2017

Preliminary Analysis of Cyberterrorism Threats to Internet of Things (IoT) Applications

Bilge Karabacak
Franklin University, bilge.karabacak@franklin.edu

Mobolarinwa Balogun
Tallinn University of Technology

Hayretdin Bahsi
Tallinn University of Technology

Preliminary Analysis of Cyberterrorism Threats to Internet of Things (IoT) Applications

Mobolarinwa Balogun [a], Hayretdin Bahşi [a] and Bilge Karabacak [b]

[a] *Centre for Digital Forensics and Cyber Security, Tallinn University of Technology, Estonia*
[b] *Cyber Security Association, Turkey*

Abstract. The era of Internet of Things (IoT) being a combination of various networking and computing technologies already in a state of growth that introduces a new age of data aggregation mechanism and ubiquitous connectivity among physical objects. However, the most of the cyber threats still remain unsolved and may create huge impact on our lives. One of the possible major changes in impact landscape is the imminent physical results of cyber threats as IoT technologies enable closer interactions between humans and information systems. Although the cyber threats to critical infrastructures have been highly considered by the cyber security community, the cases with catastrophic physical impacts are rare which means the impact posture has not exactly shifted from information centric impacts to physical ones. However, widespread usage of IoT technologies have the potential to accelerate this shift which may bring the threat of cyber terrorism into the picture. This paper provides a preliminary comparison of a typical IoT application in health area with an industrial control system (ICS) in order to show that IoT applications are required to be deeply assessed as terrorists may attack them with easy-to-implement cyberattacks for the purpose of creating physical harm.

Keywords. Internet of Things, cyberterrorism, critical infrastructures

1. Introduction

Internet of things in the simplest of terms can be referred to as the connection of things or objects over the internet. It is a major concept in technological revolution that is set to leap frog the current internet infrastructure concept with a more advanced computing network where all the physical objects around us can be uniquely identifiable and ubiquitously connected to one another [1]. One of the keys to ensuring internet of things is the combination of different technologies among several billions of objects such as the internet (including wireless technologies and Bluetooth), RFID sensors, Near Field Communication and infra-red etc.

Despite the enormous advantages and perceived ease of life, there exist challenges and threats this comfort can pose. It is already identified that some challenges such as improper authentication mechanism currently present in RFID, tag cloning, wireless technologies being more vulnerable to hacks including eavesdropping and excess noise signals can cause RF Jamming [2]. Intelligent transport systems are already present in smart cities, wearable devices in hospitals, smart sensors for braking system in automobiles. Next maybe a connection between a refrigerator and a mobile device, smart environment, smart cooking utensils that will perceive and smell. Over reliance and the perceived implication of IoT in the future will mean that the current threat perception established for the existing technologies needs to be channeled towards securing the IoT technologies.

There is still no general definition for cyberterrorism, but it can be characterized as the use of cyber means to create havoc that can lead to the crippling of a nation's critical infrastructure such as power grid, air traffic control system, banking and military systems, health systems and in turn resulting to violence, fear and loss of life and property. The concept of cyberterrorism underlines the involvement of a non-state actor that is a group or an individual carrying out cyber attacks [3]. Till date an official cyberterrorism act has not been confirmed anywhere around the world [4].

From the technical point of view, major requirement of a cyberterrorism activity is creating a physical harm with cyber means. Stuxnet and Ukrainian power outage cases showed the possible destruction and disruption consequences of cyber attacks although they have not been classified as cyberterrorism acts due to the fact that threat actors behind the incidents are likely to be state-sponsored rather than non-state groups. These cases, however, showed that physical harm by cyber attack is possible and raised the question whether there exists a terrorist organization that may have willingness and capability to utilize such kind of cyber means. The most prevailing prediction is that the terrorist organizations have not sufficient technical capabilities for the realization of such sophisticated attacks and other physical attack alternatives are cost effective than cyber ones [5] [6].

