Bachelor's Thesis

Degree programme in Information and Communications Technology

2021

Dung Ho

ENTERPRISE IOT DEVICE VISIBILITY

Forescout Technology Inc

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree programme in Information and Communications Technology

2021 | 52

DUNG HO

ENTERPRISE IOT DEVICE VISIBILITY

Forescout Technology Inc

This thesis examines the common protocols that are used in Enterprise IoT devices, especially the Bluetooth protocol. Bluetooth is a wireless technology that had been used widely since it was introduced by Ericsson in 1994. There are also several vulnerabilities that need to be addressed.

It is very important to gain a better understanding of the Bluetooth protocol in an enterprise in order to implement a secure Intrusion Detection System (IDS) and optimize the use of these devices. The goal of the thesis was to provide Bluetooth visibility, to study threat scenarios arising from the use of IoT in the enterprise, and to examine how to extend a commercial IDS in the ICS.

The thesis presents the work by researching through various reputed magazines to collect all the IoT protocols and their specifications and a Bluetooth module is implemented in the ICSP – a specific system that had been developed by the commissioning company, Forescout Technologies Inc. The module was implemented by assessing each technology stack access such as Python, Lua, and specialized wireless access points like Cisco Meraki SDK, Aruba.

The final Bluetooth module functioned properly and I was able to retrieve the list of wireless devices with the principal information of each device. Despite that, this module is a small but important part of IDS whose purpose is to identify the assets, the first important phase in Threat modeling. For further development, the project can be implemented by using the Simple Network Management Protocol (SNMP), an effective way to monitor the local traffic. The whole module can be used to develop the IDS in various industries such as Energy, Water, Fleet, Healthcare.

KEYWORDS:

IoT, Devices visibility, BLE, Protocol, SilentDefense, Cisco Meraki, Aruba, Python, Lua

CONTENTS

FIGURES

LIST OF ABBREVIATIONS

6LoWPAN	IPv6 and Low-power Wireless Personal Area Network
BD_ADDR	Bluetooth Device Address
BLE	Bluetooth Low Energy
CoAP	Constrained Application Protocol
HTTP	Hyper Text Transfer Protocol
HVAC	Heating, Ventilation and Air Conditioning
ICS	Industrial Control System
ICSP	Industrial Control System Patrol
IDS	Intrusion Detection System
IoT	Internet of Thing
MIMO	Multiple Input Multiple Output
MRI	Magnetic Resonance Imaging
mDNS	Multicast Domain Name System
RSSI	Received Signal Strength Indication
SDK	Software Development Kit
SNMP	Simple Network Management Protocol
SSDP	Simple Service Discovery Protocol
TCO	Total Cost of Owner
WLAN	Wireless Local Area Network

1 INTRODUCTION

Bluetooth is increasingly used in Enterprise IoT. Since it is a wireless communication system, so it is always possible for attackers to deliberately jam or intercept the transmission, or pass false, or modify information on the IoT device. When evaluating Bluetooth vulnerabilities and identifying the risks, it is very important to use the Bluetooth version and the efficiency of connectivity between devices. For instance, the device with the oldest version has a weaker connection and is less insecure than the device with the newest version.

The work carried out in this thesis will be referred to as the Bluetooth asset inventory project, as it has been commissioned as part of the greater Bluetooth project by Forescout Technologies Inc. In order to provide devices visibility in Enterprise IoT, the thesis collects a wider range of protocols that are currently available, including lower-layer protocols (especially wireless protocols such as Bluetooth, ZigBee, and Z-wave), application-layer protocols such as CoAP, and service discovery protocols such as mDNS and SSDP, to allow device visibility in the Enterprise IoT.

The goals of the thesis are:

- To understand the usage of Bluetooth and other IoT protocols in the enterprise (Chapter 2.3).
- To compare two solutions for improved visibility of wireless IoT devices (Chapter 3.2):
    - Leveraging enterprise-grade Wi-Fi Access Points (e.g., Cisco Meraki, Aruba Series 300 or series 500, and Juniper Mist).
    - Deploying a new sensor to scan for wireless devices.
- To extend a commercial IDS to provide Bluetooth visibility to validate the study by implementing a Bluetooth asset inventory project within the company (Chapter 4).
- To study threat scenarios arising from the use of IoT in the enterprise (Chapter 2.6.1).
- To develop and implement the threat modeling plan which is an effective way of identifying risks from a technical perspective (Chapter 2.6.2).

2 LANDSCAPE ANALYSIS

2.1 The company – Forescout Technologies Inc

Forescout Technologies Inc is the leader in visibility and control. Forescout has developed a unified security platform that enables enterprise and government agencies to achieve complete situational awareness of their extended enterprise environment and orchestrate actions to reduce cyber and operational risk. According to the latest report, more than 3700 customers in over 90 countries are relying on Forescout's infrastructure-agnostic solution to reduce the risk of business disruption from security incidents, ensure and demonstrate compliance with security and increase productivity in security operations (Forescout, 2020).

Forescout Technologies B.V formerly being known SecurityMatters was founded on Dec 9, 2009, in Eindhoven, the Netherlands. SecurityMatters is an international company that produces and delivers to the market cutting-edge network monitoring, intelligence, and protection technology to make its customers more secure and in control. SecurityMatters was acquired by Forescout Technologies Inc in 2018.

Forescout develops SilentDefense for the Operational Technology (OT) market, a network security monitor sold globally to customers in all kinds of industries including electricity, water distribution, oil & gas, and manufacturing.

2.2 Enterprise IoT

An IoT device is a bunch of hardware, sensors that transmit data from one place to another place over the internet, intranet, or LAN where they are connected. The Enterprise IoT devices are more specifically defined as devices connected to the network which gather usage, other data and provide insights based on that data to allow companies to cost reduction, efficiency gains, and new business opportunities. The enterprise networks can be chaotic and change often as devices move on or off the network. They might co-exist with other wireless or wired networks for fire and safety or environment controls.

Since the IoT devices have been used widely, IoT security has increased significantly and become an important aspect of IoT devices management. Every unsecured IoT device is considered as a vulnerability backdoor into an otherwise secure enterprise network. Hence, an enterprise IoT devices management platform is a requirement for the companies to efficiently and securely deploy, connect and maintain the range of IoT devices and sometimes overwhelming amounts of data.

2.3 IoT protocols

In the Industry 4.0 generator, IoT is one of the core elements and has several potential benefits.

Accordingly, to SecurityToday Research (Maayan 2020, 2), the number of IoT devices deployed all over the world during 2020 was estimated at 31 billion. Every second, 127 new IoT devices are connected to the internet. IoT devices keep increasing continuously, their number will reach 35 billion by 2021, and there will more than 75 billion IoT devices by 2025.

There are various types of IoT communication protocols available that have different capabilities, data rates, communication range, power, and memory. In terms of one or several of these factors, each has its own advantages and drawbacks. The following sub-sections present the most common protocols among the use of IoT devices in the enterprise.

2.3.1 Bluetooth Low Energy

Among the IoT protocols, the Bluetooth Low Energy (BLE) protocol was introduced recently. Bluetooth is the most widely used wireless technology for effective communication within the short range of approximately 10 meters (Figure 1). Between 2001 and 2004, it has been optimized as lower consumption and lower cost version Bluetooth Lowe Energy protocol or Bluetooth Smart by Nokia. The main advantage of BLE is offering significantly reduced power consumption while maintaining the communication range which is approximately 100 meters, ten times of standard Bluetooth (Ficco and Palmieri 2018, 217).

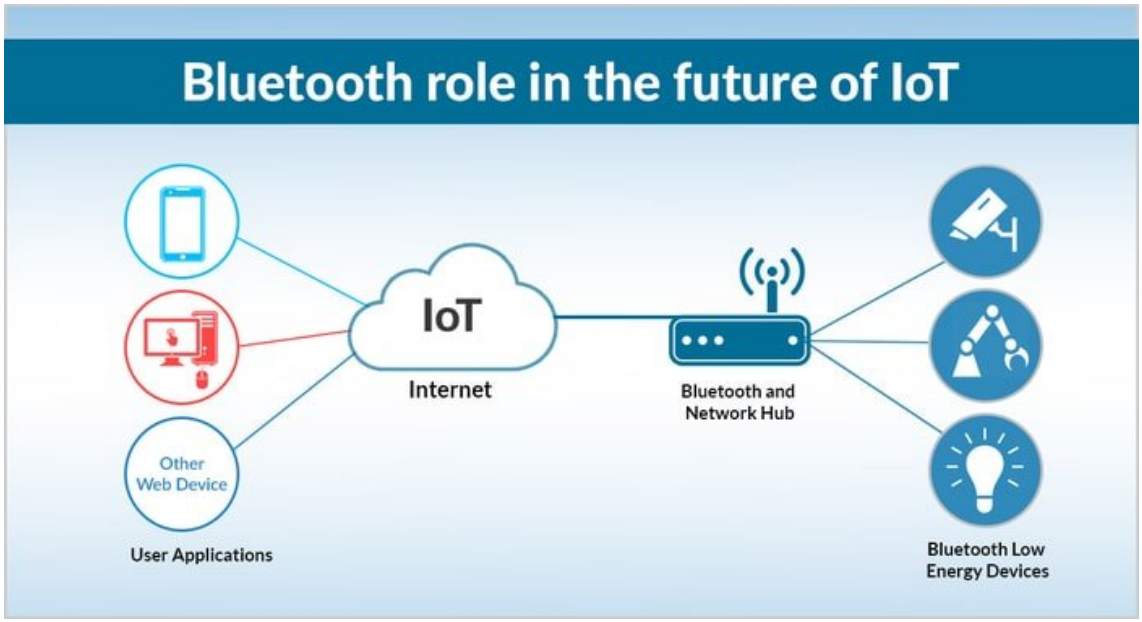


Figure 1. The role of Bluetooth in the future of IoT (Hasan 2020).

BLE operates perfectly with the small portions of data. Due to that attribute, Bluetooth is one of the leading protocols used by IoT devices in this current state. The newly invented Bluetooth Core 4.2 Specification permits Bluetooth Smart Sensor to connect the internet straight via 6LoAPAN which is allowing for the smallest devices with limited processing the ability to transmit information wirelessly through the Internet protocol. 6LoWAPN can communicate with 802.15.4 devices as well as other types of devices on an IP network link. Version 5.0 is completely developed and optimized for IoT which adds an innovative Internet Protocol Support Profile (Woolley 2019, 5).

