities, Install Malicious Code}	2	1	5	3
8	8	C	{Deliver malware via email attachment, Port Scanning, Command injection }	2	2	4	3
9	9	C	{Deliver malware via email attachment, Port Scanning, SQL Injection}	2	2	3	3
10	10	C	{Deliver malware via external drive [USB] , Port Scanning, Command injection }	2	2	4	3
11	11	C	{Deliver malware via external drive [USB] , Port Scanning, SQL Injection}	2	2	3	3
12	12	C	{Spear Phishing}	2	2	3	3
13	13	C	{Trick the Administrator}	3	2	1	1
14	14	C	{ Access to traffic from a certain host or network, Replay Attack}	2	3	3	3
15	15	C	{ Access to traffic from a certain host or network, Spoofing}	2	2	3	3
16	16	C	{ Access to traffic from a certain host or network, Manipulate data in real time, Handle SSL/TLS, Forward data}	2	2	5	5
17	17	C	{Access to traffic intended for a certain host or network, Replay Attack}	2	3	3	3
18	18	C	{Access to traffic intended for a certain host or network, Spoofing}	2	2	3	3
19	19	C	{Access to traffic intended for a certain host or network, Manipulate data in real time, Handle SSL/TLS, Forward data}	2	2	5	5

Fig A.5 Healthcare IoT infrastructure derived attack Scenarios



Row (of 36)	Scenario	Scenario Type	Attack Scenario	Accessibility	Noticeability	Technical Ability	Time to Exploit
1	1	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Instal...	2	2	4	4
2	2	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Instal...	2	2	4	4
3	3	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Instal...	2	2	4	4
4	4	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Instal...	2	2	4	4
5	5	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Instal...	2	2	4	4
6	6	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Instal...	2	2	4	4
7	7	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Instal...	2	2	4	4
8	8	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Instal...	2	2	4	4
9	9	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Instal...	2	2	4	4
10	10	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
11	11	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
12	12	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
13	13	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
14	14	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
15	15	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
16	16	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
17	17	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
18	18	C	{Crack Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
19	19	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Insta...	2	2	4	4
20	20	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Insta...	2	2	4	4
21	21	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Insta...	2	2	4	4
22	22	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Insta...	2	2	4	4
23	23	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Insta...	2	2	4	4
24	24	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Insta...	2	2	4	4
25	25	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Insta...	2	2	4	4
26	26	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Insta...	2	2	4	4
27	27	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Step 7 project files, Create System Admin Account, Escalate Privileges, Insta...	2	2	4	4
28	28	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
29	29	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
30	30	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
31	31	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
32	32	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
33	33	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
34	34	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
35	35	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4
36	36	C	{Extract Password File, Disable Anti-Virus, Exploit Vulnerable Application, Exploit Vulnerable WinCC Database Files, Create System Admin Account, Escalate ...	2	2	4	4

Fig A.6 Industrial IoT infrastructure derived attack Scenarios

Reports

File Reports

Select report type: Attack Scenarios ☑ Wrap Cell Text

Attack Scenarios

Row (of 11)	Scenario	Scenario Type	Attack Scenario	Accessibility (Behavioral)	Noticeability	Technical Ability	Time to Exploit
1	1	C	{Bluetooth Jamming, Spoofing, Official Documentation, close to the pump, Replay attack}	2	1	4	3
2	2	C	{Bluetooth Jamming, Spoofing, Official Documentation, close to the pump, Modify data}	2	1	4	3
3	3	C	{Bluetooth Jamming, Spoofing, Brute Force, close to the pump, Replay attack}	2	2	4	3
4	4	C	{Bluetooth Jamming, Spoofing, Brute Force, close to the pump, Modify data}	2	2	4	3
5	5	C	{Bluetooth Jamming, Spoofing, Online search shodan.io, close to the pump, Replay attack}	2	1	4	3
6	6	C	{Bluetooth Jamming, Spoofing, Online search shodan.io, close to the pump, Modify data}	2	1	4	3
7	7	C	{Official documentation, Internet Search / Publicly available data, FCC Website, Get controller details from patient, Exploit wireless transmission vulnerabilities, Install Malicious Code}	2	1	5	3
8	8	C	{Deliver malware via email attachment, Port Scanning, Command injection }	2	2	4	3
9	9	C	{Deliver malware via external drive [USB] , Port Scanning, Command injection }	2	2	4	3
10	10	C	{ Access to traffic from a certain host or network, Manipulate data in real time, Handle SSL/TLS, Forward data}	2	2	5	5
11	11	C	{Access to traffic intended for a certain host or network, Manipulate data in real time, Handle SSL/TLS, Forward data}	2	2	5	5