Threat actors behave in a rational manner as they choose cost-effective methods requiring less amount of efforts and cheaper equipment and try to minimize the probability of being caught by law enforcement bodies or defenders. There occurs huge number of actual cybercrime or cyber espionage incidents as criminals have identified very easy ways for having economic gains and cyber espionage provides a safer method for criminals or nation-sponsored groups. The common denominator of all these incidents is that threat actors intend to create information-based damages on the target information systems. On the other side, very limited cyber incidents with major physical damage have happened although there exists widespread fears about the security of critical infrastructures. Based on these facts, it can be derived that current cyber security posture is mostly composed of threats having information-based rather than physical-based impacts. Cyberterrorism threats may extend the threat landscape with the latter category in case of any possible alterations in the cost-effective equilibrium. As IoT applications increase the interaction between humans and information systems, their security vulnerabilities may enable terrorist organizations to conduct easier attacks with physical impacts. The studies in the literature analyze the likelihood of cyberterrorism

threats according to the context of critical infrastructures and come up with the conclusion that cyber mean is not a cost-effective attack method [4, 5, 6]. IoT applications, however, have not been analyzed in their specific application context from the cyberterrorism point of view.

This study provides a preliminary comparison between a sample IoT application and a industrial control system (ICS), a typical information system in critical infrastructures, in order to show that IoT applications may change the cost-effective equilibrium for cyberterrorism threats. A smart healthcare system is chosen as an IoT application in the study.

The rest of the paper is organized as follows: Section 2 gives an overview of cyber incidents that have occurred or may likely occur in in health sector particularly in a smart healthcare systems. Section 3 gives information about the major incidents with significant physical results in various critical infrastructures. The comparison of both systems is given in section 4.. Section 5 evaluates the comparison from the cyberterrorism perspective. The conclusion is presented in section 6.

2. Cyber Threats to Smart Healthcare Systems

According to the 2016 internet security threat report by Symantec [7], the health services sector remains the most breached industry sub sector in terms of the number of incidents occurred. Just recently in 2015, over 80 million patient records were stolen by a hacktivist group from a leading health care facility in the United States [8]. Health data is considered as more valuable than credit card numbers in black market and the resiliency level of relevant systems is lower than the systems in similar sectors such as financial and retail which means health sector is one of the important targets of cyber criminals who are seeking economic gains [9]. There has happened many ransomware incidents in hospitals such as Hollywood Presbyterian Hospital Medical Center paid 40 Bitcoins ($17,000), and Horry County school district in South Carolina paid $8500 to decrypt a crypto ransomware [10]. Although these attacks were not targeted towards individual patients, paying the ransom meant they were significant situations for hospitals as they rely on up-to-date information from patient records. Without quick access to drug histories, surgery directives and other information, patient care can get delayed or halted, which makes hospitals more likely to pay a ransom rather than risk delays that could result in death and lawsuits.

While information-based damages of cyber threats is the current significant concern, IoT applications in this field may cause physical-based consequences as they directly interact with physical phenomenon related with humans. According to [11], of the 15 billion devices found within the IoT in 2015, 30.3% belong to healthcare which includes electronic recordkeeping, portable health monitoring, pharmaceutical safeguards and the remaining 69.7% were found elsewhere. This shows that millions of people are relying on smart devices to keep up with their health status which means these devices can be an important target for the cyber threat actors seeking ways to physically harm humans.

In 2007, a supposed attack on the United States vice president, Dick Cheney was assumed to be prevented by disabling the wireless function of the implantable Cardioverter Defibrillators (ICDs). The possibility of exploiting the device was further confirmed by researchers at the University of Massachusetts, Harvard Medical School and University of Washington who suggested a software radio-based attack was possible [12]. Medical devices such as pacemakers, insulin pump, neuro-stimulators, and drug delivery pumps are increasingly in demand to manage medical conditions. These devices are mostly communicating via wireless technology and so are exposed to cyber threats. In 2014, the United States Homeland Security pointed out two threat scenarios. One was instructing insulin pumps to overdose a patient with drugs and the other was to control pacemakers to perform battery draining operations that would result to loss of pacing output without warning [13]. An attack also demonstrated in [14] also showed how insulin pumps could be remotely turned off and also changing the device configurations without the patients' knowledge.