2.3.2 WiFi

Among IoT devices, WiFi is a widely used protocol for communication (Figure 2). Offering fast data transfer along with the aptitude to handle huge amounts of data. According to many electronic device designers and a wide range of infrastructure, WiFi has become an essential part of modern life. The communicational range between two devices using WiFi is approximately 50 meters, much higher than Bluetooth technology (Mitchell 2019, 1).

Figure 2. WiFi, common usage (Hasan 2020).

In 1997, the first version of WiFi based on the IEEE 802.11 family of standard (Mitchell 2020, 1) was released. The first version came with the capability of delivering up to 2Mbits/s link speed. At present, the most common standard of WiFi is 802.11n, but the latest version that provides even faster communication is 802.11ac Although WiFi consumes excessive power for some of the IoT applications, WiFi is still the most powerful protocol for file transfer among most IoT devices (Taylor 2019, 2).

2.3.3 ZigBee

ZigBee is designed to operate at the 2.4 GHz frequency and the fixed data-rate of 250 Kbit/s. Low power consumption, high scalability, security, and durability along with the high node count are ideal for communication between IoT devices. ZigBee can use 128-bit AES encryption, while the range can be up to 200 meters with the maximum number of nodes being 65536 (Farahani 2008, 265). ZigBee is the most powerful, low-cost, low-power wireless mesh for networks that operate over longer ranges (Figure 3).

Figure 3. ZigBee, Smart Future (Hasan 2020).

The ZigBee specification is based on the IEEE 802.15.4 standard like 6LoWPAN, but it cannot communicate with other protocols easily. The greatest advantage of ZigBee is that it can drastically extend battery life as the nodes can remain in sleep mode most of the time. The data in a ZigBee network is ”hopping” around a mesh of transceivers until it reaches the host. The ZigBee protocol is suitable for use in home automation and security system in large industrial sites where low power is required (Taylor 2019, 3).

2.3.4 Z-Wave

Like ZigBee, Z-Wave is a protocol that is designed for home automation and electronic devices with lower-power radio frequency communication (Figure 4). The Z-Wave’s radio

frequency is 800-900 MHz and the range is between 30 to100 meters, and the data-rate ranges approximately from 40 kbps to 100 kbps (Taylor 2019, 4).

Figure 4. Z-Wave infrastructure.

In fact, on the mesh network Z-Wave can use up to 232 nodes which is a small number compared to ZigBee's nodes. However, Z-Wave is still adequate enough for smart home automation. At CES 2018, the latest version 700 series of Z-Wave was launched which can broads a range of 100 meters from point-to-point contact and operates at lower-power. In most sensors, Z-Wave is widely used for temperature, motion, door/windows and the battery with a single coin cell can last for 10 years (Knight 2018, 1).

2.3.5 CoAP

CoAP stands for the Constrained Application Protocol which is a specialized web transfer protocol for use with constrained nodes and constrained networks in the IoT system. CoAP is primarily designed for machine-to-machine, restricted smart devices, internet productivity, and utility protocol. CoAP is ideally used among devices that have an identical restricted community. This includes general nodes and devices on the internet and different restrained network and devices that joined on the internet. (Shelby 2014, 1)

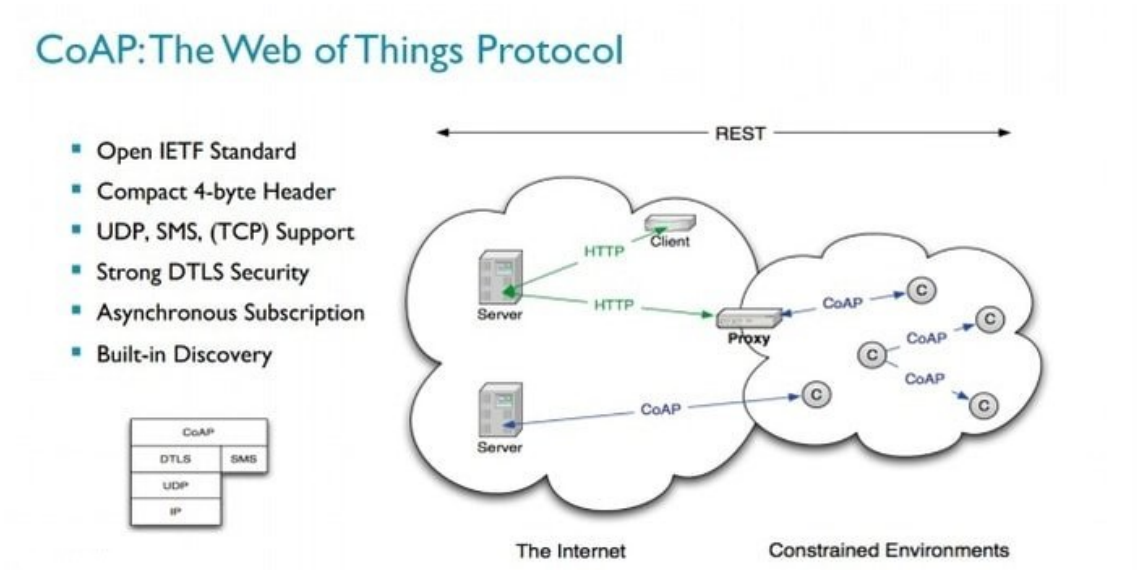


Figure 5. CoAP infrastructure (Hasan 2020).

The CoAP protocol can be used by IoT systems based on the HTTP protocols. It uses the UDP protocol for lightweight data implementation. The REST model is the base of CoAP, just like HTTP, CoAP helps in eliminating the ambiguity of the HTTP methods such as GET, PUT, POST, DELETE. It is also used inside mobiles as well as other social networks. (Hasan 2020)

2.3.6 Multicast DNS

The Multicast Domain Name System (Cheshire 2013, 1) is a DNS discovery protocol for resolving local network hostnames at IP addresses without the use of the DNS unicast server as well as in the network without any other infrastructure. This protocol uses UDP (as a transport layer protocol on port 5353) packets with IP multicast (Ipv4 224.0.0.251), in which a node on the local network tests the name of all other nodes. The client node sends a query message to respond with a different named node. A multi-cast response message with an IP address will be sent to the node when the node with the correct name receives the query. As a multi-cast response, the address and name of the target device are also stored in the local caches by all devices (nodes) of the network, thus it is possible to identify the device uniquely and reliably within the local IoT network. (Cheshire 2013, 33)

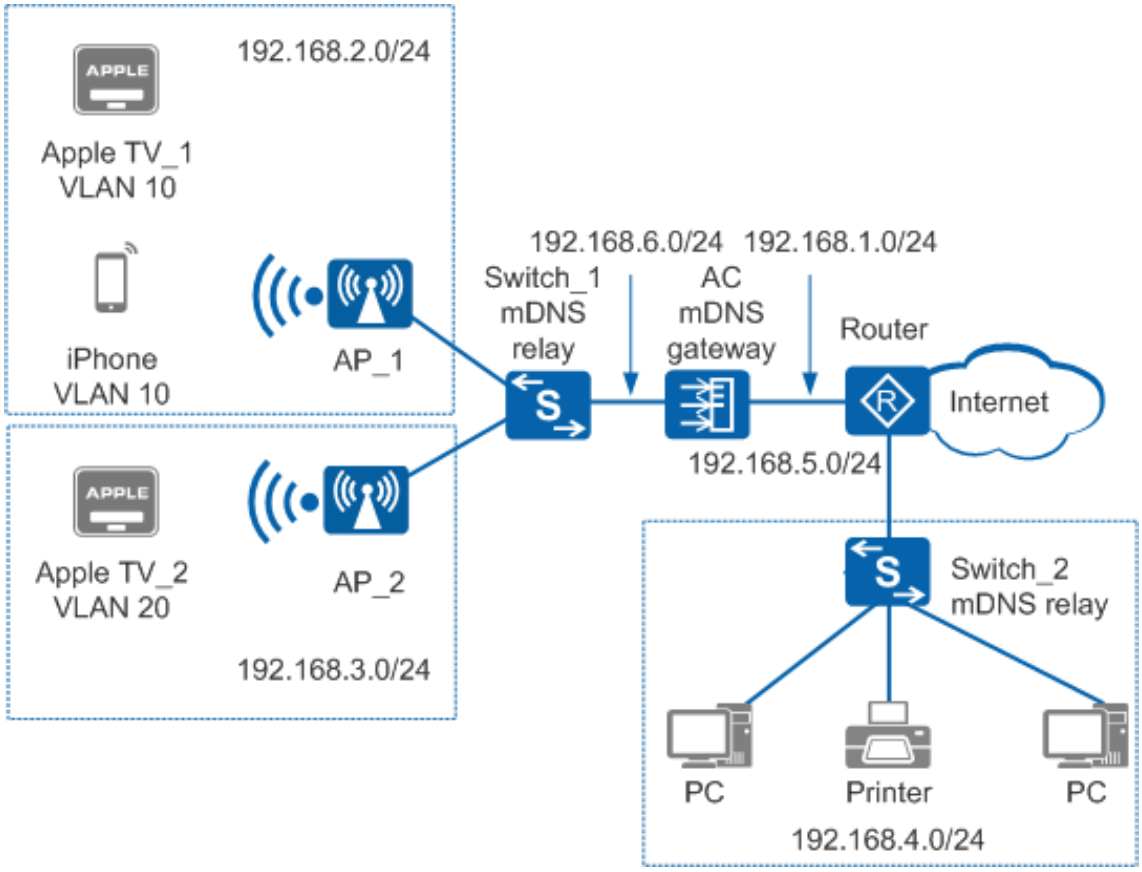


Figure 6. mDNS, application scenarios (Huawei 2020, 1).

2.3.7 SSDP

SSDP (Simple Service Discovery Protocol) is a discovery protocol used to determine what services are available on a network. It is defined as part of the UPnP spec. SSDP is a zero-configuration networking protocol designed to allow nodes to be added and removed from a network without any involvement from a central service such as DNS or by assigning static IP addresses to specific nodes. This decentralized, dynamic approach is possible because SSDP uses UDP as its underlying transportation protocol which allows for multicast communication (Majkowski 2017, 3).

Multicasting allows a node to transmit one message onto the network and for that message to be forwarded on to all interested nodes on the network without the sender node having to know what other network nodes are available (forwarding happens at the IP routing level). SSDP takes advantage of this forwarding functionality to allow any node to ask other nodes if they support a particular service, or conversely for a node that offers services to tell other nodes about those services (Majkowski 2017, 3).

