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

ITC70LT

Sho Yano 144714IVCM

SECURITY ANALYSIS ON HEALTHCARE IOT PROJECT

Master thesis

Olaf Manuel Maennel
Ph.D
Professor at Tallinn University of Technology

Tallinn 2016

Declaration

I hereby declare that I am the sole author of this thesis. The work is original and has not been submitted for any degree or diploma at any other University. I further declare that the material obtained from other sources has been duly acknowledged in the thesis.

Author : Sho Yano [May 25, 2016]

Annotatsioon

Lõputöö on kirjutatud Inglise keeles ning sisaldab teksti 59 leheküljel, 8 peatükki, 9 joonist, 1 tabelit.

Abstract

In this study we are finding undiscovered threats in IoT systems. Since IoT devices have direct connectivity to Internet, threats for IoT affect Cybersecurity directly. From various application fields of IoT, healthcare system is selected for an analysis. Development of IoT healthcare is based on strong demands for innovation however the idea has potential threats to life of people. For example remote attack to healthcare devices may cause crisis of life. Regarding the backgrounds of IoT healthcare, security is an important field to study however there are not enough research activities. Therefore this study is motivated to contribute to secure IoT healthcare.

An academic healthcare IoT project was picked up as an example target to attack. Following to standard penetration testing steps, security analysis for the system was performed. As a result, spear fishing, which is trying to steal personal data, is a potential case but it has not been reported now. Besides the result, from related works, ransom ware for healthcare and abuse network function for botnet are revealed as typical security incidents for IoT systems. In addition, based on the spear fishing scenario, an exploitation test in a network simulation was performed. Though the tests, preliminary concept was proofed. More precise, the story is an attacker puts a malicious IoT node on the side of smart house to intercept wireless communication.

For technical background readers, through this study it is confirmed that there are wide free space to study security about IoT. For decision makers such as IT managers or politicians, this study provides an example to think about how to secure IoT system with potential threats.

The thesis is in English and contains 59 pages of text, 8 chapters, 9 figures, 1 table.

Acknowledgement

I would like to express my gratitude to my supervisor, professor Olaf Manuel Maennel for the useful comments, remarks and engagement through the learning process of this master thesis. Furthermore I would like to thank Dr. George Oikonomou for introducing me to the IoT OS (Contiki) and the IoT projects organised by University of Bristol. For reviewing my thesis, I would like to thank Dr. Andro Kull for valuable advices. Finally, I thank my family for supporting me throughout all my studies at University.

List of Acronyms and Abbreviations

ISP	Internet Service Provider
DDoS	Distributed Denial of Service
PLC	Programmable Logic Controller
APT	Advanced Persistent Threat
NSA	National Security Agency
CIA	Central Intelligence Agency
DTSL	Datagram Transport Layer Security
CoAP	Constrained Application Protocol
RTSP	Real Time Streaming Protocol
SCADA	Supervisory Control And Data Acquisition
DVR	Digital Video Recorder
ECU	Electrical Control Units
RTOS	Real Time Operation System
MITM	Man In The Middle
RF	Radio Frequency

Contents

List of Figures

List of Tables

1. Introduction

This study is trying to reveal security threats for IoT especially on healthcare applications. From beginning of this year (2016) some ransom ware targeting hospitals were reported thus people are starting aware that some vulnerabilities exist in medical systems or devices. Besides IoT is emerging technology for innovative solutions and healthcare is a key application for example wearable monitoring devices. Regarding those two modern phenomenon, cyber threats in healthcare and rapidly developing IoT technologies, it is worth to studying IoT security for healthcare now.

Main problem of secure IoT for healthcare is that there are not enough studies about the field. One of the reasons is the technologies are under developing now. Regarding to demands for innovative solutions by business sectors the IoT field is the hottest field to technical development. However, as always, it is hard to say that there is enough effort for security features. Since direct connectivity to Internet is a key feature of IoT thus IoT development means new type of devices will communicate to Internet. Therefore partially developed unsecured devices may bring negative impact to Internet.

Healthcare application is also an issue because it is strongly connected to life of people. Recently some ransom incidents are reported from hospitals. From now, it is easy to say it was predictable because there were some warnings about network medical devices at hackers' conference. However incidents were happen in practice. IoT for healthcare is a future concept but regarding to the facts studying about future threats has some meaning.

It is hard to study upcoming technologies because initially those stories are recognised as science fictions. In other words social recognition is quite low until some huge impact case is reported. In order to tackle the situation, a technical study has a chance to contribute for more secure healthcare IoT instead of shallow buzzing articles.

Regarding those backgrounds, there is a possibility of undiscovered threats in IoT for healthcare. One of the approaches is application centric analysis. Secure IoT is a hot topic for academic society and also for hackers' conference however there are not many analyses by holistic approach. There are some reports about IoT specialised malwares but those activities are just targeting end devices. Hacking IoT devices also popular hobby for hackers but this is also a narrow field of view. Based on the situation this study is based

on application point of view. Holistic is a key term for security analysis in order to handle huge IT systems. In addition from IT system developing field, people understand profit come from whole system not from each device itself.

Another point of view is focusing IoT features, which is resource, constrain. Embedded platforms are resource constrained for example low computational power comes from battery powered electric board. Financial cost or physical special issue on a board are also restriction for security features. Compared to conventional network devices such like personal computers or network routers, those IoT restrictions affects security not only to IoT but also Internet. Regarding those features, this study is trying to reveal new security threats in IoT technologies.

In order to show potential threats for healthcare IoT, an academic project is analysed as an example target. SPHERE is a project to research targeting better-designed healthcare in United Kingdom[5]. Around 100 smart houses, which have smart sensors, are participated in the project in Bristol area. Basic concept of the research is continuous monitoring in living environment (smart house) to improve level of health. Contiki, open source IoT OS, is introduced as a platform of those smart sensors.

For starting point of the security analysis, as the first step of penetration test, C-I-A threat analysis method was introduced. The analysis is resource-based technique to illustrate threats in a system. Output of the analysis was summarised threats scenarios to explain as realistic stories. After the initial analysis technical tests were also performed. A spear fishing scenario, which is targeting personal data in the smart home, was introduced as a basis of the technical test. Network simulator provided by the developer group of IoT OS was selected to test.

Contribution of this study is to build up a summary of potential threats for healthcare IoT. The threats are introducing reported cases until now and also findings from this study. Especially spear fishing, which is targeting personal healthcare data has not been reported thus it is a key finding.

In addition it is a step for creating a material for future penetration testings to IoT systems. Though the technical test, cheap attacking method was showed possibility of IoT based attack for spear fishing. More precisely it shows if attacker can approach physically to IoT wireless network, it just need put IoT device near the wireless area because

the attacking method utilise proper transmission path to send out intercepted user data. To avoid undesired data leakage with this method, packer filtering to out going direction is a basic solution.

2. Hypothesis

This study challenge to discover threats which have not reported for IoT healthcare until now. Until now various incident reports were published related IoT systems however IoT technologies are under developing now. Therefore continuous security study for developing IoT have chance to find future vulnerabilities. More precisely this study is focusing healthcare application thus the method have potential to find healthcare specialised threats.

Another key point is technical simulation based method have chance to show proof of concept. Ordinary penetration test are conducted to target system directory. On the other hand this study introduce network simulator as preliminary test target. This idea comes from Cybersecurity exercise environment organised in some test environments. One of a merit of the way is that it does not cost compared to physical actual environment. In order to achieve applicable results, the test environment should be as practical as possible.

Core motivation of this study is to realise secure IoT systems and also secure Internet. Key feature of IoT is direct communication to Internet thus securing IoT is directory connected Internet security. More precisely findings from this study may contribute more secure IoT system development. This is not only contribution from technical aspect but also from business aspect. Business demands are one of core driving force of technical development but on the other hand security is breaking the speed of emerging technology. Thus enabling secure IoT system support those high-speed business developing for example venture businesses.

3. Background

In this section, related backgrounds are widely reviewed. Since IoT is an innovative concept but it is not unclear about potential impact to cybersecurity. Though the review, it is possible to say introduction of IoT to Internet may have more negative impact than mobile phones with IP but not exceed invention of router or computer virus. Compared to mobile phone technologies, which is almost under control, by big IT companies (Apple, Google, Microsoft), development of IoT is not regulate enough. Therefore IoT have more space for unpredictable use cases by malicious factions.

In order to illustrate the meaning of IoT technologies in Cybersecurity context, short history of Cybersecurity is introduced first. In this review, Cybersecurity matters are listed from initial stage of Internet to current status. Next subsection introduces general information about IoT then tried to define IoT. It is difficult to define the things under emerging however it is important to define the things before studying it. Regarding those backgrounds or not, there are many articles about IoT security. Therefore some of those articles introduce but most of them are mentioning surface of the issue. Finally an academic IoT project is explained. The project is analysed in this study to understand threats for IoT technologies as an example. In addition the project have a feature, which is challenging ubiquitous healthcare (telemedicine). This is not a simply challenging research project toward future healthcare but also provide clues for secure IoT.

3.1. Short History of Cybersecurity

Invention of Internet is key milestone for cyber securities since originally Internet provide worldwide communication for polite manners. However if some group of users have malicious intention and utilise Internet to accomplish their mission, the platform of international communication turn to very useful tool or target for remote attacks.

Before Internet era, computers or local networks are isolated like islands in the ocean. When they needed communication between the islands, hands should transfer some physical medias. Punched cards, open reels, cassette tapes or floppy disks were typical media for them. Harmful things for computers were some bugs from a moss stacked in mechan-

ical switch to coding errors in software [9]. Computer virus is another harmful part of computer society. There are also some historical stories about virus. First computer virus for research purpose is reported in 1981 [10][11]. It was targeting Apple II and named Elk Cloner. Another historical case of computer virus was BRAIN [12]. It was discovered in 1986 and author was in Pakistan. Amazingly the author is still working at the same address, which was written in the code of virus and Mikko Hyponen, CTO of F-Secure visited him in 2011.