Doctors are being trusted by their patients when they administer drugs. This same trust is established when a smart health system administers drug to a remote patient. Suppose a smart health system that returns drug prescription to a patient were to be threatened by a man in the middle attack. A remote attacker could intercept data and return a health threatening prescription and thousands of patients' lives could be endangered due to intentional medication errors. The use of computerized drug dispensaries can cause havoc and possible death of patients [15].

Although, recent cyber-attacks on health systems has been for the purpose of copying patients health records for monetary gain, there is a possibility to further extend the attack by terrorists to jeopardize the patients safety. Copying patients' records from a directory gives the terrorist an idea of what to modify in the system that may take the doctor a long time to detect. Doctors rely on records in treating patients and so a modified record used to treat patients could have a long standing effect of the patients' health. Lives could be lost in the process. It is also possible for a terrorist to manipulate the functions of a sensor by an easy attack that deceives the user into thinking the sensor is functioning effectively and then passes malicious data [16]. Another danger in use of IoT in healthcare system is in the use of the automated medical devices itself in performing daily medical operations. Most of these devices are known to have loopholes that provides the opportunity to be controlled from remote locations by attackers. As reported in [17], zeus and citadel malwares were discovered in an x-ray system, a blood gas analyzer and a PACS (Picture Archive and Communications System) which left backdoors that basically provided remote access and control. This is extremely detrimental to the safety and well-being of patients and in a situation where the primary goal of the cyber terrorist is to cause harm to human lives, a resulting death is possible.

3. Cyber Threats to ICSs

Industries before the evolution of automated control systems have relied heavily on manual labor in carrying out daily industrial activities and controls. To make it easier, ICSs provided the possibility to interact with physical processes by providing an

automated control from a remote location with the use of SCADA, distributed control systems and programmable logic controllers [18]. This systems are present in well-known critical infrastructures such as the electric power grids, oil and gas infrastructures, industrial chemical and production plants, pipeline infrastructures [19] as well as in discrete manufacturing which includes aerospace and automotive sectors [18].

Stuxnet can be considered as the most significant case that shows how a cyber threat can harm a very strategic critical infrastructure, Iranian uranium enrichment plant in Natanz, with a physical destruction. It is a very sophisticated malware that targets industrial control system by modifying the codes of programming logic controllers with the aim of causing fast-spinning in nuclear centrifuges and hiding these effects from operators [20]. The complex attack vector includes windows and PLC rootkits, zero-day vulnerabilities, compromised digital certificates, command control infrastructure and antivirus evasion techniques [21]. Besides these advanced technical methods, collection of detailed intelligence about the industrial control systems and a testing environment having similar hardware, software and industrial equipment are highly required to conduct such a highly complicated cyber attack. Only the state-based actors which have advanced technical and intelligence capabilities can be the origins of these threats.

Critical infrastructures and sectors are dependent on the power grid for proper functioning which means they can be primary targets as in the Ukrainian power grid cyber-attack. On December 23rd 2015, the Ukrainian power grid was attacked from a remote network point that resulted in disconnecting about 230,000 people from the power source after an infiltration into the SCADA system [22]. One part of the attack steps was to disable the backup power source which was the Uninterruptible Power Supply [23].

Oil and gas pipeline systems under the control of an ICS could be physically damaged by a cyber attack. A report in [24] stated an attack as far back as 1982 where SCADA systems were used to increase the pressure of a liquid flow thereby causing a burst that damaged the pipeline infrastructure. In the description of the attack, a Trojan horse was used to initiate a major explosion of the trans-Siberian gas pipeline. The Trojan horse was installed after the pipeline control system was hijacked and was used to increase the usual pressure leading to an explosion. It is argued that the attack was known as the first cyber-attack causing external physical effect on an oil and gas operation [24]. However, it is not clear whether such incident happened as there is no any media report from 1982 and former officials of Soviet Union denies the incident [25].