2.4 Applying IoT into Enterprise

The Internet of Things (IoT) is a strong and one of Industry 4.0's core elements. However, there were few and far differences between actual implementation in the enterprise. IoT devices should seamlessly collect information, allowing faster and better decision-making, when the technology is fully adopted. IoT devices drive companies' automation initiatives which then optimizes performance, reduces waste, and maximizes productivity.

With billions of devices connected every day, leaders in the industry use IoT to put individuals and machines together and pursue new concepts. And while IoT can still support market change at an evolving level. CEOs can experiment with smaller initiatives to examine the actual advantages of the Internet over traditional smartphones and computers in order to decide if the gains are genuine or not.

For example, in logistics from devices capable of handling, detecting, and tracking functions to achieve efficiencies and increase reaction times without human intervention. The same refers to the management of operations using IoT tools to make inventory more visible. Increased management and tracking of inventories are needed in industries such as retail, purchases, and product consumption is assessed in order to know when supply is low while stock growth is prevented. By 2025, the effect could range from 410 million dollars to 1,2 billion dollars. (Nawjin 2019)

2.4.1 Industrial preventative maintenance

In the field of preventive maintenance, IoT equipment is primarily commercial, one of the most robust applications. The application is very easy. By using IoT tools such as vibration and wear sensors companies calculate the tension and usage of industrial equipment. Such sensors collect useful data and communicate with the cloud endpoint or server that can be then processed through an AI system that compares historical data and preempts maintenance.

IoT technology will certainly minimize maintenance and downtime by maintaining equipment before critical times in this application (Tech Wire Asia 2019).

2.4.2 Fleet management and tracking

Another big IoT usage is fleet management, whereby IoT devices can communicate their location back to the central control of the organization through a mobile network, using the GPS locator. Many companies with many vehicles like auto rentals, trucks, and other suppliers that have to track the movements of their products make use of this application.

Much more accurate data such as travel speed, engine tempers, fuel level, battery standing, and thus preventive and predictive maintenance can be transmitted to certain cars with advanced sensors. In order to maximize the supply route, shipping firms may even control the freight load at any given time (Tech Wire Asia 2019).

2.4.3 Building management

Cases for IoT use are not restricted only to businesses of heavy equipment and large car fleets. Many businesses use the equipment for building maintenance purposes and are linked to a shared network of motion sensors, cameras, and other surveillance tools.

Instead of using the preset settings or random schedules the central console that gathers all the data automatically controls the temperature, the lighting, the elevators, and HVAC systems depending on the actual use and operation.

Adopting this intelligent strategy would be more environmentally friendly and would reduce the running costs of the business (Tech Wire Asia 2019).

2.4.4 Smart agriculture

Another sector that has adopted IoT is agriculture. Farmers are installing a wide variety of IoT tools on the field to pursue a smarter and more contemporary approach to agriculture. Precision navigation and monitoring devices have made it possible for farmers to perform precision farming, to maximize their harvests for optimum yield. In addition, the pH, moisture, and nutrient compositions may be calculated by soil sensors and transmitted to the computer farming industry, thereby supplying more detailed field knowledge (Tech Wire Asia 2019).

2.4.5 Healthcare system

The health sector continues to use IoT technology for computer interface applications as well as its functions as the IoT systems become more stable. Efforts are underway to incorporate medical equipment and software for more efficient data transfer that will enhance the precision of diagnostics, such as blood pressure sensors, MRI devices, and other health management services, into more sophisticated back-end systems.

In summarize, IoT infrastructure is now deployed in various industries and businesses that already enjoy the advantages of investing in IoT systems.

More efficient and secure networks will lead to a new age of networking that will only further revolutionize businesses with the explosion of IoT products (Tech Wire Asia 2019).

2.5 Secure Enterprise IoT

The implementation of these systems is one of the main problems for the system. 55 percent of respondents listed health as their first concern for the deployment of such technologies in a survey conducted by 451 Research in 2018. Organizations must achieve the correct degree of protection for these tools to secure data at all points of the life cycle of an endpoint. A business that is more and more connected ensures that no defense target can be ignored. Any of the main targets for attacks at work are printers and HVAC devices, all of which are wirelessly exploited by hackers to breach the networks of an organization and steal data (Lerner 2018).

Probably no industry has addressed risks from these sensors more to cybersecurity than the healthcare sector. In 2018, at the Black Hat security conference (Dameff and Radcliffe 2018, 1), researchers showed that hackers could quickly infiltrate heart tracking systems and install malware remotely. About every medical system uses patients' machine-to-machine capabilities, but other security flaws exist.

“Healthcare facilities face the challenge of weighing out the cost of replacing medical devices versus the possibility of potential cybersecurity threats, safety, and device effectiveness,” according to Rizwan Jan, Chief Information Security Officer for the Henry M. Jackson Foundation of Advancements In Military Medicine. “Mitigating information

security risks can be challenging as they require a contributing balance to protect the safety and security device development from both the manufacturer and health care facilities to manage the risks of devices." (Lerner 2018).

The fleet industry faces increased higher security with the growing use of IoT. According to Maerisk (a Logistics company) report, over $250 million in losses due to the computer virus attack that halted its port activities in many countries (Greenberg 2018, 1). The attack did not include any IoT technologies but highlights the dangers inherent with using automation over manual processes where hardware, including IoT apps, could be the starting point for cyber attacks on the company's network.

The lack of a protection and privacy system for IoT devices may have a significant effect. The lack of effective testing of IoT devices/systems to identify security flaws provides an easy target for hackers. The risk is that critical software that once ran in its secure environment is now linked to a wider network. The IoT network was formerly a separate operating infrastructure network, but now the system links this private network to the majority of the company's IT network – this may cause significant damage because sensitive, business-critical data is within reach.

For other company vulnerability models, the presence of the Internet of Things (IoT) apps in the homes of workers are ignored. Alert is definitely needed here, but your knowledge of the risks and safe intelligent devices can be enhanced calmly and assessed absolutely.

It has implications for privacy and protection. The future effect of all data production points in your technical environment is in everyone's best interest. Any of these devices could affect your digital connections' protection. It is important to comply with the following best IoT security practices, in order to reduce personal and corporate risk (Myers 2020).

- Inventory Smart Devices in the Enterprise Environment:
  - Listing every device in the network. After the device is mounted, it can be possible to forget that it is still there, so a detailed inspection is required.
  - Re-checking every IoT device which is paired with inspectional devices to make sure it works properly in the safety range. Check carefully which devices had been paired with personal devices.
- Identify Potential Risks to Personal and Enterprise Data:

- Looking up carefully the specifications of each IoT device, because it might have more features. Check software permissions thoroughly to see what the details need to keep updated, as there are might exist some security control flaws and need to keep an update from the manufactures.

- Mitigate Know IoT Security Risks:
  A lot of steps need to perform to improve Enterprise IoT security.
  - The first important thing is to strengthen the authentication of each device. Make sure to set strong and unique passwords (e.g. allows more than 16 characters, includes numeric, capital, and normal characters, special characters), if possible enable two-factor authentication (2FA).
  - Temporarily of permanently removing unneeded functionalities of the IoT devices to reduce their potential risks.
  - Set a restriction range and put separate smart devices in every range. It is helping to detect an intrusive attack and remedy the consequences of the attacks that had been taken.
- Minimize Data Output
  Data sharing will certainly reduce such risks on a global scale, but it is important to reconcile the advantages of sharing with possible risks. Sharing data from your health care or exercise facility can help with public health programs, but the choice of whether or not to participate in such projects will ultimately depend on the particular threat model.

2.6 Threat Modeling BLE and ZigBee

In preparation to develop and implement any type of intrusion detection system, it requires a solid understanding of the ecosystem and related threats. This means knowing the architecture, involving infrastructure, related connectivity, and the courses learned if compromised (Figure 7). By getting that knowledge will help an intrusion researcher realize which threats to be searching for, whether present or not, and choose the right placement of the intrusion detection sensors. The internet attacks can be observed with sensors between the placement and the IoT gateway.

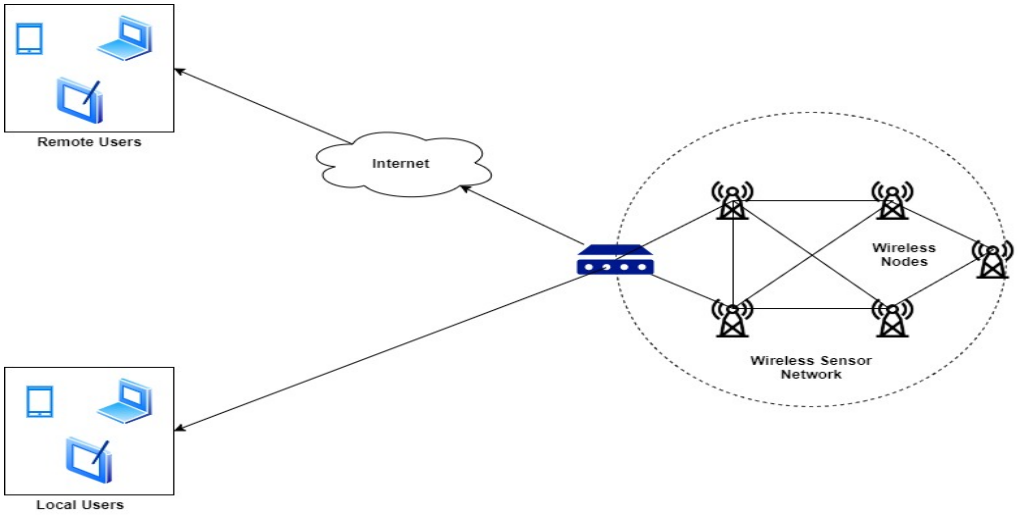


Figure 7. IoT Communication Architecture

The manufacturers decide whether to configure Bluetooth compatibility and discoverability choices with a Bluetooth protection setup. There are three types of protection standards of the different networking and exploration capabilities combined (Haattaja 2009, 55):

- Silent: The are no connections that will be accepted by the device. It simply monitors Bluetooth traffic.
- Private: Non-discoverable device in which the device cannot be discovered. Connections only are approved if the master is aware of the interface BD_ADDR. Typically, a 48-bit BD_ADDR is special and only extends to one individual Bluetooth device.
- Public: A discoverable device that can be both discovered and connected to.

2.6.1 Common Threats and Vulnerabilities

Bluetooth is becoming a popular use in enterprise IoT. Since it is a wireless communication system, so it is always possible to deliberately jam or intercept transmissions, or to pass false or modified information on the IoT devices. The device should maintain protection at many protocol levels in order to secure the system.