Original of Internet can go back to ARPANET established in 1969 [13]. Key features of the innovative network are packet switching and TCP/IP protocols since both are critical technology for today's Internet. Next milestone of Internet was CSNET [14] [15]. From 1984, the network started communication to Israel, Korea Australia, Canada, France, Germany and Japan. After commercialisation of Internet some ISP were established at 1995, various services have been launched together with gaining more users all over the world. Internet provide international country communication more easily with affordable prices for any users therefore so many social changes are happened. Originally Amazon started book retailing from 1994. There are some conflicts especially with local small retail stores until now. File shearing is strongly based on advantage of digital medias. Cost of copying and transferring via network is lower than physical exchange methods. Napster was a popular P2P file sharing services from 1999. SNS for example Facebook or Twitter provide huge social impacts. Advanced mobile technologies for smart phones accelerated impact of them. Some social revolutions in early 2010s are based on those innovative services [16] [17]. Wikileaks with anonymity networks made some disclosures and it affected greatly. Crypt currency is also playing interesting role on Internet. Key impact of the idea is it transfers value via Internet with lower cost compared to conventional financial methods.

When Internet became an universal space for everyone in the world, which is idealistic situation from computer culture, some of unexpected cases happened. Nowadays cyberspace became a battlefield ranging from obviously state owned units to some suspicious group or voluntary members. Cyber attack to Estonia on 2007 was a key event to an IT oriented country to understand Cybersecurity as an important issue. After relocation of the Bronze Soldier, some websites including parliament, bank, ministries and media were beaten by DDoS attack. At the moment Tallinn, capital of Estonia, also under attacks physically by riots then it was a case of hybrid incident [18]. Similar case was happened the next year 2008 at Georgia. It was happened with Russian invasion to South Ossetia. At the

moment, there was not only DDoS attack but also cross-site scripting and SQL injections [19].

More sophisticated attacks are introduced by malwares. Most famous case is Stuxnet, which was targeting nuclear project in Iran [20]. According to an analysis report of the malware, various types of technologies were combined to accomplish their objectives. Critical part was PLC software which control centrifuges then malicious control signal break the centrifuges. More important fact was the malware were well designed and it indicates the attacker group has sophisticated developing capability. For example, multiple security holes in Windows are abused together with information of targeting PLC units with model numbers. Therefore some level of cooperation between a developing team and an information-gathering group can easily assumed.

Another type of group is APT, which is utilising hacking ability to collect intelligence. Security firm Mandiant by a report "APT1" pointed out PLA Unit 61398 on 2013. In this report, the group explained, " APT1 is likely government-sponsored and one of the most persistent of China's cyber threat actors." [21] The group conducted cyber espionage then stole confidential information from numerous firms in some countries. Dukes are another cyber espionage case reported by F-Secure [22]. The group has been worked as an espionage unit for Russian foreign decision making since 2008.

There have been also defensive activities in order to respond to attackers. Antivirus software was a main actor in early stage. 1980 to middle of 1990s was early stage for antivirus. For instance John McAfee founded the McAfee Company in 1987 and Norton Anti-Virus released in 1991. From 2000, more useful tools were developed. AV-Test Gmbh started for antivirus software comparison in 2000 and Virus Total, which is offering one stop online, scan engine for suspicious files launched in 2004. Those virus scans are categorised as static analysis. On the contrary there are also dynamic method, which is sandbox analysis. Cuckoo is an example of automated analysis tool with dynamic framework started around 2010. For additional information, nowadays McAfee acquired Intel and Google bought Virus Total in 2012. The fact shows those studying computer virus became a valuable business.

In addition, private companies are not only actor for computer security filed. There are some communities to keep cyber space safe. IETF is volunteer based community for Internet standards from 1986. Internet Advisory Board (IAB) was an origin of IETF that

created in 1984 and it had Security task force from origin [23]. USENIX also have security related activity, which named USENIX Security Symposium now. Original of the activity is back to 1988 according to history of USENIX [24]. Top two popular hackers communities started almost same time by a person, Jeff Moss. Some more conferences focusing offensive hackers were also launched. DEF CON was from 1993 and Black Hat was from 1997. Open Web Application Security Project (OWASP) is an online community for free materials for web application security and it was founded in 2001 [25].

Still there are spaces to discuss about hybrid warfare. Cybersecurity can be a part of it therefore military point of view is one of the important aspects. For example introduction of commercial technologies like mobile phone and photo sharing by Hezbollah is a distinguished case of hybrid warfare [26]. United States Army defined Cyberspace as fifth domain along with Land, Maritime, Air, Space [27]. In the cyber domain, three independent functions such as offensive, defensive, Information Network Operations, are listed. Building structure of cyber capability is also an issue because in cyber domain not only current military capabilities but also civilian organisations are strongly related. For example in United States, NSA or CIA is famous actors in the cyber domain. Regarding some needs for unified force, US Cyber Command is in active from 2009 [28]. In this paper, author mentioned Billy Mitchell, historical Army general, who is regarded as the father of the United States Air Force as an example of emerging new military domain. Timing of forming air force is a preceded case because United States Air force formed after WWII but Royal Air Force emerged 1918. Historical study, how new domain force was established is one of an historical theme which give suggestions for future Cyber forces[29] [30].

3.2. Overview of IoT

According to a publication of the IEEE Computer Society, the phase of "Internet of Things" coined as a new idea of RFID in 1999 [31] [32]. Furthermore, Stephan Haller defined the IoT as "a world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. [33]. ITU also defined in a recommendation ITU-T Y.2960 as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and

Table 1. Applications of IoT [8]

Application	Description
Building and Home automation	Monitoring and controlling for smart homes and buildings in order to achieve security or to reduce energy consumption.
Smart cities Smart grids	Lighting, surveillance and control systems for reduce cost and energy consumption
Wearable	Smart watches or other fitness gear for healthy people
Healthcare	Drug tracking, proactive healthcare (online diagnosis)
Manufacturing	Real-time inventory, asset tracking

communication technologies." [34]. Regarding those background, fundamental concept of IoT seems that "objects which have sensing ability, network connectivity".

IoT is a latest keyword for various business fields. Texas Instruments summarised applications of IoT. Table 1 shows the examples. One of a key feature of IoT is data acquisition. Because of smaller size of electric devices and lower energy consumption technologies, IoT system acquires data with large amount of sensor nodes. Cloud computing and artificial intelligence are also related technology for IoT. Cloud computing services enable flexible storages for big data and also offering data processing services. Amazon AWS is a popular service in this field together with an IoT focused service [35]. They are offering authentication and authorisation platforms for secure connections to cloud services. Currently, data acquisition and analysis are main goals for IoT systems however feedback control is a next step for innovative IoT solutions. This means, an algorithm decide control parameters or orders regarding results of processing of huge amount of data with well trained artificial intelligence. In other words, IoT technologies will be a fundamental basis of those kind of smarter systems.

Since IoT devices are "objects" which means compared to conventional network nodes (PCs, servers, routers), naturally their resource is limited. Usually embedded platforms are introduced for IoT devices. A key feature of those devises is resource constrains. Total memory size, processing speed and battery size are fundamental resource for computations and those of them are limited compared to ordinary personal computers. However thanks to rapid growth of mobile device market, more advanced electric components are realised. Those developments support the idea that embedded devices will gain functions to communicate to the Internet directory.

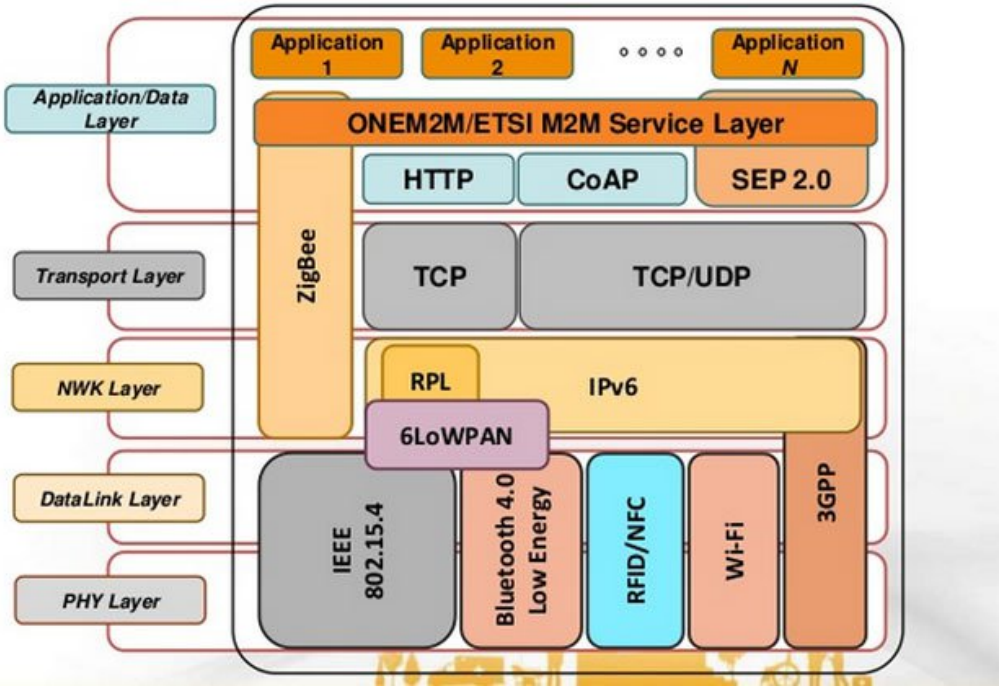

Figure 1. New protocols for IoT[1][2]

Regarding those background, new network protocols are also emerging. Figure 1 shows overview of those special protocols. CoAP is one of a protocol for IoT devices and a RFC is issued by IETF [36]. It is an UDP protocol and designed lightweight integration of HTTP. There is a paper about an implementation for IoT specialised OS and reporting about energy consumption [37]. XMPP is another standard for IoT devices. It is originally developed text exchange system for messaging on top of TCP [38]. RPL is a routing protocol and 6LoWPAN is a header compressed IPv6 for low power wireless networks. IEEE 802.15.4 is a wireless standard for physical layer and basis of ZigBee. For more details there is a survey papers around those protocols [39].