4. Comparison of Smart Healthcare and ICS

In this section, smart healthcare and ICSs are compared with each other from the perspective of ongoing organizational practices in the relevant business sectors and actual technical characteristics of both systems as cyber security is a matter of organizational and technical aspects. The main aim is to evaluate the factors that may influence the required sophistication level of threat actors and the amount of resources for conducting the cyber attacks with major physical impacts.

The security and safety approaches of business sectors have different variations. The sectors of many critical infrastructures such as energy and transportation share a

profound safety culture. Although ICSs have not been designed and developed with resiliency against cyber threats, safety standards and practices have addressed many human errors, system failures and environmental threats in the related sectors. This common safety culture is supported by effective organizational measures like detailed contingency plans, operative maintenance procedures and effective auditing activities. Health sector is lack of similar standards and organizational practices. Privacy culture in this sector can be considered as an advantage when compared to critical sectors but privacy practices mostly deal with the regulation and management of intentional information sharing activities between relevant parties which causes a loss of focus on fighting with cyber threats. From technical point of view, in critical sectors, safety standards may assist to eliminate some system failures and human errors which may otherwise make the attacks easier. Increased organizational capabilities may at least enable them to effectively deal with incidents after they happen.

A typical network topology of a critical infrastructure is composed of mainly two major networks, enterprise network and industrial control network. Enterprise network is the one that highly interacts with Internet as it includes the common network services such as e-mail and web servers, other main assets like database servers and user computers.

Industrial control network consists of master terminal unit (MTU) that runs a SCADA system and carries out the central control function for entire industrial processes. Programmable logic controllers (PLC) and remote terminal units (RTU) distributed to the different parts of a critical infrastructure collects data from sensors and field devices, convey it to MTU and relays the control commands of MTU to those devices. Enterprise network is separated from Internet and industrial control network with firewalls. MTU and PLCs/RTUs are located in a wide area networks which use dedicated lines rather than Internet. On the other side, in a smart healthcare system, sensors deployed in different formats such as wearable device or a component of mobile phone obtain data from individuals and send it to a central database of a hospital.

Although similar type of data exchange between sensors and command control units take place in both industrial control and healthcare systems, the interfaces of healthcare systems are more exposed to attacks coming from Internet. Data between industrial field devices and the SCADA system is sent over a dedicated network rather than a public network such as the internet as shown in Figure 1. This is in contrast with communication in the smart healthcare systems where data is forwarded over Internet via wireless or cellular networks. In order to compromise the industrial control network, an attacker is required to have foothold in the enterprise network and then attack to endpoints, MTU and RTUs/PLCs, or manipulate the data communication between these parties. In a healthcare system, however, communication parties and the data traffic are directly exposed to Internet based threats. The data collection part is integrated to insecure home networks where attackers can take advantage of many easily exploitable vulnerabilities in those networks. The command control and data storage functions are performed by the systems in health organizations of a sector having many security breaches [7]. As the data flow occurs over Internet, this system is more vulnerable to the man-in-the-middle attacks. Abovementioned architecture difference shows that healthcare systems can be compromised by the attackers with lower sophistication levels.