In evaluating Bluetooth vulnerabilities, it is very important to use the Bluetooth version and the reliability of communications between devices that is as strong as the weakest link. Because many older models tend to be used today, the flaw continues to be

persisted in newer Bluetooth versions. Based on the version, the attackers can exploit many techniques to take advantage and compromise. E.g, in the version before Bluetooth 1.2, the original devices could be eavesdropping and spoof by the malicious; version before Bluetooth 2.1, due to the short length of the PIN code, so it can be guessed by the attackers (Sensor and Actuator Network 2018, 8).

Following Figure 8, highlights and classifies Bluetooth-based threats throughout the Bluetooth Threat Taxonomy. The classification system can assist in determining the seriousness of threats, providing safety precaution methods, and reactionary strategies. Certain threats may have multiple classifications but are categorized according to their prevailing feature.

Classification	Method	Threats
Obfuscation	Techniques are used to hide the attack and prevent detection.	HCIConfig (Device Name)
		HCIConfig / BTClass (Class of Device)
		Bdaddr (Device Address)
		SpoofTooph
Surveillance	Device monitoring is done to collect information.	HCITool (Device Discovery)
		Sdptool (Service Discovery)
		Redfang
		Blueprinting
		Bt Audit
		War-Nibbling
		Bluefish
		BNAP BNAP / BlueProPro
		BlueScanner
Range Extension	Range of connectivity is extended so attacks can be conducted at a distance.	BlueSniping / Bluetooone
Sniffing	Sniffer is used to intercept data by capturing network traffic.	Merlin / FT4USB (External Based)
		BlueSniff (Frequency Based)
		HCIDump (Host Based)
Man-In-The-Middle	Attackers trick devices into thinking they are paired, when in reality they are both connected to the attacker.	Bthidproxy
Unauthorized Direct Data Access	Data stored in cloud is directly accessed due to vulnerabilities.	Bluesnarf / Blooover
		BTCrack / Btpincrack
		Car Whisperer
		HeloMoto
		Bluebugger
		HID Attack
		Btaptap
Denial of Service	Services are disrupted, making a machine or network unavaiable to users.	BlueSmack / Tanya
		Blueper
		BlueJacking / BlueSpam / Smurf
		vCardBlaster
		Signal Jamming
		BlueSYN / Pingblender (Multi-Vector DoS)
		Battery Exhaustion
Malware	Intrusive or harmful software is put on a computer to disrupt operations, steal data, or extort a target for ransom.	BlueBag
		Caribe
		CommWarrior
		Skuller
Fuzzer	Injects data into a stack or program and has the ability to detect bugs.	Bluetooth Stack Smasher / BluePAss
		BlueStab
		HCIDump Crash
		L2CAP Header Overflow
		Nokia N70 L2CAP DoS
		Sonyericson Reset Display

Figure 8. Bluetooth Threat Taxonomy. (Sensor and Actuator Network 2018, 9)

The pairing process is a significant contributor to Bluetooth security issues. The process can be compromised in different stages both before and after devices are connected. The followings are some of the most common attacks against IoT devices (Sensor and Actuator Network 2018, 9 - 15):

- MAC Spoofing Attack

  The attack can be carried out prior to encryption and when linking keys are generated during piconet creation. Devices can authenticate by generating connection keys for each other. The attackers can copy another use during the attack. By using special tools, the attackers can terminate the connections or intercept/alter data.

  A piconet is an Adhoc network linking a wireless group of devices by using Bluetooth technologies protocols. A piconet might be consist of two or more devices on the same physical channel. It enables a Master device to connect up to 7 active slave devices. (Barry and Crowley 2012)
- PIN Crack Attack

  The attack can be performed during device pairing and authentication. The attackers can collect the RAND and the BB_ADDR of the targeted device by using a frequency sniffer tool. The brute-force algorithm is used to test the information collected until the correct PIN is found.
- Man-in-the-Middle Attack

  The attack occurs during the pairing process. Messages are unintentionally relayed between the devices during the attack. It allows authentication without the shared secret keys. The user believes that the pairing process has been finished during a successful attack, but that does not happen because the two devices are paired with the attacker.
- BlueJacking Attack

  The attack can submit unsolicited messages to a device during a BlueJacking attack to trick the user to a secret of the access code. It allows the adversary to explore the data on the targeted device. The attack can be performed in the short range of 10 meters between the devices involved and the exact source of the message received. Although data are not usually altered, devices could be vulnerable to other attacks.
- BlueBorne Attack

  A stack overflow fault is used for the attack. The attacker is able to hijack Bluetooth links by exploiting the collection of pending network L2PCAP setup

replies. This allows the attacker to control the integrated content and function of the targeted device (Seri and Vishnepolsky 2017, 5).

- Fuzzing Attack
  The attack takes place by transmitting malformed data packets and non-standard data to the Bluetooth radio of the device, it causes a device to does inappropriate behavior. By watching the reaction of the device to the received data packets, the attacker could identify a vulnerability in the protocol stack if the device tends to stop or sluggish during the attack.

2.6.2 Threat Modeling

Threat modeling is an effective way of identifying risks from a technical perspective. The implemented process might involve many phases (Figure 9) to understand the architecture of the network which recognizes potential threats subsequently (Microsoft Azure 2017).

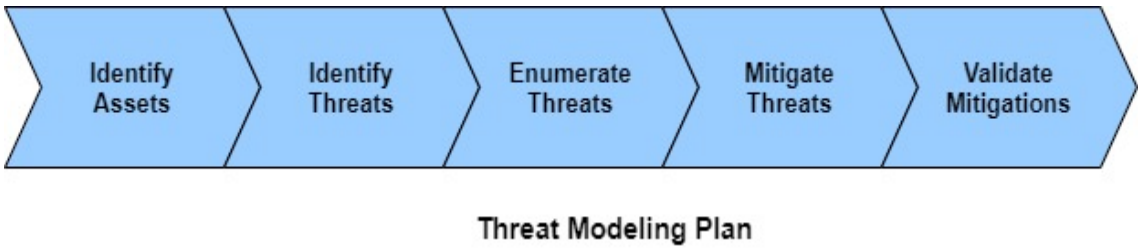


Figure 9. Threat Modeling Plan.

- Identify Assets:
  Identify assets is the first important phase in Threat Modeling. By identifying the correct type of assets can help the enterprise easily to manage, control, and integrate systems efficiently. There various types of IoT devices, based on the purpose of each system, the enterprise can choose the right type for specific requirements. For example, for a location tracking system, the IoT devices have a duty to collect all GPS information and return it to the server.
- Identify Threats
  Threat identification is a key element of the intrusion system. Identifying threats enable the preventive actions of the organization. Classifying and categorizing the threats give important information to prevent unauthorized users and prevent system breaches.

Once the assets have been identified, each device can be measured for threat using the STRIDE model which was developed by Microsoft. The STRIDE is an acronym that stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges.

The STRIDE model (Shostack 2007):

- Spoofing: The identification and authentication of users are the keys to most safety systems. Spoofing threats involve using other user credentials without their knowledge. The target is a device that has a weak authentication mechanism.
- Tampering: The systems or data can only modify by authorized users. If an attacker is able to control, it will bring crucial consequences on the usage or purpose of the system.
- Repudiation: The attacker always tries to repudiate their actions to hide their malicious activities, to avoid being detected or blocked.
- Information Disclosure: The aim of the attackers is to gain access to the confidential information of the system.
- Denial of Service: Attackers will have a certain interest in preventing regular users from accessing the system.

Elevation of Privilege: The attacker tries to gain additional privileges by spoofing a user with high privileges, or by tampering a system by modifying its privileges.

- Enumerate Threats

  Once the threats had been identified, the next phase is classifying, and categorizing the threats into different catalogs depends on the types of threats or what will affecting the system. Enumerating threats helps the intrusion researchers have a bright vision to develop and implement an efficient intrusion system that addresses directly those threats.

- Mitigate Threats

  During this phase, the intrusion researchers should do the correct actions, preventions to secure the system, and minimize the effect of threats. The goals of the mitigation threats must be set in order to evaluate and validate.

  Base on the STRIDE model, there are several steps that can be taken in this phase:

  - Spoofing threats: Every device within the system must be assigned the identity and authenticate by using Transport Layer Security (TLS), IPSec, and pre-shared key (PSK) on those devices. The Field gateway to the Cloud must

be authenticated by using strong mechanisms such as Cert-based or Claim-based.

- Tampering, Repudiation, Information Disclosure, and Denial of Service threats: The trusted platform module (TPM) is used as the most effective mitigation. TPM enables to store the keys in special on-chip circuits from which the keys can be used only for encryption operations, and can not be read or disclosure.

Elevation of Privileges threats: Applying the Authentication scheme to control the device.

- Validate Mitigations

  Mitigation goals tend to involve broad policy and vision declarations that explain what the mitigation strategy is to achieve. The goals present the aims the organization to achieve through the implementation of a mitigation plan and must be directly related to vulnerabilities in the risk assessment. The goals must be addressed the vulnerabilities of the IoT devices, as well as the potential threats that have been identified in the risk assessment.

  Validation must be taken continuously, for every phase in the threat modeling plan in order to discover any error and correct it in time

3 BLUETOOTH ASSET INVENTORY

3.1 Passive Solution

During the two first decades of 21st century, Bluetooth Low Energy has been built as one of the most common protocols for communication between smart devices with low power and short-range. Since the Internet of Things is becoming increasingly popular, there are even more reasons for learning how it operates from the beginning. BLE sniffing is basically a way of analyzing packets sent from master and client, this is important for detecting critical errors, finding performance bottlenecks, or interest protocol for the reverse engineer.

Sniffing Bluetooth packets is possible by using a Bluetooth antenna/dongle and specific Blue Hydra (Pwnie Express 2017). Blue Hydra is an open-source software from Pwnie Express which is used for tracking the presence of traditional Bluetooth, BLE devices, and BLE "iBeacon" proximity sensors for security professionals. However, it can also provide an alert on the presence of particular devices by connecting to other resources. BLE devices use MAC addresses and the universally unique identifier (UUID) to advertise to each other device. By specific UUID to the BLE devices, the devices can be tracked and get the distance by using the Received Signal Strength Indication (RSSI). The RSSI will be used to produce movement data about the people who carry those devices and to search for devices that are not meant to exist.