Expand IoT devices provide more amount of data but behind that there is an ultimate goal

with how to utilise it. Big data analysis or artificial intelligence is related technologies for them. Goal of the development is realisation of feedback control with smarter system. For example in medical application, online home monitoring with wearable sensors enables real-time diagnosis and proactive care for patients. Another case is smart grid. Each smart meters provide consumption data to control centre then the central control system adjust parameters for smart grind in order to optimise production and distribution of electricity.

Usually initial stage of IoT system targeting data acquisition however regarding the direction of developing IoT technology feedback signal will be more focused. For instance speed of down stream or security of those communications. Another important technology is of course artificial intelligence. Google, Microsoft and some other groups started to provide their platforms.

3.3. IoT Security

There are strong interest of IoT security however various articles on web medias are just describing surface of the issues. Ukrainian power industry is an example of the problem[40]. Some title said attacking to devices connected to network causes the black out but the fact was DDoS attack to telephone system. As a result, communication process was damaged then it took long time for recovering. Another interesting case is web accessible security cameras. A web site took attention to web cameras from worldwide and some of them are supposed not intentionally opened [41]. Insecam.com is an example of them and it is directory of online surveillance cameras in the world. Some articles, which are pointing the issues, were published from 2014 but still there are more than 10000 cameras are listed in.

Building secure IoT technologies is important goal but there is another effect to conventional system by emerging technology. CVE is a reference for publicly known security hole. US Department of Homeland Security supports the database and the CVE-ID is common identification number for security professionals to share the issue. Recently they put a message on the top page of CVE [42]. Main message is because of growing number of IoT devices, issuing CVE-ID has delayed. This phenomenon is not an issue but may imply future similar case for Internet. There are many organisations, societies or groups are working to keep Internet running thus those system need some changes for

adapt forthcoming IoT era.

3.4. The SPHERE project

Health care is a field of IoT application in order to realise continuous feedback care. Figure 2 shows fundamental concept of the idea. The idea is that wearable sensors or ambient sensors acquire living data then submit to medical institution. The data is analysed by medical staff or some algorithm to provide appropriate feedback to patients. If the concept is applied to rehabilitation, remote monitoring improves quality of care. Compared to conventional workflow, occasional diagnosis at a hospital, main difference is continuous monitoring. The approach enable online monitoring and it supports caring negligible alternation or more accurate diagnosis in normal condition, which means customers house. There is a survey report for such systems[3].

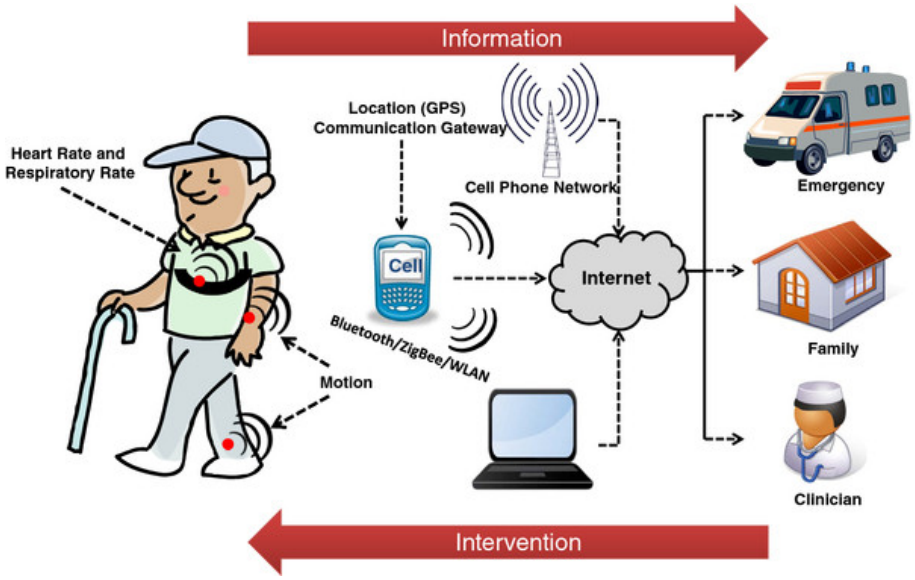

Figure 2. Remote healthcare feedback schematic [3]

SPHERE project is an academic project toward improving healthcare with IoT technologies. Key feature of the project is introducing ambient assisted living, which is providing patients data to healthcare professionals as well as standard living at home. Various sensing methods are implemented in smart homes for the sake of acquiring various information. For example, environment sensors, wearable censors and videos are working to detect falls in the house. From technical point of view networking technologies are also

studied. In a paper, wireless standards and IPv6 are mentioned as related components [5]. In this research, around 100 smart houses are established in Bristol, UK.

4. Related work

4.1. Studies about secure IoT Protocol; academic approach

From academic point of view, most of studies are conduced in order to achieve new secure IoT protocols. This is because IoT need lightweight protocols since devices are resource constrained. Therefore small memory footprint is preferable but this cause weak security. Regarding the situation, there is a critical contradiction between security assurance and lightweight protocol. J. Granjal summarised security issues for IoT protocols with a survey paper [43]. More specifically, a combination of DTSL and CoAP is also studied [44]. Another important topic is key management. One of the papers introduced overview of dynamic key management for IoT [45]. Besides those studies, IPv6 is a related topic for IoT to provide unique identification numbers to every devices [46]. IPv6 is still under deploying technology thus there will be more security related issues not only with conventional network equipments but also with IoT devices.

4.2. Proof of a security hole; hackers approach

In some hackers' communities, security of IoT is an emerging topic. IoT Village at DEF CON is a workshop for IoT security. In the workshop, Wes Wineberg reported some clear overview of IoT security. The reason is more and more new IoT devices are launching in the market, therefore efficient method for security testing is required. He categorised components of IoT system; hardware, PC apps, Mobile apps, Cloud communications. Figure 3 shows the idea. This figure shows amount of interest from attackers thus a vulnerability, which is exposing to Internet is most popular for attackers.

4.3. shodan

Shodan is a search engine for connected nodes in Internet [47]. User can search service banners from various ports and which provide information about the devices. Especially port 554 is taking attentions since it is RTSP (Real Time Streaming Protocol). SCADA

Figure 3. "physical" include data extraction from onboard memory chip or direct serial communication to the board. "local network" means intercepting wireless communications. "remote" is port scanning or more further trial from remote site [4]

systems are also took information by the crawlers. This is a serious security issue because it provides way to control infrastructures. A security researcher at DEF CON also mentioned medical devices [48]. In the presentation, author mentioned healthcare industry is 10 yeas behind from others for example most risks were found in 1 hours with known vulnerabilities by open source reconnaissance tools.

4.4. Cryptocurrency mining

It is known that huge computational power is essential to mine crypto currency. In 2014 a Linux based IoT worm, which is targeting to mine Doge coins and Mincoins was reported [49] . According to the report, their gain was around US$200 however the report mentioned they will increase capability because mining function was implemented only to x86 architecture instead of their full capability on ARM, MIPS and PowerPC. The reason of attacking to IoT devices was explained that a lot of devices left default password/username and many user do not care about that. There is another report about Bitcoin Miner malware on DVR [50]. The DVR (Hikivision) is usually used to record surveillance cameras. Exploitation was happened at telnet port with default root password "12345".

4.5. IoTPOT

IoTPOT is an excellent work about IoT malware analysis [51]. Behind the study, authors observed skyrocketing attacks to port 21 (telnet) from Internet attack detection system in 2014. From basic analysis, weak protections for authentication and global IP address as well as nonstop running were pointed out as reasons for attacks. In order to reveal

more details about offensive activities, they created the honeypot with multi architecture virtual machines. Through the research some monetise ways were revealed; abuse network function for DoS, fake search engine hosting, click fraud for advertising and stealing credentials for pay per view. What is an interesting finding in the study is attackers are interested in capability of IoT devices instead of data. Thus attackers are simply looking IoT devices as light Internet devices with weak security.

4.6. RERUM

Some of advanced projects have conducted security analysis for IoT system. RERUM is an example of IoT security research project funded from European Union's Seventh Programme for research[52]. The project started in 2013 and providing their achievements as deliverables for public. Deliverables 2.1, Use-cases definition and threat analysis, is showing results of security analysis for IoT system. They defined four use cases, which were smart transportation, environmental monitoring, home energy management and comfort quality analysis. Based on the use cases, asset based threat analysis were conducted. According to the document those IT assets were identified, Authentication Credentials, User Data, Command and Control data and Software. This categorisation provides clear distinguish for assets, which should be considered, from security point of view and it helps further security analysis. Next step was threats identification based on asset analysis. Each assets are analysed for C-I-A threat analysis way one by one. One of the example is "Loss of Confidentiality of Authentication Credentials". After all threat cases are identified, concrete scenarios with use cases were introduced so that threats are clearly explained. For example, false data injection attack was mentioned for Integrity of Smart Transportation use case. For more details about those scenarios, some references are also pointed out [53].

5. Methodology

In order to find potential vulnerability in IoT healthcare, following two steps were applied to an academic project (SPHERE). First step is a security analysis based on C-I-A aspects based on asset identifications. Result of the analysis is summarised by type of attackers as well as attacking scenarios. The reason for introduction of attacker type based scenarios is they have different goals with various rage of capabilities. Secondary step is imitate a scenario from previous analysis in a simulation environment. In this step a preliminary penetration test is tried with small number of IoT nodes. The simulation environment is provided by an open source group of IoT OS for developers.

5.1. CIA threat analysis for a project

CIA threat analysis is a resource centric methodology. In this manner, important assets, mainly information, for the project is clarify then those assets are analysed by three aspects, confidentiality, integrity, availability. User data is typical information asset for IoT projects because data acquisition is the main purpose currently. From privacy point of view, user data need careful handling.