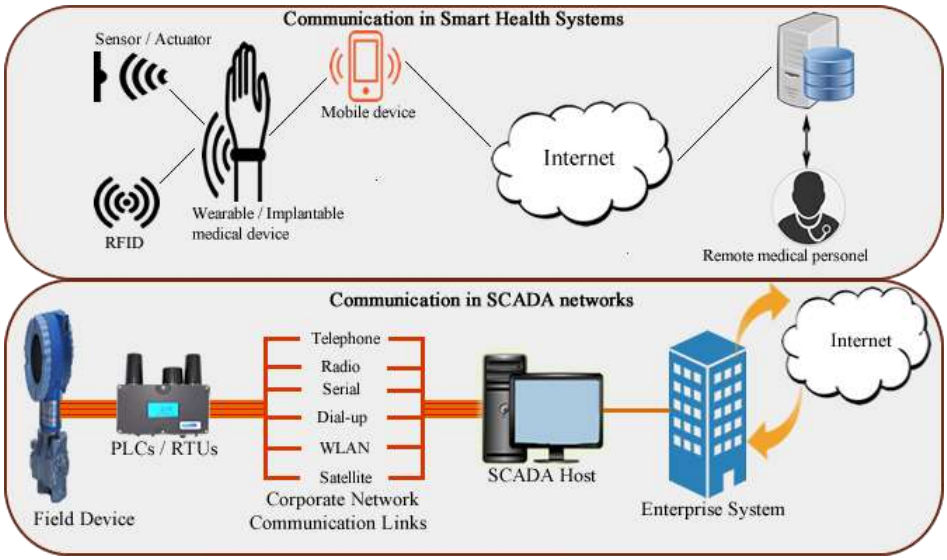

Figure 1. Comparison of communication in smart health systems and SCADA network

Smart healthcare systems uses various devices that utilize a combination of several technologies such as sensors, actuators, RFID, bluetooth, Wi-Fi, NFC, ethernet, GSM/UMTS, mobile aggregators (PDAs, mobile phones), databases and cloud servers [26] with each having existing security issues. This susceptibility makes it easier to initiate an attack since several technologies can lead to many vulnerabilities. Health devices do not require a lot of sophistication to be attacked [27]. It was seen how patients who thought their insulin pumps weren't functioning as they wanted, went online to search for the hard coded authorization credentials, logged in to the devices and then increased the dosage. They later had issues with their respiratory system [27].

Integration of different technologies requires evaluation of the whole system from an interoperability point of view. Apart from the existence of individual vulnerabilities in each system component, lack of interoperability may create additional security burden especially on the data collection part of a smart healthcare system. IoT applications in healthcare suffers from many interoperability problems [28]. On the other side, in spite of existing problems in industrial control networks, interoperability has been addressed by the safety community for a longer time than the recently developed IoT community. If the existing vulnerabilities in IoT devices are considered together with the increased susceptibility of healthcare systems to internet-based attacks, interoperability problem may act as a multiplier effect on the system weaknesses.

Malicious actors utilize social engineering techniques as an initial penetration vector in their attacks such as in their spear phishing campaigns. The improvement of user awareness is the main countermeasure against these type of attack methods. Customers are not directly interact with ICSs, only a particular set of staff deals with them whereas in smart healthcare systems, customers have main roles in the system. In a critical infrastructure, an attacker can get a foothold in the enterprise network with a spear

phishing attempt but he is also required to penetrate into industrial control network. An attacker can reach to the same goal with an easier method in a healthcare system. Although lower user awareness level is still an important problem in critical infrastructure companies, it is more problematic in healthcare systems as the customers are at the core of applications. Critical infrastructure companies can apply strict internal security practices, procedures and technological solutions to tighten the security within their premises and conduct user awareness campaign for their staff but it is more difficult to take the same actions against customers of a smart healthcare system.

Critical infrastructures have different systems that monitor the ongoing industrial processes and environmental factors. In cases of process anomalies, this advanced monitoring capability, which is mostly complemented by well-developed maintenance procedures, enables maintenance and other technical staff to intervene into the problem in their earlier stages after physical consequences start to be appear. Unless monitoring capability is compromised, a cyber threat with physical damage can be detected and a maintenance or recovery procedure can reduce the consequences. In a smart healthcare system, additional monitoring capabilities do not generally exist due the system simplicity or if they exist, they can be easily compromised by attackers. The consequences of attacks can be imminent so that a possible physical effect of a cyberattack cannot be easily recovered. In critical infrastructures, recovery methods based on manual controls may be alternative options for limiting the damage as it happened in mass power outage case in Ukraine.

5. Evaluation of Comparison Results

The above preliminary comparison between smart healthcare and ICSs shows that such an IoT implementation can be compromised by cyber attacks requiring less sophistication and resources. Although ICSs also benefit from IoT technologies for the improvement of their functionalities, the main perspective in the comparison is that many IoT applications such as smart healthcare application enable humans to directly interact with information systems in more uncontrolled environments which may lead to extend current cyber threat posture with threats creating physical-based impacts.