Fig A.7. Attack Scenarios for Threat Level 1 – Healthcare IOT attack Tree

Reports

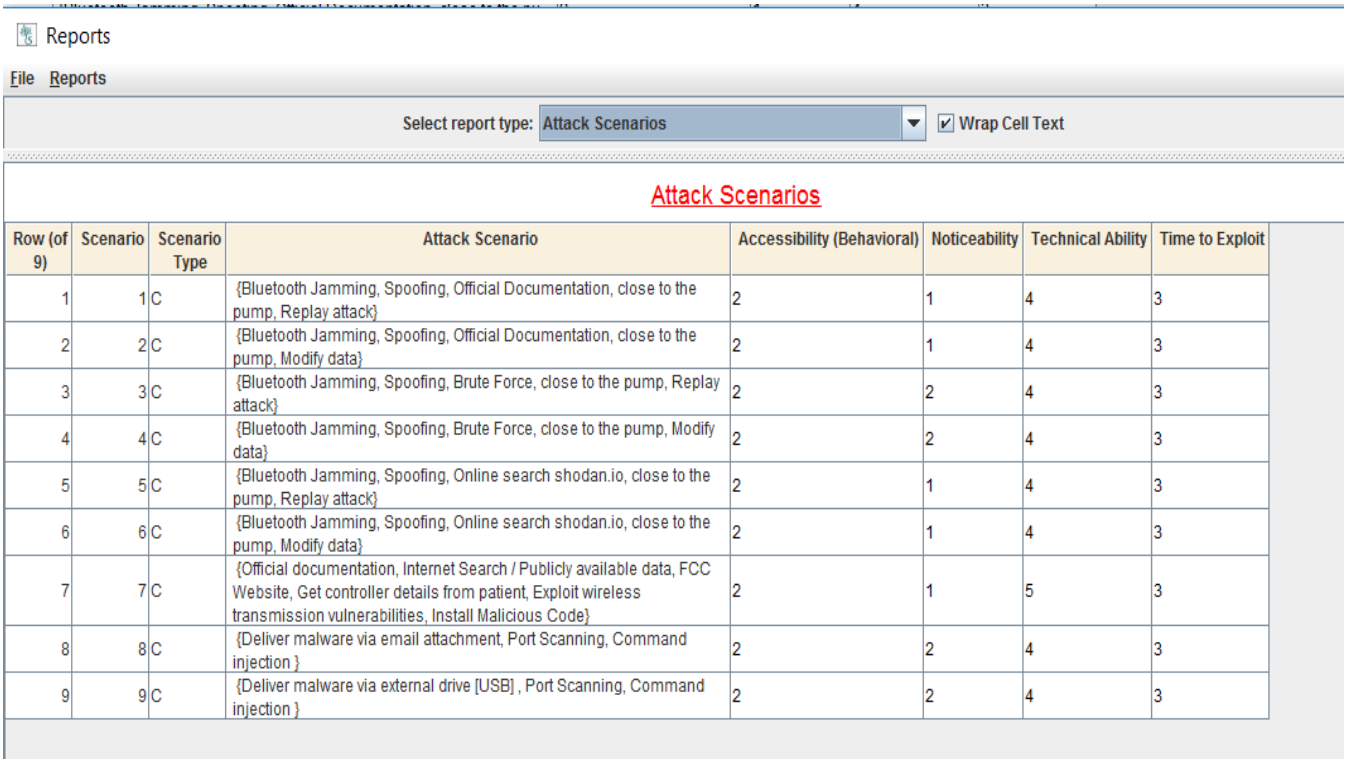
File Reports

Select report type: Attack Scenarios ☑ Wrap Cell Text

Attack Scenarios

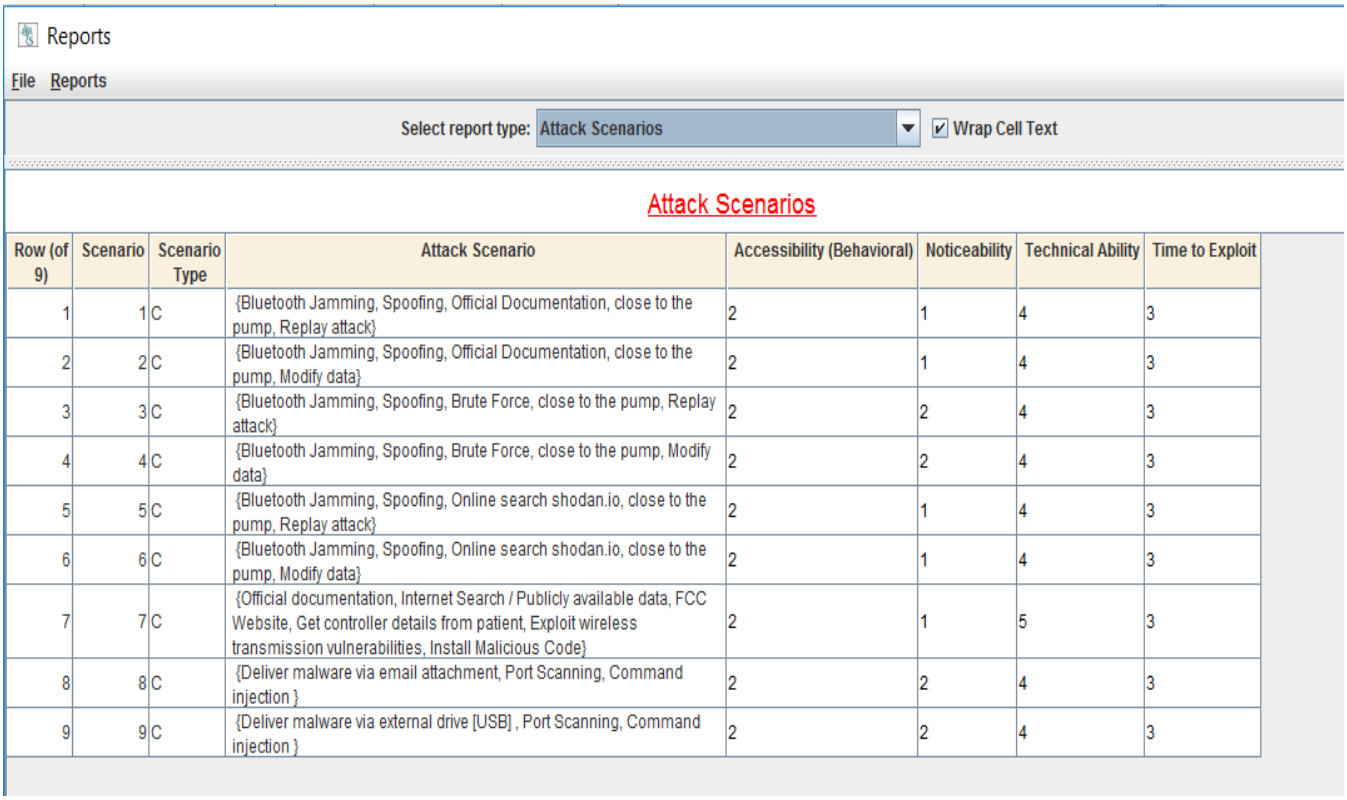
Row (of 5)	Scenario	Scenario Type	Attack Scenario	Accessibility (Behavioral)	Noticeability	Technical Ability	Time to Exploit
1	1	C	{Deliver malware via email attachment, Port Scanning, SQL Injection}	2	2	3	3
2	2	C	{Deliver malware via external drive [USB] , Port Scanning, SQL Injection}	2	2	3	3
3	3	C	{Spear Phishing}	2	2	3	3
4	4	C	{ Access to traffic from a certain host or network, Spoofing}	2	2	3	3
5	5	C	{Access to traffic intended for a certain host or network, Spoofing}	2	2	3	3

Fig A.8. Attack Scenarios for Threat Level 2 – Healthcare IOT attack Tree



Row (of 9)	Scenario	Scenario Type	Attack Scenario	Accessibility (Behavioral)	Noticeability	Technical Ability	Time to Exploit
1	1	C	{Bluetooth Jamming, Spoofing, Official Documentation, close to the pump, Replay attack}	2	1	4	3
2	2	C	{Bluetooth Jamming, Spoofing, Official Documentation, close to the pump, Modify data}	2	1	4	3
3	3	C	{Bluetooth Jamming, Spoofing, Brute Force, close to the pump, Replay attack}	2	2	4	3
4	4	C	{Bluetooth Jamming, Spoofing, Brute Force, close to the pump, Modify data}	2	2	4	3
5	5	C	{Bluetooth Jamming, Spoofing, Online search shodan.io, close to the pump, Replay attack}	2	1	4	3
6	6	C	{Bluetooth Jamming, Spoofing, Online search shodan.io, close to the pump, Modify data}	2	1	4	3
7	7	C	{Official documentation, Internet Search / Publicly available data, FCC Website, Get controller details from patient, Exploit wireless transmission vulnerabilities, Install Malicious Code}	2	1	5	3
8	8	C	{Deliver malware via email attachment, Port Scanning, Command injection }	2	2	4	3
9	9	C	{Deliver malware via external drive [USB] , Port Scanning, Command injection }	2	2	4	3