It is also possible to have specific hardware to enhance the ability to discover BT devices by using Ubertooh One (Github 2017). The Ubertooth project has three main components:

- Hardware: Ubertooth One's hardware architecture is fairly stable, can be built or bought from the owner's project site.
- Firmware: This require the bluetooth_rxtx software is running on the Ubertooth One ARM processor. The firmware is quite stable for now but also possibly to enhance more in the future.
- Host code: The control manager computer which is connected to Ubertooth One via USB will run this software. The software is available on the project site.

Ubertooth performs based on the operation of Bluetooth that is hopping through frequencies within a specific range. Once the Bluetooth packets are captured, it starts with a Bluetooth Device Address (BD_ADDR) from the Lower Address Part (LAP). Like the Ethernet device's MAC address, the BD_ADDR is a 48 bits MAC address. The LAP consists of the lower 24 bits of the BD_ADDR which is transmitted with every packet (Doss, Piramuthu and Zhou 2015, 75).

3.1.1 Sequentially allocated addresses

Even if the connection is encrypted, the packet header is plaintext and the BDADDRs can be derived. If the device does not generate Bluetooth traffic and is only listening, it is still possible to "guess" the BDADDR, by sniffing its WiFi traffic due to the sequential MAC and BD_ADDR assignment.

"This is possible since WiFi MAC addresses appear unencrypted over the air and because of the commonly agreed standard among OEMs and hardware manufacturers that the MACs of internal Bluetooth/WiFi adapters are either the same or vary even in the last digit (one being +1 of the other)." (Seri and Vishnepolky 2017, 6).

BD_ADDR values can be identified by MAC addresses of chosen Wi-Fi clients. By incrementing or decrementing the MAC address by the value of one, the former can infer the MAC and BD_ADDR values due to the sequentially allocated for the case of certain Apple, Windows, and Samsung devices. The derived BD_ADDR is subsequently validated if the response is received to a targeted scan.

Unfortunately, the technique can be prone to false positives and false negatives as a sequential address assignment is only used for specific device types. By testing on several devices, this method only returns the true value for Apple, Windows, and Samsung devices (Figure 10 - 11).

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8260
   Physical Address. . . . . . . . . : 28-16-AD-06-6D-B4
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::8416:12c:2d49:7df4%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.106(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, May 20, 2020 11:17:25 AM
   Lease Expires . . . . . . . . . . : Monday, May 25, 2020 11:36:33 PM
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 86513325
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-7F-F8-1A-D4-81-D7-80-95-7B
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 28-16-AD-06-6D-B8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

Figure 10. The sequentially allocated Addresses on Windows 10 machine.

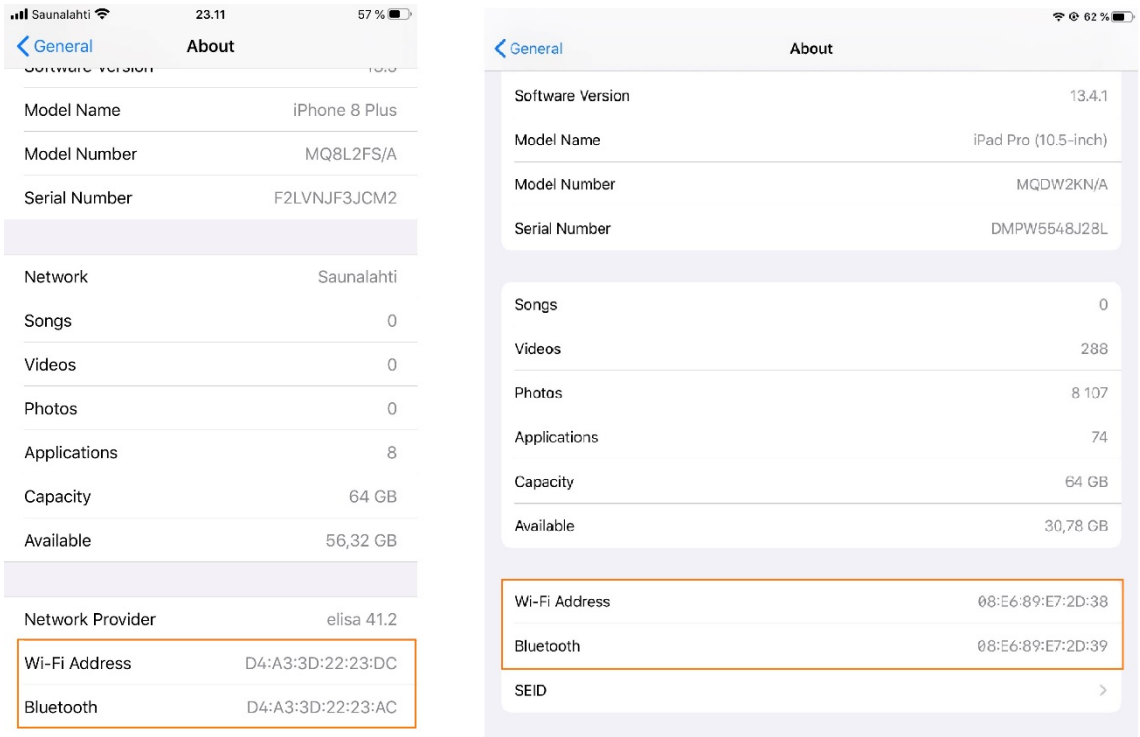


Figure 11. The sequentially allocated Addresses on Apple devices.

3.2 Active Solution

The ICS system consists of multiple network sensors that have the ability to collect the live network traffic in the network system and return it to the server for analyzing and monitoring. The thesis chooses Cisco Meraki and Aruba as a sensor and implements the active queries for collecting the live network traffic in the network. In industry 4.0, Cisco Meraki and Aruba are using widely to manage, control, and monitor BLE and ZigBee.

3.2.1 Cisco Meraki MR30H

Cloud technology is currently playing a critical role in the network industry. Meraki MR30H Wireless Access Point is one of the most commonly deployed access point tools delivering cloud-managed WLAN services. Meraki MR30H is designed for complex corporate environments, including integrated 802.11ac and 802.11n systems, including MIMO (Multiple-Input-Multiple-Output), beam shaping, and channel bonding, to provide the performance and robust coverage needed by demanding business applications (Cisco Meraki MR30H 2020).

3.2.1.a Specifications

The Meraki MR30H is a wireless access point that provides cloud-managed WLAN access points. Designed for challenging enterprise environments, the MR access points use advanced 802.11ac and 802.11n technologies including MIMO (Multiple-Input-Multiple-Output), beamforming, and channel bonding to deliver the throughput and reliable coverage required by demanding business applications. This AP has various features that could help the business site to manage, maintain, and integrate in a convenient way.

- Hardware features (Cisco Meraki MR30H 2020):
    - Integrated 4 port gigabit switch.
    - 3 radios band: 2.4 GHz, 5.0 GHz, and Dual-Band WIDS/WIPS.
    - Integrated Bluetooth BLE radio: 2x2 MU-MIMO 802.11ac Wave 2.
    - Up to 1.3 Gbps aggregate dual-band frame rate.

    - 802.3af PoE compatible.
- Cloud management:
    - Network-wide visibility and control. Self-provisioning for rapid deployment.
    - Provides REST API services to deploy on its own server.
- Enterprise Security:
    - 802.1X Integration.
    - Air Marshal: real-time WIPS with forensics.
    - Stateful Layer 3-7 firewall.
    - Built-in antivirus scan (NAC).
- Radio Frequency Optimization:
    - Dual-concurrent, 2-stream MIMO radios.
    - Radio optimize for rate and rang performance.
    - Third radio dedicated to security and RF management.
    - Built-in real-time RF spectrum view.
    - Cloud-based automatic RF optimization.
- Layer 7 traffic shaping
    - Classify hundred of applications.
    - Create per-application bandwidth limits.
    - Prioritize productivity apps.
    - Restrict recreational traffic.
- Location Analysis:
    - Measure visitor capture rate, visit length, and repeat visit rate.
    - Measure visitor trends over time and compare performance across locations.
    - Enable location services through integrated iBeacon functionality.

3.2.1.b Meraki Cloud API

The Meraki Dashboard API is a web framework that enables you to communicate directly with the Meraki cloud network and the Meraki managed tools. The API provides a series of tools known as endpoints for developing apps and applications that interact with the Meraki Dashboard for use in situations such as provisioning, bulk configuration updates, reporting, and role-based access controls. The Dashboard API is a modern RESTful API service that uses HTTPS requests to the URL and JSON as a human-readable format.

There are many purposes for using the Meraki Dashboard API, for examples (Cisco Meraki 2020):

- Manage organizations, admins, networks, VLANs, SSIDs.
- Building an automation script that can process thousands of new sites in just one click.
- Build a new server based on the specific needed of each business site.
- Control, manage, and provision of BLE devices.

Cisco Meraki supports multiple tech stacks to help end-users easy to deal with daily needed use such as RESTful framework, Ruby, Node.js, and Python. For each stack, Cisco provides specific documents for use.

Before getting started to use Meraki Cloud Dashboard API, there are some configurations that need to perform:

- Register Cisco Meraki account for adding devices, creating the networks.
- Add devices and update license, create the network, set up a placement where is the Access Point located.

Generate the API key for deployment purposes. The API is the unique key that allows users to communicate with the Cloud and retrieve useful information.

3.2.2 Aruba 303P

Aruba 303 Series 802.11ac Wave 2 Campus Access Points provide high-performance 802.11ac with MU-MIMO (Wave 2) for medium density enterprise environments. Aruba 303 Series supports the integration of Bluetooth radio, Bluetooth Low Energy (BLE), and 802.3af technology as well as the integration of Zigbee radio for IoT networking, which enables the enterprise to enhance workflow efficiency and productivity with the lowest TCO. (Aruba 2020, 1)

The integrated BLE radio can be used as an Aruba beacon for advanced locationing, indoor wayfinding, asset tracking, and to enable proximity-based push notification services. The integrated beacon radio also enables the remote management of battery-powered and other standalone beacons in a large-scale network of Aruba beacons. It allows the enterprise to leverage connectivity background and create apps that will offer

an improved customer interface and improve the utility of the wireless network for enterprises.