State-sponsored groups can be interested in conducting cyber attacks with physical-based impacts for sabotage purposes as Stuxnet and Ukrainian mass power outage cases clearly demonstrated. These groups may acquire required sophistication level and find relevant resources. As the anonymity of an espionage activity and safety of spies are significant concerns for states, cyber means can be an effective method when compared to other methods.

Cyberterrorism threat, however, is highly contested issue. It is argued that terrorists prefer physical attacks as they require lower sophistication levels and less resources. The other main argument is that cyber attacks are not suitable for creation of a widespread fear due to their limited media impact [5]. Terrorist organizations, however, may try to give a message to people that they are not even safe while sitting at their homes by attacking to IoT applications such as smart healthcare system. They can plan to conduct cyber attacks to different targets in addition to separate physical attacks within the same time-frame in order to rise the level of fear. They may even want to strengthen the belief of their members to the organization by demonstrating that they have also advanced

cyber capabilities which means internal politics of organization may be a primary reason in some cases. It is probable that terrorist organizations may identify how to benefit from the cyber capability once they acquire it.

Cost-benefit analysis of cyberterrorism activities have been done with the consideration of critical infrastructures [4, 5, 6] . Although problems in critical infrastructures may threaten the whole city, region or even state, the possibility of cyber threat is very low due to the high sophistication need and ineffectiveness of attacks from cost-benefit perspective. It means there exists a risk with enormous impact but very small possibility. With the advent of IoT technologies, a new spectrum of systems have been emerged that have different characteristics than the usual critical infrastructures. The overall impact of a cyberterrorist activity on these systems may not be as high as the impact on critical infrastructures, however they may be still reasonable target for terrorists due to possible physical results. Abovementioned preliminary comparison argues that IoT applications such as smart healthcare systems can be targeted by attackers with less capability and resources. It is important to deeply analyze the situation and be ready for the possible cyberterrorism threats.

6. Conclusion and Future Work

In many studies, it is argued that cyber-attacks are not preferable tools for terrorists to reach their main objectives of physical damage. Not having any reported cyber terrorism incident supports this argument. However, the viability assessments of cyber threats have been done according to the considerations of critical infrastructure environments. On the other side, IoT technology which establishes high interactions between humans and information systems has been adapted to provide many applications in various areas of human lives. Cyber threats addressing these applications may cause physical destruction. This paper presents a preliminary comparison of a sample IoT application with a industrial control system to show that IoT applications can be an important target for the cyber attacks of terrorists as they may require less sophistication and resources

As a future work, cyber attacks to different IoT applications will be analyzed in detail with attack tree method which can provide a coherent way for the analysis of adversarial factors such as capability and resource requirements.

References

[1] D. Singh, G. Tripathi and A. J. Jara, "A survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services," *IEEE World Forum on Internet of Things (WF-IoT)*, 2014.

[2] M. U. Farooq, M. Waseeem, A. Khairi and S. Mazhar., "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," *International Journal of Computer Applications*, vol. III, no. 7, 2015.

[3] D. E. Denning, "A View of Cyberterrorism 5 Years Later," *Internet Security: Hacking, Counterhacking and Society*, pp. 123-139, 2007.

[4] T. M. Chen, "Cyberterrorism After Stuxnet," Strategic Studies Institute and U.S. Army War College Press, 2014.

[5] M. Conway, "Reality Check: Assessing the (Un) likelihood of Cyberterrorism," in *Cyberterrorism*, New York, Springer, 2014, pp. 103-121.

[6] G. Giacomello, "Bangs for the Buck: A Cost Benefit Analysis of Cyberterrorism," *Studies in Conflict and Terrorism*, vol. Vol. 27, pp. 387-408, 2004.

[7] Symantec, "Internet Security Threat Report, Volume 21," 2016.

[8] J. D. Maggio, "The Black Vine Cyberespionage Group, Version 1.11," Symantec, 2015.