CIA is the abbreviation of Confidentiality-Integrity-Availability. Loss of confidentiality is disclosure of information to unauthorised entities. For example, privacy information must not disclose for unapproved third parties. Loss of integrity caused by unofficial modification. If packets source IP addresses are tampered, reply packets will reach arbitrary destination by attackers. Typically loss of availability is provoked by DoS attack. Another way especially for wireless communication is radio jamming with transmitting same frequency signal.

5.2. Type of attackers

Purposes are different from type of attackers and methodologies are diverse. Therefore, security analysis based on category of attackers provides realistic scenarios. CTO of F-Secure, Mikko Hypponen hold at the IT-collage, Estonia [54], refers the categories from

a public talk. Similar categorisation for threat source to cyber security is done by United States ICS-CERT [55] [56].

5.2.1. Grey hat hackers

It is not easy to distinguish colour of hat for hackers therefore hackers are defined as grey colour in this study. This matter is related to anonymity in Internet since if a hacker plays as a white hack in public but it is still possible to conduct harmful attack with some anonymisers.

Some of them are doing computer security research for example bug hunting. They are getting social recognition or financial profit with their achievements. Blog posts or talks in hacker's conferences are typical media of them. Find vulnerability then provide article with evidences (source code or machine code) is typical procedure for them. Sometimes exploit scripts are also provided.

One of the popular case by white hacker is hacking car. Dr. Charlie Miller and Chris Valasek are very famous name for car hacking. In 2013 they published white paper granted by DARPA about hacking Toyota Prius and Ford Escape [57]. They hacked CAN bus which is automotive standard for control used by ECU. At DEF CON23 in 2015, next target was Jeep [58] [59]. In both case, they successfully hijacked car control include steering, brake or door lock. They also found remote attacking method which means attacker can steer a car via Internet. Main point of their activity is they disclose finding for manufacture first instead of opening publicity. Thus security researchers take public attention without harmful events because security holes are treated by manufacture before the information is disclosed. On the other hands malicious factions abuse those findings just for attacking as a zero day exploit. They are utilise unknown vulnerability for malicious activity. Therefore previous notification by white hat hacker is important proceeding in security researches.

Kevin Mitnick is an interesting example of tuning "black to white" case. He conducted various unauthorised hacking based on social engineering in teenage and charged multiple wire fraud [60]. After five years prison, he changed career to security consultant from 2000. This is an example case of hackers' two faces and a story of shifting side.

Ethical hacker or penetration tester is alternative expression of white hackers. They are using hacking ability to test purpose thus all activities are regal and agreed with customer who asked to hack own system. Sometimes they form groups and build certifications or standards. PTES is a standard of penetration testing provided by a group of information security practitioners. [61].

5.2.2. Hactivism; anonymous

Their activities are based on propagandas about politics or social matters. Suspended or defaced web page is typical method in order to take social attention and spread their messages. Especially deface a web page or DDoS attack is typical case. "anonymous" is the best known group of this category because they perfomed various operations. Origin of their activity came from 4chan image board in 2003 and it reflects anonymous online community culture. They use special hash tag for each their activity like #OpExample but actual members are not fixed. Therefore wide range of attacks was happened. Sometimes they target government organisation and sometimes-international companies. Regarding their flexible way to organise attack it can be said cyber demonstration by anonymous Internet users. It's not easy to predict those attacks but one of the clues of their movement is indicated by #tangodown in Twitter. It is a slogan of them thus search results of #tangodown show on going attacks.

For more facts, here is an interview-based book about activist [62]. Contents of the book are interviews for people who involved anonymous activities. The author, a Forbes magazine journalist, showed two face of anonymous activity in an interview [63]. As a answer to a question about good or bad to Anonymous, she commented that "It depends what it's for. You asked earlier has Anonymous done well for the world. In some cases, yes, I think it has in terms of some of the stuff they did in the Middle East supporting the pro-democracy demonstrators. But a lot of bad things too, unnecessarily harassing people – I would class that as a bad thing. DDoSing the CIA website, stealing customer data and posting it online just for shits and giggles is not a good thing. But it comes with the territory of having a free and open Internet that people can do whatever they want. We'll just see whether that freedom will be there 20 years from now."

5.2.3. Criminal

Main goal of them is financial profit therefore there are business model based on profit and loss balance. Hostage information or IT infrastructures by ransom ware is typical way to earn. Ransom ware abuse cryptography to seize victim's data then asks ransom. Famous case is CryptoLocker in 2013. The malware transported via email attachment and botnet to Windows machines. When a victim pays enough amount with crypto currency until deadline, decrypt key will be provided. Similar cases are happened to computer systems. There are some cases at hospitals in 2016 and a hospital in California paid $17,000 according to an article[64]. In 2015 some security firm predicted for this ransom ware to medical systems [65].

As previously mentioned, some hackers noticed medical devices have security holes and it is not hard to find those vulnerability remotely. Based on the fact targeting medical system in a hospital is considered criminal model (business model) to monetise hacker's skill. It is not hard to imagine people tend to pay money for one's life than anything else therefore medical sector is a desirable target for cyber criminals.

5.2.4. Terrorists

Their objective is to bring terror to countries or regions. Although there are no report but it is possible to spread rumour with physical attack such as bombing. Denial service attack to public infrastructures is also possible scenario. There are two way to introduce cases by terrorists. One of the way to think about terrorists in Internet is pickup famous name for physical terrorist activities. ISIL is recognised as the most influential terrorist group in the world. Propaganda or recruiting in some social networks and encrypted communication in Internet are recognised their daily activity in cyberspace. On the other hand, direct harmful activity in Internet was not so common until now. Malware attack to reveal opposite media group location is an example reported by the citizen lab [66]. According to the analysis, ISIL send an URL linked to images of US air strikes via email to opposite media group, which revealed human rights, abuse by ISIL. The link was crafted to download malware, which send out IP address of downloader to detect geo location.

Another way to illustrate terrorism in Internet is back to definition of cyber terrorism.

According an analysis from CCD COE, term of "cyber terrorism" should be used only when the incident "matched with the combination of political or social motivation, serious damage, and fear" [67].

5.2.5. State sponsored group

Ultimate goal of their activity is to take advantage from oppositions. Based on great capability, state sponsored group conduct attacks with integrated various methods. Stuxnet is the most famous case, which have state owned background [20]. Operation Cleaver is suspected as a counter campaign to Stuxnet by a security firm, Cylance. In the report, targets from the Iranian group are " military, oil and gas, energy and utilities, transportation, airlines, airports, hospitals, telecommunications, technology, education, aerospace, Defence Industrial Base (DIB), chemical companies, and governments" [68]. They extracted sensitive information from those target in following countries: "Canada, China, England, France, Germany, India, Israel, Kuwait, Mexico, Pakistan, Qatar, Saudi Arabia, South Korea, Turkey, United Arab Emirates, and the United States" [68].

5.3. Attacking test in a network simulator

Based on a scenario from previous security analysis, a preliminary attack was performed in the network simulator. The scenario is similar to spear fishing attack, which is targeting to steal user data. The attacker tries to intercept radio communication with a malicious IoT device, which is developed same IoT OS. Based on the scenario, packet sniffing and sending the data to desired IP address are implemented. Then the malicious IoT functions are tested in the network simulator. Open source developer for an IoT OS, Contiki, provides the simulator. The simulation environment is distributed as virtual machine image with some useful tutorials.

The scenario is that an attacker approach to a smart house physically then conducts MITM attack in wireless network. The reason to attack wireless network instead of remote attack is the IoT wireless network is under home routers. Therefore direct attack to IoT devices need bypath firewall of home routers. Regarding the network structure sniffing wireless communication is chosen.

Since Contiki is well organised open source project, there are well-developed core modules. Therefore it enables speedy IoT system developing on top of the OS. In this test, same IoT OS is introduced to build malicious IoT device. Prepaired core software module for speedy development is a reason to chose Contiki but also same framework let more easier communication to target devices is another reason.

6. Security Analysis

6.1. Purpose

The purpose of the analysis is studying security issues especially for the IoT projects. Though the analysis special threats for IoT are considered since there are unconventional cases compared to ordinary network devices. Result of this security analysis may help to establish future security guidelines for IoT system development. In this study an IoT project is picked up in order to study actual case. The SPHERE project, introduced in background section, is an academic healthcare IoT project. Therefore this analysis contributes two axis for next IoT development.

First point of view is healthcare. Healthcare data is obviously sensitive information from life support and privacy. Naturally information from medical devices may contain some indication of disorder. Currently those sensitive data is treated only by health care workers however if healthcare data leaked to unauthorised groups there will be unexpected harm cases.

Another feature is that the project is an academic study. Compared to private sector projects, there are more challenging studies in academic. Those studies are leading latest technology but on the other hand projects are proceeding with many unclear matters. When an attacker gets interest to those activities it will lead unfamiliar cases from known examples. Normally academic activity reports their findings for scientific contribution. Those opened information have also potential for reconnaissance use to future attacks.

6.2. Scope

Scope of this study is the SPHERE project and mainly for IoT related part. Figure 4 shows overview of the network. The project collects data from end devices (sensors and camera) to home gateway/hub once. After collected data from end devices then the data send to data hub. Thus the flow between end devices and home gateway/hub is IoT communication therefore it is the main target for analysis. After processes include download data

from data hub or data analysis in researchers PC are out of scope. Technical information, which is network schematics or running OS, is obtained from opened materials. Main sources of technical details are those academic papers [5] [69].