Key features: (Aruba 2020, 2)

- “IoT Platform Capabilities: Aruba 303P includes an integrated Bluetooth 5 and 802.15.4 radio (for Zigbee support) to simplify deploying and managing Meridian and IoT-based location services, asset tracking services, security solutions, and IoT sensors. This allows organizations to leverage the AP as an IoT platform which eliminates the need for an overlay infrastructure and additional IT resources.
- Unified Access Point: deploy without controller either controller-based (ArubaOS) or controller-less (InstantOS) deployment mode.
- Dual Radio 2x2 802.11ac access point with Multi-User MIMO (wave 2).
- Built-in Bluetooth Low Energy Radio which enables location services and asset tracking services.
- Advanced Cellular Coexistence (ACC): minimizes interference from 3G/4G cellular networks, distributed antenna systems, and commercial small cell/femtocell equipment.
- Aruba AppRF technology leverages deep packet inspectors to classify and block, prioritize or limit bandwidth for over 2,500 enterprise apps or groups of apps.
- Radio Frequency management.
- Spectrum Analysis.
- Aruba Secure Core: Device assurance, Integrated wireless intrusion protection, IP reputation, and security services identity.”

For Bluetooth Asset Inventory, Aruba 303P provides various methods to perform: Aruba User Interface (UI), Aruba CommandLine Interface (CLI), Aruba Central Cloud.

3.2.2.a Aruba User Interface

Instant virtualizes Aruba Connectivity Controller functionality on 802.1 compliant access points providing a feature-rich enterprise-grade WLAN that combines flexibility and setup usability. Instant is a simple, easy to deploy turnkey WLAN solution consisting of one or

more instant Access Points. An Ethernet port with routable connectivity to the internet or a self-enclosed network is used for deploying an Instant Wireless Network. An Instant AP may be mounted at a single site or distributed through several geographically scattered sites. Designed primarily for quick delivery and efficient control of networks.

The Instant User Interface a simple web-based GUI which is designed to deliver ease-of-use that helps the users easily to configure, manage and control all the useful information such as BLE devices, Wi-Fi networks from a central location. The Instant UI can be launched by Microsoft Internet Explorer 10 or later, Apple Safari 6.0 or later, Google Chrome 23 or later, and Mozilla Firefox 17 or later through a remote management console or workstation (Figure 12).

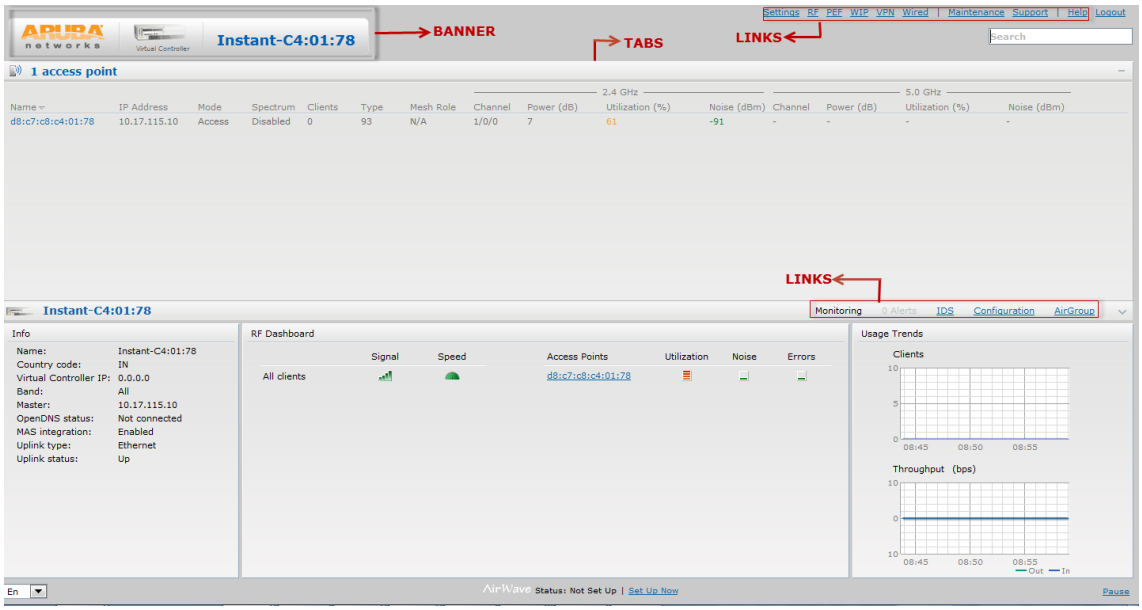


Figure 12. Aruba Instant User Interface (Arubanetwork 2020, 36).

Once, the IAP is set up to the network, the users can connect to the UI following the IAP's IP address. The username and password were provided by default by the manufacturer. The dashboard page looks easy to use with the navigated links and buttons. On the Dashboard page, the network status and the AP information shows all as well.

Aruba provides a huge amount of commands to perform, this task only focusing on getting the information about BLE devices which is used BLE scanning functionality to perform. It scans for nearby devices through BLE and displays the information on the webpage about BLE devices for Bluetooth Asset Inventory purposes.

3.2.2.b Aruba CommandLine Interface

The Instant CommandLine Interface (CLI) is a text-based interface for scripting purposes enabled instantly. The CLI is accessible through a Secure Shell (SSH) session or the serial port. SSH session requires to enable Telnet access on the IAP, configure an IP address, and a default gateway on the IAP, and connect the IAP to the network. This typically performs when the Instant network on an IAP is set up.

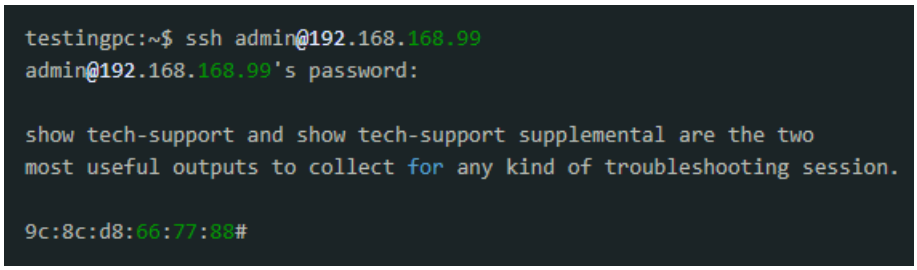


Figure 13. Aruba CommandLine Interface.

The systems display its hostname and the login prompt when connected to a CLI session. Use the default credentials provided by the manufacture to login. Once the authentication is checked, it activates the privileged mode and displays the command prompt. The users can perform various commands to show, clear, ping, traceroute, and commit commands.

Aruba 303P supports built-in Aruba BLE for tracking and proximity detection. The BLE Beacon Management Console (BMC) feature allows the users to configure parameters for managing the BLE beacons and establishing secure communication with the BMC.

3.2.2.c Aruba Central Cloud

Aruba offers the Cloud solution to facilitate the deployment, management, and optimization of WLAN, LAN, VPN, and SD-WAN. The cloud is called Aruba Central Cloud which uses integrated AI-based machine learning, IoT protection analysis, and streamlined control of technology to improve conventional management for the intelligent edge today.

Aruba Central Cloud comes with tons of features that help the enterprise control, manage, and analyze networks, BLE information easily (Aruba Central 2020).

- Streamlined Network Operations:
  - Provides the united interface for quick and easy to manage, analyze, and maintain the networks.
  - With an easy-to-set-up guide and optimized installation devices that help to simplify the IT operations.
- Unified Infrastructure Management:
  - Provides a global or site view and comprehensive visibility for all managed devices from the dashboard.
- Advanced AIOps:
  - Provides real-time visibility and alert in the network reply on AI-based connectivity insight.
  - Deliver the right context at the right time.
- Reporting and In-depth Troubleshooting: Enables the development of detailed reports covering access, network performance, and user accounts.
- SD-WAN Orchestration and Management:
  - Integrated topology views for interactive portal and site information.
  - Provides performance score for WAN circuit health, bandwidth availability, and tunnel status.
  - Public cloud-hosted gateways extend policies directly by Virtual Gateway Management.
  - Provides VPN services.
  - Threat Defense with IPS/IDS.
- Automated Mobile and IoT Device Security:
  - Using AI/ML-based profiling to display information gathered from Aruba ClearPass Device Insight directly.
  - Generate behavior profiles for the devices connected to the network.
- Cloud Security and Reliability:
  - Capability for a large amount of data with Cloud responsive performance.
  - Offers service redundancy for connecting to data centers from multiple locations.
  - Provides the highest protection level with HTTPS connectivity based on a certificate.

4 IMPLEMENTATION

4.1 Implement BLE asset discovery on a ICS

By implementing the asset inventory on an ICS will help the organization have a better vision for efficiently developing the intrusion system. This is an important phase to identify assets in the threat modeling system. The asset inventory enables the ability that allows the enterprise to extend a commercial IDS Patrol module on an ICS.

4.1.1 SilentDefense

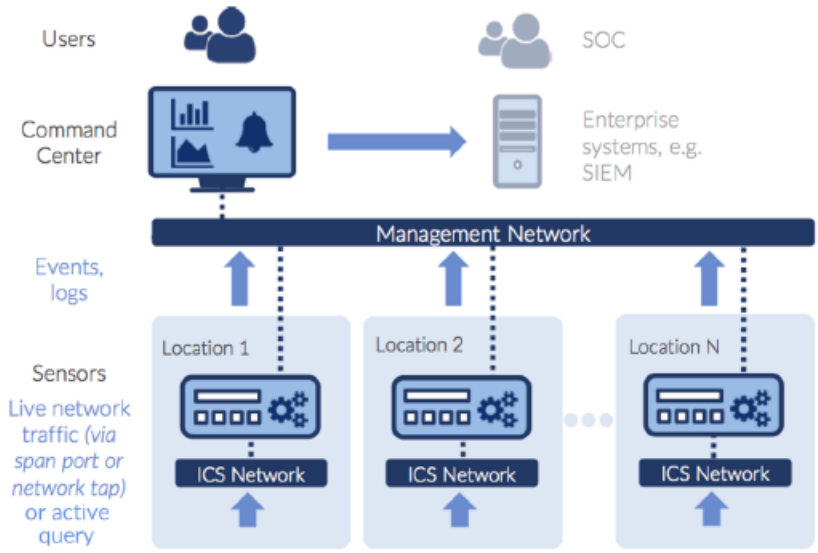


Figure 14. SilentDefense Architecture (SilentDefense 2020).