[9] J. Finkle, "FBI warns healthcare sector vulnerable to cyber attacks," Reuters, 23 April 2014. [Online]. Available: http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-exclusiv-idUKBREA3M1Q920140423. [Accessed 16 June 2016].

[10] J. Scott and D. Spaniel, "The ICIT Ransomware Report," Institute For Infrastructural Technology, 2016.

[11] Intel Corporation, "A Guide to The Internet of Things Infographic," Santa Clara, 2016.

[12] BBC News, "Dick Cheney: Heart Implant attack was credible," 21 October 2013. [Online]. Available: www.bbc.com/news/technology-24608435. [Accessed 21 May 2016].

[13] Kennedy Law, "Cyber attacks on smart devices: get smart," 2 March 2016. [Online]. Available: http://www.kennedyslaw.com/article/cyber-attack-smart-devices/. [Accessed 18 June 2016].

[14] DarkReading, "Veterans Administration Adoptrs UL security Certification Program For Medical Devices," 20 June 2016. [Online]. Available: www.darkreading.com/vulnerabilities---threats/veterans-administration-adopts-ul-security-certification-program-for-medical-devices-/d/d-id/1325968?. [Accessed 3 July 2016].

[15] W. Jones, " FDA Urges Tighter Cybersecurity for Medical Devices," IEEE Spectrum, 16 June 2013. [Online]. Available: http://spectrum.ieee.org/riskfactor/telecom/security/this-week-in-cybercrime-fda-urges-tighter-cybersecurity-for-medical-devices. [Accessed 16 June 2016].

[16] Z. Benenson, P. M. Cholewinski and F. C. Freiling, "Vulnerabilities and Attacks in Wireless Sensor Networks," *Wireless Sensors Networks Security*, pp. 22-43, 2008.

[17] K. J. Higgins, "Hospital Medical Devices Used As Weapons In Cyberattacks," 6 August 2015. [Online]. Available: http://www.darkreading.com/vulnerabilities---threats/hospital-medical-devices-used-as-weapons-in-cyberattacks/d/d-id/1320751. [Accessed 23 May 2016].

[18] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," *NIST Special Publication*, 2015.

[19] D. Whitelegg, "Combating IoT Threats - Top Security Best Practices," 30 September 2015. [Online]. Available: https://www.ibm.com/developerworks/library/iot-security-best-practices-iot-apps/. [Accessed 23 May 2016].

[20] D. Kushner, "The Real Story of Stuxnet," IEEE Spectrum, 26 February 2013. [Online]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/. [Accessed 18 July 2016].

[21] N. Falliere, L. O. Murchu and E. Chien, "W32. Stuxnet Dossier (version 1.4)," Symantec Corp., 2011.

[22] Electricity Information and Sharing Center, "Analysis of the Cyber Attack on the Ukraininan Power Grid," SANS, Washington D.C, 2016.

[23] Availabilty digest, "How the Ukraine Power Grid Was Hacked," March 2016. [Online]. Available: http://www.availabilitydigest.com/public_articles/1103/ukraine_outage.pdf. [Accessed 1 June 2016].

[24] E. J. Byres, "Cyber Security And The Pipeline Control System," *Pipeline & Gas Journal*, vol. 236, no. 2, pp. 58-59, 2009.

[25] T. Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, vol. 35, no. 1, pp. 5-32, 2012.

[26] Y. Gelogo, H. j. Hwang and H. K. kim, "Internet of Things (IoT) Framework for u-healthcare System," *International Journal of Smart Home*, vol. 9, no. 11, 2015.

[27] K. West, "Healthcare IoT security issues: Risks and what to do about them," *The Risk of IoT in Healthcare* , 2016.

[28] L. M. R. Tarouco, L. M. Betholdo, L. Z. Granville and J. Santanna, "Internet of Things in healthcare: Interoperability and security issues," in *IEEE International Conference on Communications (ICC)*, 2012.

[29] R. Shrestha, "A guide to healthcare IoT possibilities and obstacles," *Barriers to conquer before IoT in healthcare helps Mrs. Smith* , Jan 2015.