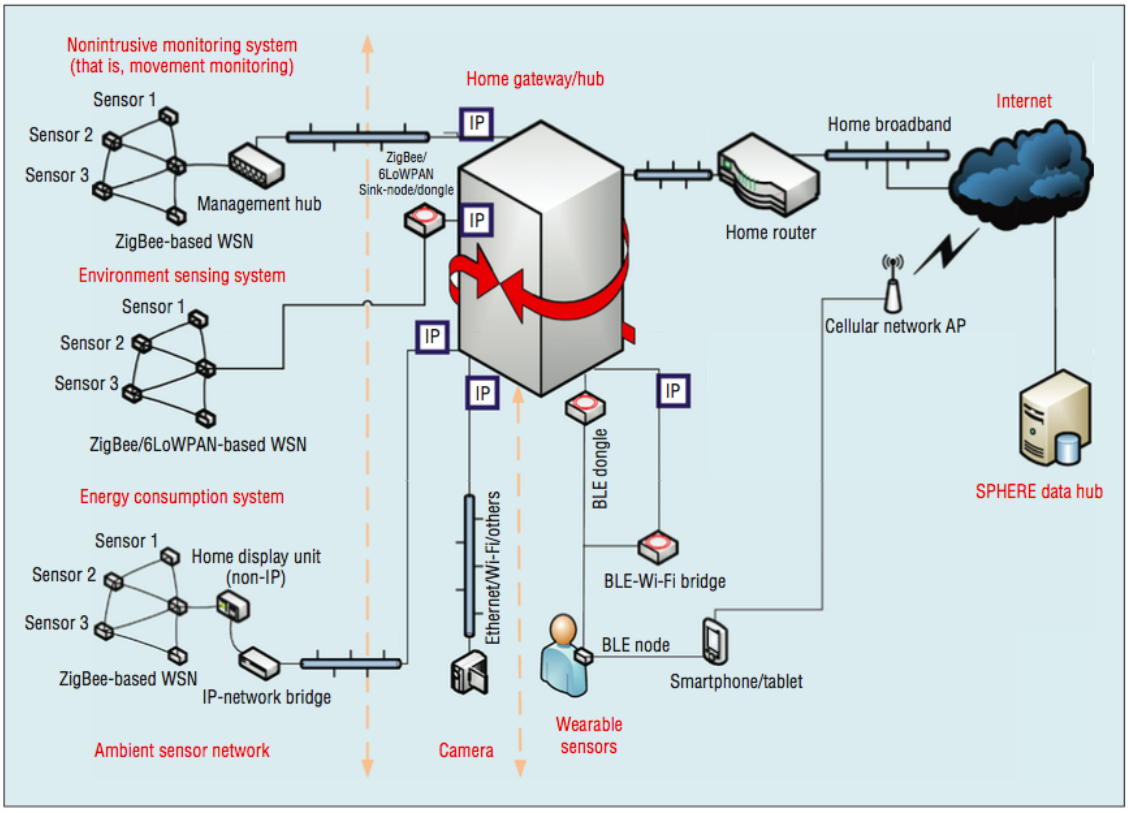

Figure 4. Network schematic of the project [5].

6.3. Research Asset Identification

All type of assets are analysed here in order to identify threats in the project. Analysis procedure is following steps; firstly research processes are identified to cover all data flows in the system then research assets, which are data in the system.

6.3.1. Research processes

Data flows are categorised to acquiring data and management of the system. Main difference between two data flow is type of data. Data acquisition flow handle private healthcare

data thus confidentiality need special care. In addition quality and amount of data need care for research activity since keys of big data analysis are those amount and quality. In this analysis the data flow has two sub categories.

- Acquire user data
  - From contiki mote or camera to home gateway
  - Home gateway to data hub

First flow is between end nodes to home gateway. The first flow has special feature because it is based on IoT technology. Special light weight OS for IoT are working for sensing real-time user healthcare data and transmit data packet to home gateway. Those activities are recognised as multitask and it needs special care to implement for resource constrain devices. RTOS is a typical solution for the multitask. The OS have scheduling function which prioritise multiple task in order to keep vital function. Network communication is the most common vital function since it needs some reaction in specific time window. Wireless communication is also typical function for IoT. It is very convenient for large number of nodes to communicate but on the other hands it also easy for sniffing communication. This means the flow has potentials to be attacked by reply attacks or various MITM attacks.

Second flow is between home gateways to data hub. This is a conventional data flow because communication structure is same to home PC to could server. What is a special for the project is the home gateway correct data from multiple node then send out to cloud. Therefore this is a break point of end-to-end encryption

- Management the system
  - Renew authentication credentials
  - Software update
  - Modification of settings

Management of the system is also important data flow. Common requirement for all data flow is scalability because there are more 100 smart houses in the project. Remote operation and automation are key ideas for efficient management.

Authentication credentials are highly confidential data to encrypt data flow. From designing point of view, there can be two type of credentials regarding the network structure. One of the credentials is IoT side and anther one is between home gateway and data hub. On the IoT communication, encryption method should be light to handle by resource-constrained devices. Public key encryption is powerful solution for untrusted routes but it needs more computational power. On the other hand symmetric key encryption is relatively light with difficulty for update key distribution .

Software update is also an interesting task for maintain network. There are always needs for update to improve the system. Sometimes it comes from security patch for software module or sometimes own specification change. Falsified software allows backdoors to attacks and disrupted software harm data acquisition activity. Settings for network devices are also same effect of them. Thus those data flow should be protected by proper methods.

6.4. Information System Asset Identification (Hardware, Software)

- Ambient sensors, Wearable sensors
- Camera
- Home hub
- Home router
- Data hub

Ambient sensors and wearable sensors are running on IoT technologies. Their OS is Contiki thus fundamental functions are based on open source software. Real implementation is not opened thus they may have some functions, which are specially developed only for the project. Basic function is sensing data then send the data to home hub. Routing, which is establish routing table, and transferring data are also a function of IoT OS. Identification and authentication are required steps for opening secure communication. Encryption is also important function for secure communication however it is know to a resource-consuming task.

Cameras are also called network camera since they have network capability for communication. When a global IP address is assigned to the camera without any modification to default password, it is a case of public disclosure for video streaming. Video streaming need computational power since an image is naturally two dimension data and usually they are processed 30 images per a second. Encoding is also costly mathematical task for processors. Thus for real-time streaming normally special hardware (graphic processor) is introduced. Regarding nature of image processing, those hardware have effective structure for parallel processing. Some malicious factions point out those advantages then abuse crypto currency mining on botnet of network camera.

Home hubs are collecting data from sensors and cameras. Collected data is send to data hub via SSH or VPN.

6.5. CIA threat analysis result

In this section, 4 research assets are analysed from CIA point of view. Each cross points is described with potential issues together with rage of failure.

	Authentication credentials	User data	Command and control data (shell commands, web interface)	Software
Confidentiality	Cause discloser of user data, provide computational or network resources for unintentional use	@Data hub; disclose whole collected user data of the project, transferring data to unauthorised external points. @Home gateway; disclose user data in a house. @Sensors, Cameras;	Provide materials for replay attacks	Provide clue for various attacks; disclosure of user data, abuse of NW or computational resource, denial of service
Integrity	Cause disability to login network hardwares	Failure to research activity, loss of acquired data	Miss configuration of network hardwares	Implementation backdoors to network hadwares
Availability	Cause disability to login network hardwares	Failure to research activity, loss of acquired data	Failure to research activity, cause system down	Failure to research activity, cause system down

6.6. Threat source based scenarios

In this section, information system assets are analysed base on type of attackers. The attacker type is characterised by their goals and techniques. Figure 5 shows overview of the threats.

	C-I-A threats category	Target	Method
Criminals	Availability of U-data	User data	Ransom data
Criminals	Integrity of C&C	Network ability	Abuse as a botnet
Hactivism	Availability of C&C	Failure of research activity	Denial of service
Hactivism	Integrity of U-data	Failure of research activity	Demolish data
Gray hats	Confidentiality of Software	Any security hole	Disclose security failure
State owned group	Confidentiality of U-data	User data	Radio interception

Figure 5. Scenarios of the threats.

6.6.1. Gray hats

Gray hats, also known as security researchers, are trying to find new security hole. In this project, therefore communication between sensors and home hub can be a target because of novelty. Some of attacking software tools (eg. killerbee [70]) is applicable for MITM attack to wireless communications. Debugging tools have also chance to introduce for sniffing. In this case, if some security hole is existing, there is a chance to break confidentiality of user data. This is costly for attackers because they need physically move to wireless communication area. Another possibility is intrusion from IoT wireless network to home network. Finding weakest link is common cense for attacker side. Therefore even if their target is to compromise whole project network, as a gate, wireless communication in home network will be a target.

In this category, insider threats also should be discussed. Physical access to IoT modes or home gateway is basically allowed only to residents. There is still chance to research

with physical communication like serial debugging tools however probability seems to be low.

6.6.2. Hactivism

Although there is not famous cases that hactivist attack academic research, availability of project resources can be a target. Loss of integrity on user data can be another threats by targeting failure of research activity. Terror based on health condition is also a possible scenario.

6.6.3. Criminals

Ransom user data at data hub is a threats because the hub keep valuable research data then it is easy to monetise. A researcher who has malicious intention can be insider threat case. Fraud based on health condition is also a possible scenario. Abuse IoT mote, home hub or home router to create botnet is another threat for the project.

6.6.4. State owned: APT

If there are interesting target person in the subjects for example high profile person, state owned group might abuse healthcare data as intelligence. This is a similar method to the spear fishing in terms of targeting personal information to accomplish attacker's purposes.

7. Attacking test

Purpose of this experiment is proof of concept based on a scenario from previous threat analysis. In this scenario, an attacker performs MITM attack with a malicious IoT device. Technically attacking idea is that a malicious IoT get into wireless network then send out payload of all packet passing the device. Procedure of the experiment started code analysis for Contiki core functions. Since Contiki OS is open source, latest version is provided via github. In this step, implementations of layered network protocols were analysed to find out way to carry out the attack. After the review of code, lowest layer of MAC was chose then copying payload and sending functions are implemented. The malicious IoT code was tested in the simulation environment (Cooja). From this test, although they were fragmented, some of payloads were sent to outside node.

7.1. Technical overview

Fundamental plan to extract user data, which is measured at IoT end node, is based on radio interception and abuse connectivity of routing protocols. From opened information it is not unclear about encryption for data handling and authentication to get into wireless network, the simplest condition is temporary set as an assumption. Therefore attacking to encryptions and spoofing credentials are out of scope for this trial.