"SilentDefense is a non-intrusive network monitoring and situational awareness platform that provides in-depth visibility and cyber resilience for the industrial control system (ICS) and SCADA networks. SilenDefense protects the ICS/SCADA network from a wide range of threats. It combines patented anomaly detection and deep packet inspection (DPI) with a library of over 2,400+ ICS-specific behavioral checks." (SilentDefense 2020)

"SilentDefense architecture includes Monitoring Sensors, ICS Patrol Sensors, and Command Center:

- Monitoring Sensors are the standard, passive type of Sensor. In general, each sensor has at least four network interfaces for monitoring and a management interface. A monitoring sensor is connected to the ICS/SCADA network via a span/mirroring port to passively listen to the network traffic, then sends events and log information to the Command Center via the management network.
- ICS Patrol Sensors are an optional type of Sensor that allows for controlled, active queries by which the user can retrieve data from assets that cannot be detected passively. An ICS Patrol sensor is connected to the network via a management interface, to enable it to send the queries to retrieve data from network assets.
- The Command Center is a web application used for sensor and event management, it also provides the visual analytics dashboard and the network map. The Command Center can interface with several third-party enterprise, e.g., a SIEM system." (SilentDefense 2020)

SilentDefense has various advantages features:

- Asset Inventory and Network Map
- Network and Process Monitoring
- SDK for Advanced Customizations
- Logging & Investigation
- Threat Hunting Framework
- Dashboard and Reporting

SilentDefense supports a wide range of Protocols from IT to OT (with various vendors). For example: BACnet, CC-Link (Field, FieldBasic, Control), CNCP (ABB), CSP (Rockwell/AB), Citect (Schneider Electric), SRTP (GE), etc...

SilentDefense is widely used in Industrial Control Systems such as the Energy sector, Water & Wastewater sector, Manufacturing sector... SilentDefense can deploy within the main control center for monitoring all remote connections, even from a single location, from devices behind the Remote Terminal Unit (RTU) to monitor incoming and outcoming connections as well as local traffics (SilentDefense 2020).

4.1.2 Meraki Bluetooth HLI – Prototype with Lua programming language

Implementing a prototype not only gives a quick understanding of the capability of the access point but also to provides Bluetooth visibility. The SilentDefense Framework and Lua programming language is used to implement the SilentDefense Script that does an active query to the Meraki Cloud and collect Bluetooth devices over the Meraki Cloud API.

Lua is a high level, dynamically type-checked language. Lua is a lightweight embeddable language for scripting. Lua has the ability to read, use, and embed in all kinds of applications such as games, web apps... in a strong and fast way (Lua.org 2020).

The script does the queries in a fixed-interval time:

- Cronjob “do_once”: to get an IP address and added as a nested host (Meraki Cloud IP address).
- Cronjob “do_periodically”: retrieve all the Bluetooth devices and added to the nested host at a given period.

The SD script requires a valid Meraki API key in order to perform the query and the base URL of the Meraki Cloud. The Meraki cloud will check whether the key valid or not, if valid it will return the corresponding information based on the query.

4.1.3 Implement ICS Patrol module

Implement a Meraki module within the ICS Patrol to provide better Bluetooth visibility. In addition to improved visibility, and even advanced proactive capabilities, such as vulnerability detection and compliance inspection, SecurityMetters has developed the ICS Patrol. ICS Patrol extends SilentDefense’s capabilities to search for certain hosts in the ICS network securely, selectively, and actively. ICS Patrol includes Selective Scanning to help better identifying and dissecting assets information, files, vulnerabilities, compliance violations, and threats by using targeted, non-intrusive network communications (Figure 15).

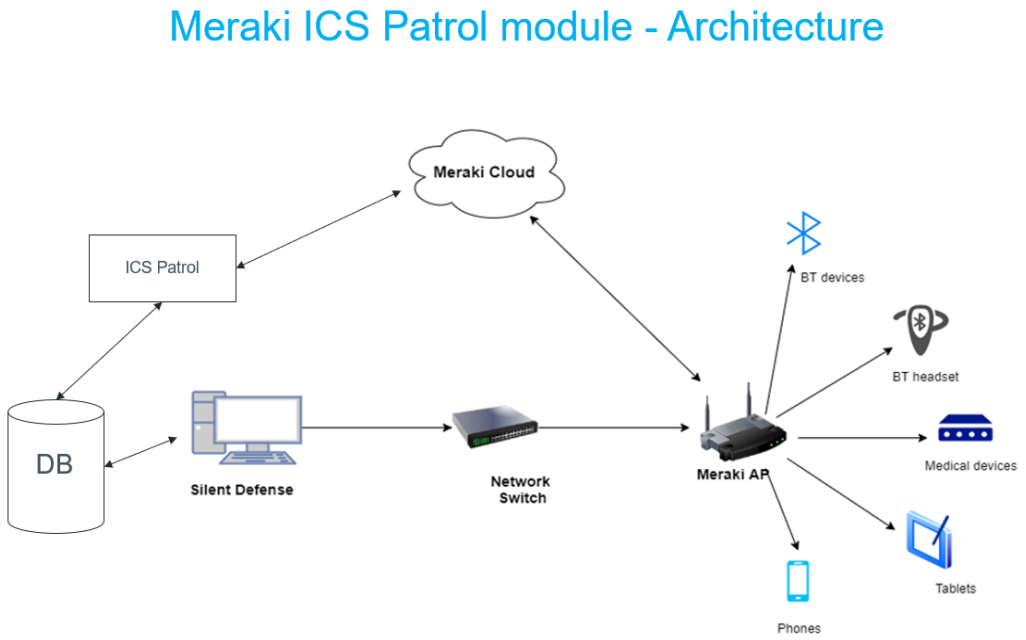


Figure 15. Meraki ICS Patrol Architecture

The Meraki AP collects the information of Bluetooth around the location where it is located and stores it on the cloud. The SilentDefense issues the queries to the ICS Patrol sensors that targeted the Meraki Cloud. The data retrieved by ICS Patrol sensors will send to the SilentDefense database for assessment purposes.

Cisco Meraki provides the Python SDK for deployment. The ICS Patrol module conduct with Python programming language and the Meraki SDK (Github: meraki/dashboard-api-python 2020).

- As a high-level language, Python is widely used in software development include games, web application framework... In the software industry, python has a larger amount of users than other languages, because of its benefits: support a wide range of libraries; integration features by invoking COM or COBRA components also processes XML that run on all modern operating systems; improve programmer's productivity with the clean object-oriented design.
- Cisco Meraki launches an improved Python SDK (Software Development Kit) with the Meraki Dashboard API recently in order to make it easier to program in Python. This library provides all existing calls to the Cisco Meraki Cloud through the Meraki Dashboard API. The library requires Python 3.6 or above. Using a Meraki library can help users focus on specific use cases, without having any

issues of writing functions to handle the dashboard API. The error handling, logging, retire can also be taken care of by this library.

The Meraki Patrol module implements a set of queries to the Meraki Cloud Dashboard. The Meraki Access Point (AP) is a cloud-managed device, which is able to collect Bluetooth and WiFi network information from the nearby Bluetooth devices and networks. This module communicates directly with the Meraki remote server and not with the device installed into the network.

The parameters needed to perform the queries are Organization ID, Network ID, and a valid API key. The Patroller target is the IP of the Meraki AP on the network. The main logic of this module checks if the target IP refers to a valid Meraki AP already configured on the Meraki Dashboard. If so, it retrieves the Bluetooth information collected by that particular device.

- TARGET: The target's IP address in the network.
- PARAMETERS: The API key.
- QUERIES: The queries used to query the Meraki Cloud and retrieve useful information.
    - BLUETOOTH: Retrieve the list of Bluetooth devices that have been seen by that AP.
    - WIFI: retrieve the list of WiFi networks that have been seen by that AP.

The main logic does the job that sends the query to the Meraki cloud and retrieves the information based on the queries. The main logic code performs following by the workflow:

Firstly, the main logic code takes the TARGET and Meraki API key as the parameter.

- The Patrol module does the job that sends the query to the Meraki cloud. The API key is used for checking the authentication on the cloud.
- If the API key is not valid, the logic code will raise an API key error.
- If the key is valid, the authentication is verified. The cloud will check the Patroller TARGET.

Secondly, the cloud will check if the Patroller target IP address refers to a valid Meraki AP already configured on the Meraki Dashboard. The Meraki AP is configured to Meraki Dashboard by the administrator with the static IP address on the network system.

Thirdly, the ICS Patrol module check the queries used for querying to the cloud:

- If the queries are not valid, the logic will raise an error invalid queries.
- If the queries are valid which are equal to the referred queries from the Patrol module, the cloud will return corresponding information based on the queries. For the BLUETOOTH query, the cloud returns the list of Bluetooth devices that had been seen by that AP; for the WIFI query, the cloud returns the list of WiFi networks that had been seen by that AP.

Finally, the module returns the result as a dictionary with the keys are the queries. The values are the results that are returned from the Meraki cloud.

4.2 Experimenting Aruba Access Point

Aruba Access Point (AP) offers a solution for tracking assets based on Real-Time Location Service (RTLS). The AP scans all the BLE devices around the placement where it is located. By using the specific command to query the AP and retrieve the corresponding BLE devices for BLE command and Wi-Fi networks for Wi-Fi network command (Figure 16 – 17).

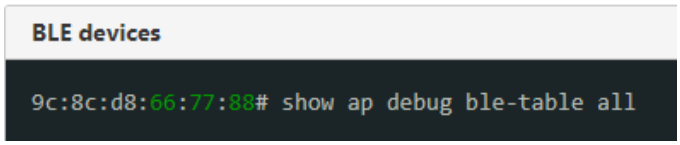


Figure 16. Command to get all BLE devices.

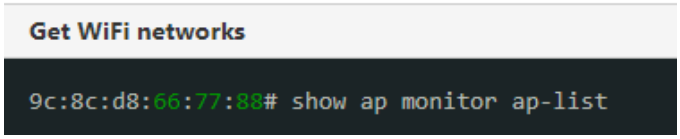


Figure 17. Command to get all Wi-Fi networks.

Since the Aruba AP can access locally that means all the results depend on the type of command and the time to do the queries, according to RTLS. Furthermore, the results are not stored anywhere else.

4.3 Results

4.3.1 Meraki Access Point

The users have the authorization to manage, control, analysis of the results from the ICSP module. The users send the payload which contains the target, parameters, and queries to the ICS. The correct payload will handle by the corresponding module. Once the payload has been executed, it will query the Cloud and return the results based on the queries.