Fig A.9. Attack Scenarios for Threat Level 3 – Healthcare IOT attack Tree



Reports

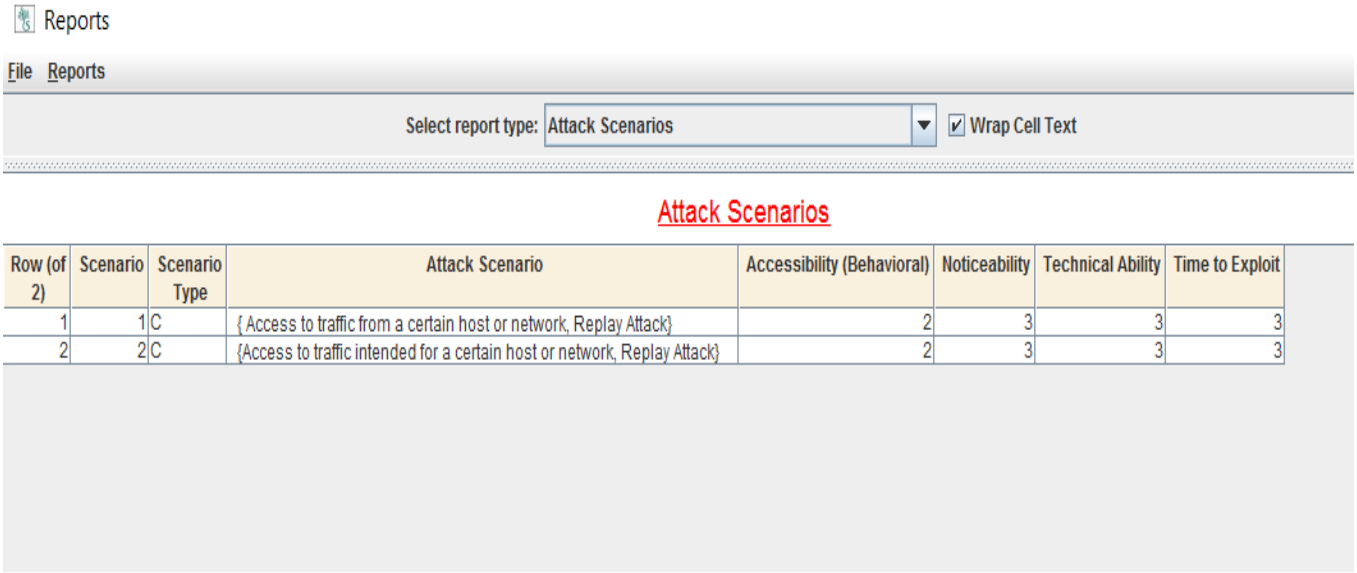
File Reports

Select report type: Attack Scenarios ☑ Wrap Cell Text

Attack Scenarios

Row (of 9)	Scenario	Scenario Type	Attack Scenario	Accessibility (Behavioral)	Noticeability	Technical Ability	Time to Exploit
1	1	C	{Bluetooth Jamming, Spoofing, Official Documentation, close to the pump, Replay attack}	2	1	4	3
2	2	C	{Bluetooth Jamming, Spoofing, Official Documentation, close to the pump, Modify data}	2	1	4	3
3	3	C	{Bluetooth Jamming, Spoofing, Brute Force, close to the pump, Replay attack}	2	2	4	3
4	4	C	{Bluetooth Jamming, Spoofing, Brute Force, close to the pump, Modify data}	2	2	4	3
5	5	C	{Bluetooth Jamming, Spoofing, Online search shodan.io, close to the pump, Replay attack}	2	1	4	3
6	6	C	{Bluetooth Jamming, Spoofing, Online search shodan.io, close to the pump, Modify data}	2	1	4	3
7	7	C	{Official documentation, Internet Search / Publicly available data, FCC Website, Get controller details from patient, Exploit wireless transmission vulnerabilities, Install Malicious Code}	2	1	5	3
8	8	C	{Deliver malware via email attachment, Port Scanning, Command injection }	2	2	4	3
9	9	C	{Deliver malware via external drive [USB] , Port Scanning, Command injection }	2	2	4	3