Figure 6 shows physical position of IoT devices in the simulation. Positions of #2 to #9 were randomly selected and #1 and #10 are located by manually to follow the scenario. There is a border router which is handling data from IoT node to send out thus all measured data pass though the border router, #1. #2 to #9 are normal IoT devices which are measuring and sending data via wireless communication. In addition, #10 is a malicious node which is sniffing radio communication and sending data to specific outside node. In the figure, green circle show radio communication area of #10. Therefore the malicious one have chance to sniff communication in the area but it is based on routing table decided by a protocol, RPL. In this scenario no authentication to join in the IoT network, physical distance is main factor to construct routing path. Other factors are related workload of each nodes since just transferring a packet is not easy task for resource constrained IoT devices. In brief, at least #10 have chance to transfer packets from #3 to #6 in this

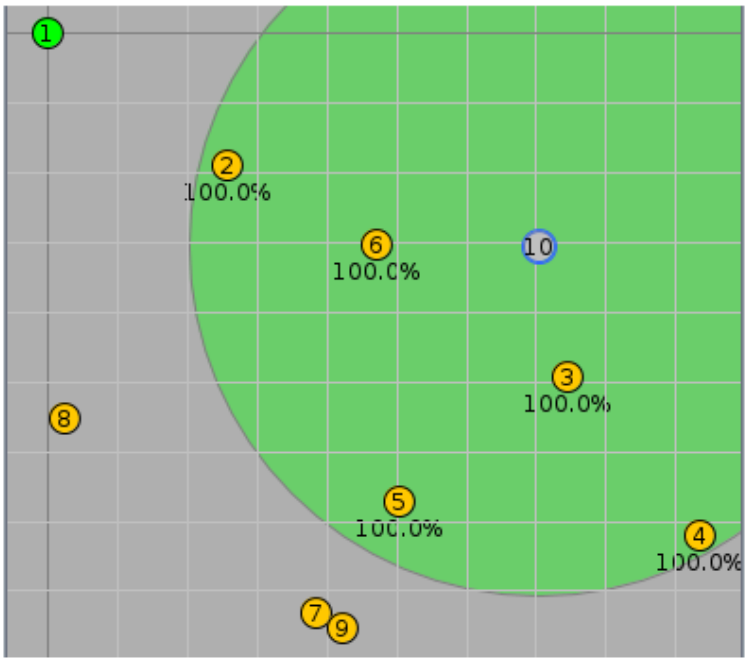

Figure 6. Positions of IoT devices. #1 is the border device and #10 is the attacker.

position.

In this test setup TUN (tunslip6) was introduced to communicate between the network simulations to host machine. Thus via the TUN interface, border router (#1) and host machine which run the network simulator communicate. Then netcat (nc) received packets. Details of those setups are provided by some tutorials [71] [72]. For communication between #10 to host running netcat, UDP is introduced regarding to level of network reliability.

To be more realistic, a sample story will be that there is a malicious attacker brings a radio intercept device and puts it close to window side of a smart house. A device is based on same IoT OS and similar devices for speedy development.

7.2. Implementation of malicious functions

In order to build malicious IoT node which have sniffing and sending data, same IoT OS was introduced because connectivity point of view. If a malicious node have some similarities it is easier to get into the network without suspicious behaviours. After the

decision of platform selection, next task was protocol stack analysis.

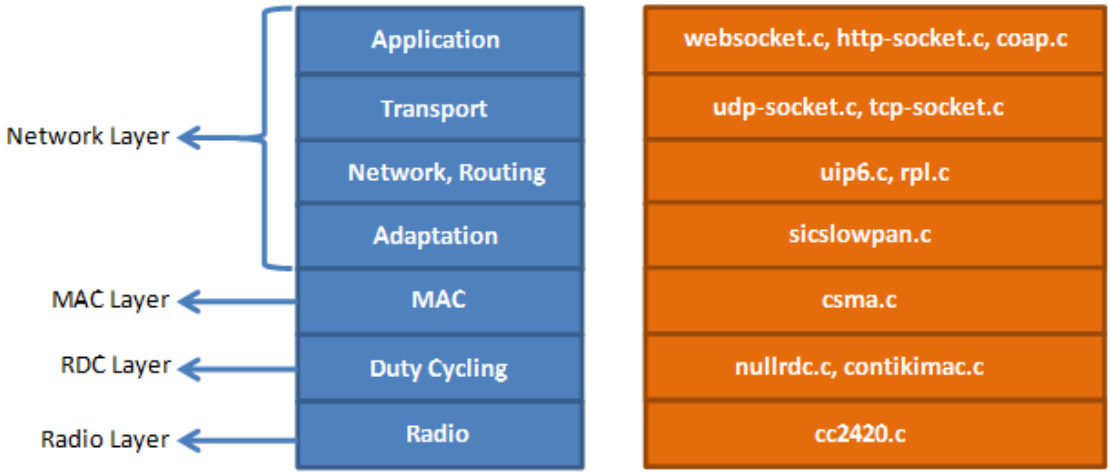

Figure 7. Network stack of Contiki [6]

Figure 7 shows network stack of Contiki. After the analysis, MAC layer was chosen to implement additional code to interceptions because transfering packets are processed in the MAC layer. However not all incoming data is processed in the node since computational ability is distributed to multiple tasks. This is a key feature of IoT node and it comes from limited capacity of embedded devices.

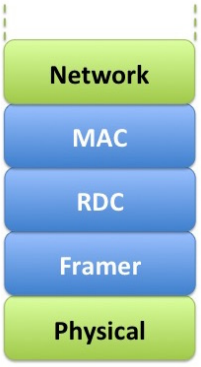

Figure 8. Inside layer of MAC layer [7]

In the MAC layer, Contiki have 3 internal layeres. Figure 8 shows the internal layers. From those three layer, lowest Framer layer is chosen to extract data because all incoming frame is examined first in the layer. The decision is based on following features of each layers. Framer, which is creating a frame, to be send and parsing incoming data. RDC means radio duty cycle which handle sleeping functions. Battery power device usually choose sleeping function to save energy but network connectivity should be kept some

quality. Therefore the RDC layer decides timing to transmit data. Top layer is MAC layer, which is handling addressing, and retransmission of lost packet.

Main concept for an implementation is sending out data as much as possible. The reason is if the implementation needs huge computational power to an embedded device, the desired function is never achieved. Based on the concept, three parameters was achieved trough multiple trials. The source code is located at Appendix 1 in this document. First parameter is reducing frames to process to 10 %. Therefore only one of ten frame is processed (at line 20). Second parameter is selecting length of array to reduce addressing information (at line 23). Final parameter make the node silent until initial routing is established (at line 23) because at the stating up device consume resource.

7.3. Output and evaluation

Through the test, some of packet payload was observed. Figure 9 shows a part of result. For more detail of the result is attacked at Appendix 2. In this experiment, some of http packets were exchanged to retrieve temperature data from normal nodes. In the output the http request and response were observed. For example IP address of #4 (aaaa::212:7404:4:404) was in the result. It indicates that data treated in malicious #10 node were captured and sent out to the desired host. Possible reasons for fragmentations are not well considered implementation or unreliable wireless UDP communication. There is more space to add evidence to explain logically and chance to improve the code however for this study, this was the best practice at this moment.

Figure 9. Observed fragmented payloads.

8. Conclusion

Through this study, multiple potential threats for healthcare IoT system were revealed. Regarding to the threats, low cost attacking method was performed in a network simulation. In addition, three main suggestions to improve security of IoT systems are proposed. For next generation IoT that handle feedback signal to end devices, further threat is also discussed.

As far as we know, spear phishing to healthcare IoT has not reported but claimed as a possible scenario by this study. Since healthcare IoT is under developing now but it can be happen at conventional medical devices. The idea should be carefully considered although it sounds a scientific fiction because it enables remote attacks. Regarding the car hacking development, it is not strange there is a state funded research activity to investigate the scenario. On the other hand, impact of the scenario may considered to disclose results of related studies. This is a contradiction about openness of information between original concept of Internet and national security. This is also a typical example that each Cybersecurity specialist is demanded to make decisions based on various ethics way of thinking or welfare of the public.

Other threats, ransom data or abuse as a botnet, are learned from related works. For these issues, enough resources should be paid in order to keep secure Internet because attacker side just think IoT as a new low security nodes. IoT have direct connectivity to Internet but weak security features, which come from resource, constrain platforms. This is the typical attacking point as a weakest chain. Of course demands for innovative products is high from business point of view but we need pay some costs to security of IoT. In this discussion, cost is not just financially but also energy (buttery usage), computational power (CPU design, duty cycle), or discussions in groups for example in the IETF.

From technical study, the spearfishing scenario was tested in the network scimitar. In this trial data interception in wireless network was partially achieved in order to proof the concept. In addition this is a finding that if malicious devices are developed on top of IoT OS to target project it provides speedy development but also hinder performance of attacks. This is because IoT hardware limits the malicious activities. Thus it is good practice for attackers to prepare highly resourced device compared to target nodes.

To improve IoT security there are three suggestions from this study. First suggestion is providing useful security module for IoT. It can be provided with OS or cloud services by software. For example, AES128 is supported in Contiki core module. In cloud services, Amazon AWS IoT supports X.509 certificate. Hardware encryption by external chip or SoC is also improove security feature in IoT systems. Of course standardisation of secure protocols is important activity as a basis of IoT technology.

Second suggestion is providing decision making support tool to decide security level to implement. It is important to chose reasonable level of security regarding requirements; cost versus security level. Thus the tool showing security index with examples can help to make the decision. The cost includes not only financially but also energy (battery usage) or computational resource (memory footprint, processing power).

Last one is continuous taking attention and rising awareness for IoT security. These activities are not only for IoT professionals but also people who have chance to be a user. Based on widely understanding to the technologies, security level will be improved from various aspects. For example, social awareness help to foster the norm then step up to legislation processes.

In short to reduce the threats in the system, RF interception on IoT network, encrypted message or secure routing algorithm are software solutions. Although it has chance to decrypt messages, basic encryption can prevent simple sniffing trial. Routing algorithm for wireless devices especially in mesh topology is complicated but it is important to validate devices for participation.

For hardware, optical or wired communication help to prevent data leakage. Wireless communication is naturally spread signals around source devices however optical communication restrict the leakage by covering light. The way is more tangible or easy to understand than restricting electromagnetic wave. Of course wired communication reduce the chance to intercept signal.

Regarding further potentials of IoT, forthcoming threats will be discussed. Currently IoT projects are focusing acquiring data from devices and also processing of those data. Big data analysis or artificial intelligence is relative topic because those technologies are applied to processing part. Behind the IoT system, there is an idea, which enables more efficient society. Sometimes it is called smarter system thus some intelligent mechanisms

are introduced. The idea is the feed back control loop with IoT nodes and artificial intelligence. Especially feedback signal and physical end effectors are key components for next generation. Those effectors, for example insulin pumps for diabetes, receive signals from controllers, which are trained by big data and sophisticated algorithms.

When the feedback loop realised there will be more physical threats. There are two reasons for this hypothesis. In this situation more medical devices receive orders from remote site therefore command and controls for those systems should be carefully designed. Another reason is training data set, which is sent from IoT node should not be contaminated. Simply, if malicious data is inserted to training data to an artificial intelligence, trained algorithm output incorrect order to end effectors. Normally noise is considered as a harm source for teaching however intentional malicious training data may lead more effective but undesirable results.

There is a case to predict future threats. Microsoft launched artificial intelligence bot on Twitter but it started tweeting racism comments [73]. This is just because the bot have "repeat after me" vulnerability which is innocently learning anything [74]. This is a proof of concept to inject malicious input to an artificial intelligence. Roman Yampolskiy, head of the Cybersecurity lab at the University of Louisville, published a paper about threats related to artificial intelligence [75]. In the paper the author classified undesirable circumstance with artificial intelligence. Sometimes science fiction stories predict future issues by technologies thus now we should start seriously thinking about HAL 9000 era.

References

[1] Postscapes. (2015) Internet of things protocols and standards. (2016, Mar. 3). [Online]. Available: http://postscapes.com/internet-of-things-protocols

[2] butler iot. (2012) Butler project overview. (2016, Mar. 3). [Online]. Available: http://www.slideshare.net/butler-iot/butler-project-overview-13603599

[3] P. S, P. H, B. P, and R. M. Chan L, "A review of wearable sensors and systems with application in rehabilitation." *Journal of Neuroeng Rehabil*, vol. 9, no. 21, 2012.

[4] W. Wineberg. (2015) Cameras thermostats and home automation controllers hacking 14 iot devices. [Online]. Available: https://www.iotvillage.org/slides_DC23/IoT11-slides.pdf

[5] N. Zhu, T. Diethe, M. Camplani, L. Tao, A. Burrows, N. Twomey, D. Kaleshi, M. Mirmehdi, P. Flach, and I. Craddock, "Bridging e-health and the internet of things: The sphere project," *IEEE Intelligent Systems*, vol. 30, no. 4, pp. 39–46, 2015.

[6] [Online]. Available: http://anrg.usc.edu/contiki/index.php/Network_Stack

[7] [Online]. Available: http://anrg.usc.edu/contiki/index.php/MAC_protocols_in_ContikiOS

[8] T. I. Incorporated. (2015) Application areas for the internet of things. (2016, Mar. 3). [Online]. Available: http://www.ti.com/ww/en/internet_of_things/iot-applications.html

[9] S. N. M. of American History. (1994) Log book with computer bug. [Online]. Available: http://americanhistory.si.edu/collections/search/object/nmah_334663

[10] konczal@csrc.ncsl.nist.gov. (1994) Next: Current protection against up: Viruses previous: Viruses history of viruses. [Online]. Available: http://csrc.nist.gov/publications/nistir/threats/subsubsection3_3_1_1.html#SECTION00031100000000000000

[11] P. J. Denning, *Computers Under Attack: Intruders, Worms, and Viruses*. ACM Press, 1990.

[12] F.-S. Corporation, “Brain searching for the first pc virus in pakistan,” 2011. [Online]. Available: https://campaigns.f-secure.com/brain/

[13] J. STRICKLAND. (2007) How arpanet works. [Online]. Available: http://computer.howstuffworks.com/arpanet.htm

[14] U. The National Science Foundation. (2000) From modest beginnings. [Online]. Available: http://www.nsf.gov/about/history/nsf0050/internet/modest.htm

[15] W. Stewart. (2000) Csnet – computer science network. [Online]. Available: http://www.livinginternet.com/i/ii_csnet.htm

[16] J. KELLER. (2010) Evaluating iran’s twitter revolution. [Online]. Available: http://www.theatlantic.com/technology/archive/2010/06/evaluating-irans-twitter-revolution/58337/

[17] C. Huang. (2011) Facebook and twitter key to arab spring uprisings: report. [Online]. Available: http://www.thenational.ae/news/uae-news/facebook-and-twitter-key-to-arab-spring-uprisings-reporthttp://www.thenational.ae/news/uae-news/facebook-and-twitter-key-to-arab-spring-uprisings-report

[18] J. DAVIS. (2007) Hackers take down the most wired country in europe. [Online]. Available: http://www.wired.com/2007/08/ff-estonia/

[19] A. International. (2012) The russo-georgian war 2008 : The role of the cyber attacks in the conflict. [Online]. Available: www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf

[20] N. Falliere, L. O. Murchu, and E. Chien. (2011) W32.stuxnet dossier. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[21] MANDIANT. (2013) Apt1 exposing one of china’s cyber espionage units. [Online]. Available: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

[22] F.-S. L. T. INTELLIGENCE. (2015) The dukes 7 years of russian cyberespionage. [Online]. Available: https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

[23] I. A. Board. (2016) A brief history of the internet advisory / activities / architecture board. [Online]. Available: https://www.iab.org/about/history/

[24] USENIX. (2016) History. [Online]. Available: https://www.usenix.org/about/history

[25] M. CURPHEY. (2014) The start of owasp – a true story. [Online]. Available: https://blog.srcclr.com/the-start-of-owasp-a-true-story/

[26] A. Deep. (2015) Hybrid war: Old concept, new techniques. [Online]. Available: http://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques

[27] U. HEADQUARTERS DEPARTMENT OF THE ARMY. (2014) Fm 3-38 cyber electromagnetic activites. [Online]. Available: http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf

[28] S. STARR, D. KUEHL, and T. PUDAS, "Perspectives on building a cyber force structure," in *Conference on Cyber Conflict Proceedings*, 2010, pp. 163 – 181.

[29] R. A. FORCE. (2005) The early years of military flight. [Online]. Available: http://www.raf.mod.uk/history/shorthistoryoftheroyalairforce.cfm

[30] J. B. A. B. Air Force Historical Studies Office. (2011) 1947 – the national security act of 1947. [Online]. Available: http://www.afhso.af.mil/afhistory/factsheets/factsheet.asp?id=15239

[31] K. Ashton. (2009, June) That 'internet of things' thing. (2016, Mar. 3). [Online]. Available: www.rfidjournal.com/articles/view?4986

[32] Z.-K. Zhang, M. C. Y. Cho, Z.-Y. Wu, and S. W. Shieh, "Identifying and authenticating iot objects in a natural context," *IEEE Computer*, vol. 48, no. 8, pp. 81–83, Aug 2015.

[33] S. Haller, S. Karnouskos, and C. Schroth, "The internet of things in an enterprise context," *Future Internet— FIS 2008, Springer*, pp. 14–28, 2009.

[34] I. T. Union. (2012) Internet of things global standards initiative. (2016, Mar. 3). [Online]. Available: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

[35] I. Amazon Web Services. (2015) Aws iot. (2016, Mar. 3). [Online]. Available: https://aws.amazon.com/iot/

[36] I. E. T. Force. (2014) The constrained application protocol (coap). (2016, Mar. 3). [Online]. Available: https://tools.ietf.org/html/rfc7252

[37] M. Kovatsch and A. D. Simon Duquennoy, "A low-power coap for contiki," *Mobile Adhoc and Sensor Systems (MASS)*, pp. 855 – 860, 2011.

[38] X. S. Foundation. (2015) History of xmpp. (2016, Mar. 3). [Online]. Available: http://xmpp.org/about/history.html

[39] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[40] itwebnnet. (2016) Ukraine power station outage – enabled by malware, but not caused by malware. (2016, Mar. 3). [Online]. Available: ttp://hardware.slashdot.org/story/16/01/11/150241/ukraine-power-station-outage----enabled-by-malware-but-not-caused-by-malware

[41] I. project, "View camera online in harjumaa, tallinn," 2015, (2016, Mar. 3). [Online]. Available: http://www.insecam.org/en/view/169414/

[42] M. Corporation. Common vulnerabilities and exposures. [Online]. Available: https://cve.mitre.org/index.html

[43] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: A survey of existing protocols and open research issues," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[44] S. Raza, H. Shafagh, K. Hewage, and R. Hummen, "Back to results lithe: Lightweight secure coap for the internet of things," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3711 – 3720, Oct 2013.

[45] X. He, M. Niedermeier, and H. de Meer, "Dynamic key management in wireless sensor networks: A survey," *Network and Computer Applications*, vol. 36, no. 2, pp. 611–622, 2013.

[46] T. Savolainen, J. Soininen, and B. Silverajan, "Ipv6 addressing strategies for iot," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3511–3519, 2013.