Fig A.10. Attack Scenarios for Threat Level 4 – Healthcare IOT attack Tree



Reports

File Reports

Select report type: Attack Scenarios ☑ Wrap Cell Text

Attack Scenarios

Row (of 2)	Scenario	Scenario Type	Attack Scenario	Accessibility (Behavioral)	Noticeability	Technical Ability	Time to Exploit
1	1	C	{ Access to traffic from a certain host or network, Replay Attack}	2	3	3	3
2	2	C	{Access to traffic intended for a certain host or network, Replay Attack}	2	3	3	3

Fig A.11. Attack Scenarios for Threat Level 5 – Healthcare IOT attack Tree

Appendix B

Table B.1 Definitions of the attack feature types and their respective SI score [7]

Feature Type	Explanation	
Social Engineering	Social engineering has generally been highlighted as an important sophistication characteristic, but by itself it may not require much sophistication. We consider targeted forms of social engineering such as *spear-phishing* to add an additional score.	1
Remote Administration	An attack is sophisticated if it is successful. However, some purposes may require little skill or resources. Attacks that contain a *remote administration tool* or *backdoor* receive an additional score.	1
Stealth	There are numerous anti-virus and anti-detection mechanisms which have been attributed as an important aspect of sophistication. However, they may also be part of standard tools. Attacks that use *root-kit* or *encryption* to hide its activities receive an additional score to the index.	1
Zero-Day Vulnerability Exploit	The vulnerability of the system indicates the level of sophistication required by an attack to exploit it. *Zero-day* vulnerabilities are difficult to find. However, they also may be purchased. One zero-day vulnerability adds an additional point to the score.	1
APT	Some attacks signal a higher level of organization and resource availability only present to certain actors. These attacks include various features, however the ones we deem most important are: *stolen digital signatures* and *multiple zero-day vulnerabilities*. The use of these features often assume the other features listed here as well.	1
E.g.	An attack that consists of a *zero-day exploit, spear phishing* and *root-kit* functionality receives a score of 3.	
	An attack that consists of *multiple zero days exploit, RAT, encryption, spear phishing and stolen digital signatures* receive a score of 5 – the highest possible.	

Table B.2 Security Breaches and their perceived sophistication and SI score [7]

Incident	PS	SI	Incident	PS	SI	Incident	PS	SI
2005-CardSystems	2.3	0	2010-Stuxnet	7.0	5	2013-Target	5.0	2
2005-University	3.3	0	2010-AT&T	5.0	0	2014-Neiman	2.7	0
2007-Ameritrade	4.0	1	2010-Aurora	6.0	4	2014-CHS	4.7	1
2007-HomeDepot	3.0	2	2010-CityLights	3.7	0	2014-EA	4.7	1
2007-TJX	3.0	0	2011-MAExecutive	5.0	1	2014-Forbes	3.0	0
2007-Monster	5.0	1	2011-RSA	5.7	4	2014-JPMorgan	3.7	2
2008-Comcast	2.3	1	2011-Citibank	4.0	1	2014-SONY	6.3	4
2008-Common	3.7	0	2012-SCDept	4.7	2	2015-Duqu	6.7	5
2008-Hannaford	4.3	2	2012-UtahDept	4.3	1	2015-IRS	2.7	0
2009-Heartland	4.0	1	2012-Yahoo	2.0	0	2015-OPM	5.3	3
2009-RockYou	2.7	0	2013-AdminOff	3.0	1			

Appendix C

Table C.1 General threat profile matrix [6]

Threat Level	THREAT PROFILE						
	Commitment			Resources			
					Knowledge		
	Intensity	Stealth	Time	Technical personnel	Cyber	Kinetic	Access
1	H	H	Years to decades	Hundreds	H	H	H
2	H	H	Years to decades	Tens of tens	M	H	M
3	H	H	Months to years	Tens of tens	H	M	M
4	M	H	Weeks to months	Tens	H	M	M
5	H	M	Weeks to months	Tens	M	M	M
6	M	M	Weeks to months	Ones	M	M	L
7	M	M	Months to years	Tens	L	L	L
8	L	L	Days to weeks	Ones	L	L	L