[47] J. Matherly. (2013) The search engine for iot. [Online]. Available: https://www.shodan.io/search?query=medtronic

[48] S. ERVEN. (2014) Just what the doctor ordered? [Online]. Available: https://www.defcon.org/images/defcon-22/dc-22-presentations/Erven-Merdinger/

DEFCON-22-Scott-Erven-and-Shawn-Merdinger-Just-What-The-DR-Ordered-UPDATED.pdf

[49] K. Hayashi. (2014) Iot worm used to mine cryptocurrency. [Online]. Available: http://www.symantec.com/connect/blogs/iot-worm-used-mine-cryptocurrency

[50] J. Ullrich, "More device malware: This is why your dvr attacked my synology disk station (and now with bitcoin miner!)," 2014. [Online]. Available: https://isc.sans.edu/diary/More+Device+Malware%3A+This+is+why+your+DVR+attacked+my+Synology+Disk+Station+%28and+now+with+Bitcoin+Miner%21%29/17879

[51] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, and C. Rossow, "Iotpot: Analysing the rise of iot compromises," *9th USENIC Workshop on Offensice Technologies*, 2015.

[52] (2013) Rerum: Reliable, resilient and secure iot for smart city applications. [Online]. Available: https://ict-rerum.eu/

[53] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," in *MILITARY COMMUNICATIONS CONFERENCE*, 2010, pp. 1830–1835.

[54] M. Hyppönen. (2015) Salvestus: Mikko hyppöneni avalik loeng it kolledžis. [Online]. Available: http://www.itcollege.ee/blog/2015/10/13/avalik_loeng/

[55] US-CERT. (2005) Cyber threat source descriptions. [Online]. Available: https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions

[56] D. of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities. (2015) Critical infrastructure protection. [Online]. Available: http://www.gao.gov/products/GAO-05-434

[57] C. Miller and C. Valasek. (2014) Adventures in automotive networks and control units. [Online]. Available: http://illmatics.com/car_hacking.pdf

[58] ——, "Remote exploitation of an unaltered passenger vehicle," in *DEF CON 23*, 2015. [Online]. Available: https://www.youtube.com/watch?v=OobLb1McxnI

[59] ——. (2015) Remote exploitation of an unaltered passenger vehicle. [Online]. Available: http://illmatics.com/Remote%20Car%20Hacking.pdf

[60] Kevin mitnick. [Online]. Available: https://en.wikipedia.org/wiki/Kevin_Mitnick#Consulting

[61] (2012) Ptes technical guidelines. [Online]. Available: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

[62] P. Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. Back Bay Books, 2013.

[63] ——. (2012) Parmy olson on anonymous: 'a growing phenomenon that we don't yet understand'. [Online]. Available: http://www.rferl.org/content/parmy-olson-on-anonymous-a-growing-phenomenon-that-we-dont-yet-understand/24607895.html

[64] R. Winton. (2016) Hollywood hospital pays 17,000 usd in bitcoin to hackers; fbi investigating. [Online]. Available: http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

[65] J. PORUP. (2015) Ransomware is coming to medical devices. [Online]. Available: http://motherboard.vice.com/read/ransomware-is-coming-to-medical-devices

[66] J. Scott-Railton and S. Hardy. (2014) Malware attack targeting syrian isis critics. [Online]. Available: https://citizenlab.org/2014/12/malware-attack-targeting-syrian-isis-critics/

[67] A.-M. TALİHÄRM, "Cyberterrorism: in theory or in practice?" *Defence Against Terrorism Review*, vol. 3, no. 2, pp. 59–73, 2010.

[68] C. Inc. (2014) Operation cleaver. [Online]. Available: http://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdfhttp://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf

[69] P. Woznowski, X. Fafoutis, T. Song, S. Hannuna, M. Camplani, L. Tao, A. P. andEvangelos Mellios, M. Haghighi, N. Zhu, G. Hilton, D. Damen, T. Burghardt, M. Mirmehdi, R. Piechocki, D. Kaleshi, and I. Craddock, "A multi-modal sensor infrastructure for healthcare in a residential environment," in *2015 IEEE International Conference on Communication Workshop (ICCW)*. IEEE, 2015, pp. 271–277.

[70] [Online]. Available: https://github.com/riverloopsec/killerbee

[71] [Online]. Available: http://cnds.eecs.jacobs-university.de/courses/iotlab-2013/cooja.pdf

[72] [Online]. Available: http://anrg.usc.edu/contiki/index.php/RPL_Border_Router

[73] R. Price. (2016) Microsoft is deleting its ai chatbot's incredibly racist tweets. [Online]. Available: http://www.businessinsider.com/microsoft-deletes-racist-genocidal-tweets-from-ai-chatbot-tay-2016-3?r=UK&IR=T

[74] A. Ohlheiser. (2016) Trolls turned tay, microsoft's fun millennial ai bot, into a genocidal maniac. [Online]. Available: https://www.washingtonpost.com/news/the-intersect/wp/2016/03/24/the-internet-turned-tay-microsofts-fun-millennial-ai-bot-into-a-genocidal-maniac/

[75] R. V. Yampolskiy, "Taxonomy of pathways to dangerous ai," *arXiv, Cornell University Library*, 2015. [Online]. Available: http://arxiv.org/abs/1511.03246

Appendix 1

A function (leak_packet) learned from "udp_client" in ipv6 example, implemented in "/contiki/core/net/mac/frame802154.c".

```
void
leak_packet(uint8_t *data, int len)
{
  static int seq_id = 0;
  char buf[MAX_PAYLOAD_LEN];
  static int c = 0;
  static int x = 0;

  seq_id++;
  printf("LEAK! %d from crafted client \n", seq_id);

  //# establish udp socket
  if(seq_id < 2){
    uip_ip6addr(&server_ipaddr, 0xaaaa, 0, 0, 0, 0, 0, 0, 1);
    //   new connection with remote host
    client_conn = udp_new(NULL, UIP_HTONS(UDP_SERVER_PORT), NULL);
    udp_bind(client_conn, UIP_HTONS(UDP_CLIENT_PORT));
    printf("udp connected\n");
  }

  if(seq_id%10==0) //# reduce work load to 10%
  {
    for(c=0; c<len; c++){
      if(c>52 && seq_id>5){ //#52:only payload 5:keep calm until rpl
  routing set up
        buf[x] = data[c];

        if(c%MAX_PAYLOAD_LEN==(MAX_PAYLOAD_LEN-1)  )
          uip_udp_packet_sendto(client_conn, buf, MAX_PAYLOAD_LEN,&
  server_ipaddr, UIP_HTONS(UDP_SERVER_PORT));

        if(c== (len-1)  ){
          buf[len] = "/n";
          uip_udp_packet_sendto(client_conn, buf, x+1,&server_ipaddr,
  UIP_HTONS(UDP_SERVER_PORT));
        }
      }
```

```
35        }
          printf("\n");
37      }
    }
```

Appendix 2

Raw output of netcat listening (nc -6ul 5678).

```
1
##??##??##????#?%‘###??##??##??##0##??P?Ah1?#P?Ah1P?Ah1P?Ahb# P#P?
    Ah1sics.se/consics.se/csics.se/cP?Ai"#?P#P?Ai"#?P# deflate
3 Connection: keepP?Ai"#?P# deflate
Connection: kee#P
5 Connection: kee
Connection: kee?Ai"#?P# deflate
7 Connection: kee#P
Connection: kee
9 Connection: kee?Ai"#?P# deflate
Connection: keePPw??#
11 Connection: keePPw?
Connection: keePPw?P# deflate
13 Connection: keePPw??#
Connection: keePPw?
15 Connection: keePPw?P# deflate
Connection: keePPw?#?P#
17 Connection: keePPw?#?P#[aaaa::212:7404:4:404]
Us
19 Connection: keePPw?#?P#[aaaa::212:7404:4:404]
UP?q.$?#12:7404:4:404]
21 UP?q.$12:7404:4:404]
UP?q.$P#[aaaa::212:7404:4:404]
23 UP?A??#=P#12:74012:7404:4:404]
UHTTP/1.0 20tp://www.2:7404:4:404]
25 U#P.2:7404:4:404]
U.2:7404:4:404]
27 UTTP/1.0 20tp://www.2:7404:4:404]
UP?q/##?P#.2:7404:4:404]
29 UP?q/##?P# deflate
Connection: keep.2:7404:4:404]
31 UP?q/##?P# deflate
Connection: keeP?q/E#0P#
33 Conn
Conn4:4:404]
35 UP?q/##?P# deflate
Connection: keeP(??#
37 Connection: keeP(?
```

```
Connection: keeP(?P# deflate
Connection: keeP(?#
                  P#
Conn
Connection: keeP(?P# deflate
Connection: keeHTTP/1.0 20
Connection: keeHTTP/1.0 20tp://www.
Connection: keeHTTP/1.0 20tp://www.
Connection: keeP#?C?#9P#.
Conn.
Connection: keeHTTP/1.0 20tp://www.
Connection: keeP#?C?#?P#.
Connection: keeP#?C?#?P# deflate
Connection: keep.
Connection: keeP#?C?#?P# deflate
Connection: kee</body></ht
Co
Connection: keeP#?C?#?P# deflate
Connection: kee##0
Connection: keeP#?C?#?P# deflate
Connection: keesics.se/con
Connection: keesics.se/c
Connection: keesics.se/cP# deflate
Connection: keePF??_#0P#
Connection: keePF??_#0P# max-age=0
Connection: keePF??_#0P# max-age=0
ection: kee#P=0
ection: kee=0
ection: keeF??_#0P# max-age=0
ection: kee##??=0
ection: kee##??=0
ection: kee##??x-age=0
ection: keeP|??-##P#=0
=0
ection: kee##??x-age=0
ection: keeContent-typ=0
ection: ke=0
ection: kee##??x-age=0
ection: keeP{???#?P#=0
=0
ection: kee##??x-age=0
ection: keeP‘##??#=0
ection: keeP‘##?=0
```

```
ection: keeP‘##?x−age=0
ection: kee##0=0
ection: keeP‘##?x−age=0
ection: keeHTTP/1.0 20=0
ection: keeHTTP/1.0 20tp://www.=0
ection: keeHTTP/1.0 20tp://www.0
ection: keeP‘# ?#?P#.0
ection: keeP‘# ?#?P# deflate
Connection: keep.0
ection: keeP‘# ?#?P# deflate
Connection: keeP‘#!#CP#
Conn
```