According to Figure 18 - 19, the results returned as a JSON format, the main function of the module will do the job to validate, verify, and turned into the corresponding attributes of SilentDefense.


```
"bluetooth_devices": [
    {
        "address": "REPLACE_TARGET_IP / 38:18:9c:2b:19:90",
        "device_name": "Apple Watch 5",
        "vendor": "Apple",
        "connectivity_history": [
            {
                "firstSeenAt": 1590410535.966,
                "lastSeenAt": 1590410535.969846,
                "seenByMac": "68:3a:1e:66:77:88"
            }
        ],
    },
    {
        "address": "REPLACE_TARGET_IP / 38:78:4c:25:0b:08",
        "device_name": "Samsung S10",
        "vendor": "Samsung",
        "connectivity_history": [
            {
                "firstSeenAt": 1000410535.966,
                "lastSeenAt": 2690410535.969846,
                "seenByMac": "68:3a:1e:66:77:88"
            }
        ],
    },
    {
        "address": "REPLACE_TARGET_IP / 38:18:4c:2b:aa:6e",
        "device_name": "Bose 5",
        "vendor": "Bose",
        "connectivity_history": [
            {
                "firstSeenAt": 1999410535.966,
                "lastSeenAt": 2999410535.969846,
                "seenByMac": "68:3a:1e:66:77:88"
            }
        ],
```


Figure 18. The result for query BLUETOOTH.

Figure 19. The result for query WIFI.

There are some fields that need to be extracted from the result and added into the SilentDefense (Figure 20):

- Address: the combination of nested host IP and nest device's MAC addresses.
- Hostname: the device's name
- Vendor/Model: The manufacturer of the devices.
- Protocol: Bluetooth

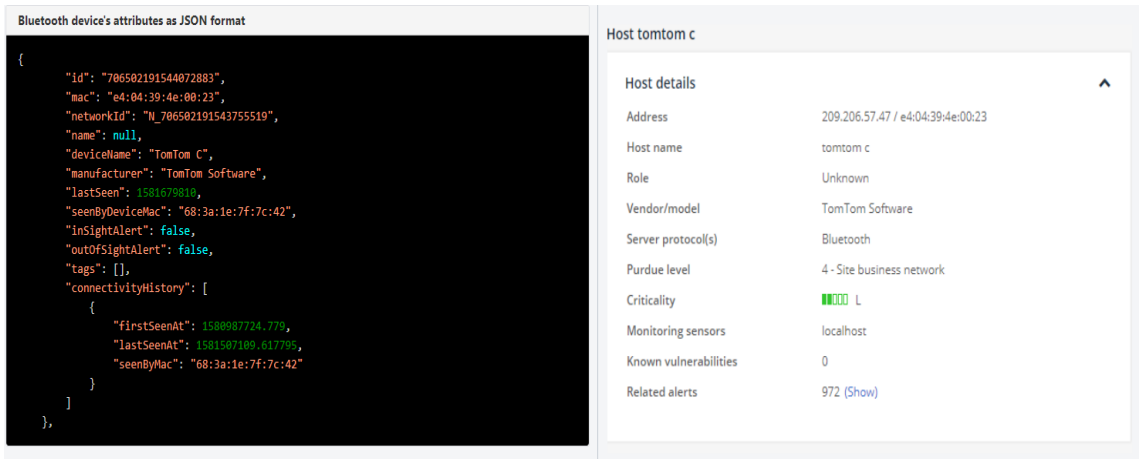


Figure 20. The correlation between Meraki's result and SilentDefense attributes.

In the SilentDefense, every device acts as a node in the network map. Each node communicates with other nodes making a complex network map. The Meraki Access Point becomes a nested host that held all the Bluetooth devices which are discovered by that access point. The nested host and nested devices can be viewed in the SilentDefense Network Map.

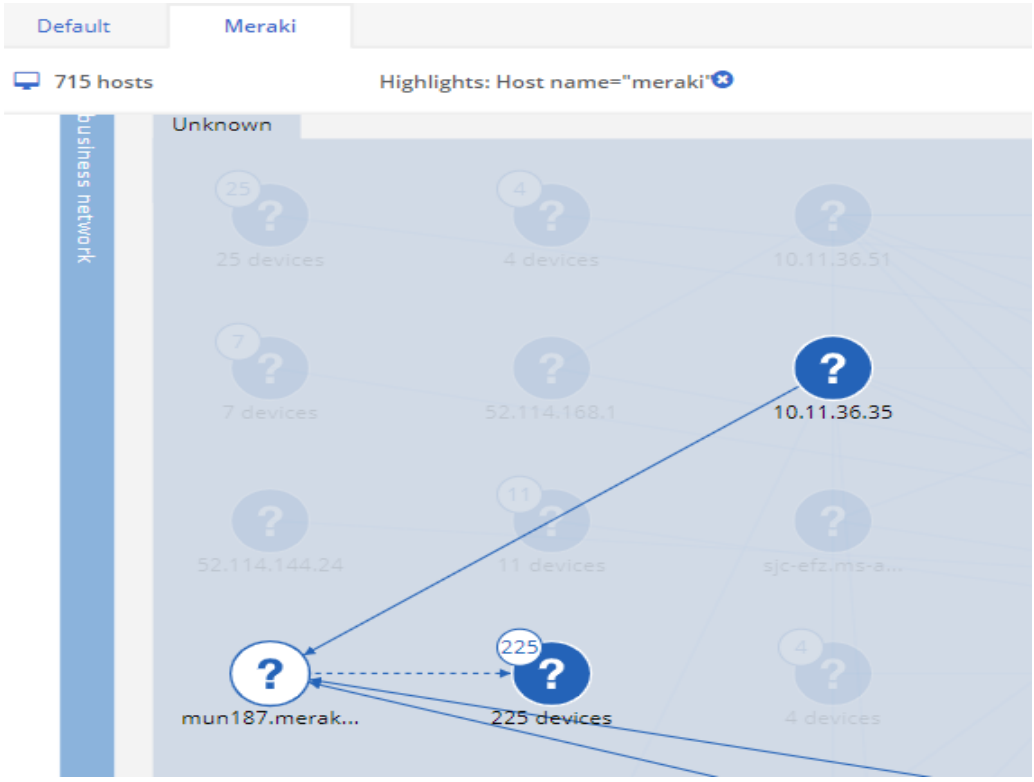
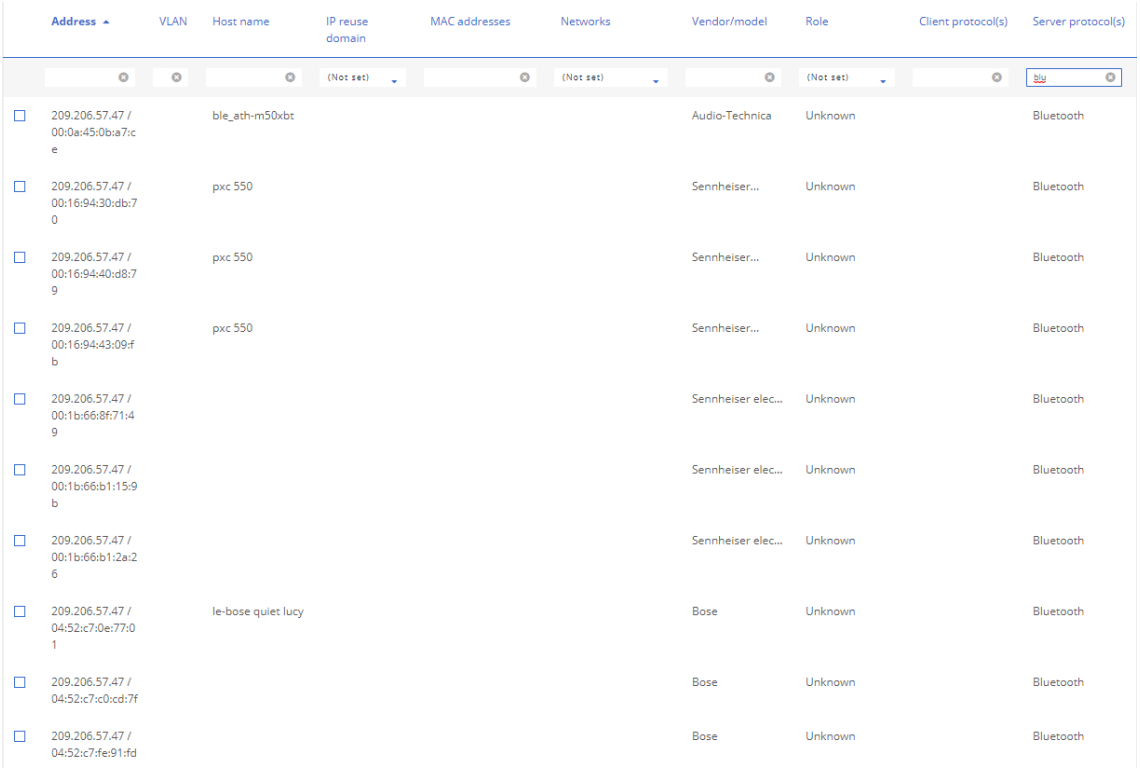


Figure 21. Network Map View.

According to Figure 21, the Meraki Access Point (AP) is showed as a nested host. The communications come in and out from that AP to other clients (the arrow) in the network as well as the Bluetooth devices, 225 devices in total for a period of 7 days (the dash line arrow).



Address	VLAN	Host name	IP reuse domain	MAC addresses	Networks	Vendor/model	Role	Client protocol(s)	Server protocol(s)
			(Not set)		(Not set)		(Not set)		blu
209.206.57.47 / 00:0a:45:0b:a7:ce		ble_ath-m50xbt				Audio-Technica	Unknown		Bluetooth
209.206.57.47 / 00:16:94:30:db:70		pxc 550				Sennheiser...	Unknown		Bluetooth
209.206.57.47 / 00:16:94:40:d8:79		pxc 550				Sennheiser...	Unknown		Bluetooth
209.206.57.47 / 00:16:94:43:09:fb		pxc 550				Sennheiser...	Unknown		Bluetooth
209.206.57.47 / 00:1b:66:8f:71:49						Sennheiser elec...	Unknown		Bluetooth
209.206.57.47 / 00:1b:66:b1:15:9b						Sennheiser elec...	Unknown		Bluetooth
209.206.57.47 / 00:1b:66:b1:2a:26						Sennheiser elec...	Unknown		Bluetooth
209.206.57.47 / 04:52:c7:0e:77:01		le-bose quiet lucy				Bose	Unknown		Bluetooth
209.206.57.47 / 04:52:c7:c0:cd:7f						Bose	Unknown		Bluetooth
209.206.57.47 / 04:52:c7:fe:91:fd						Bose	Unknown		Bluetooth

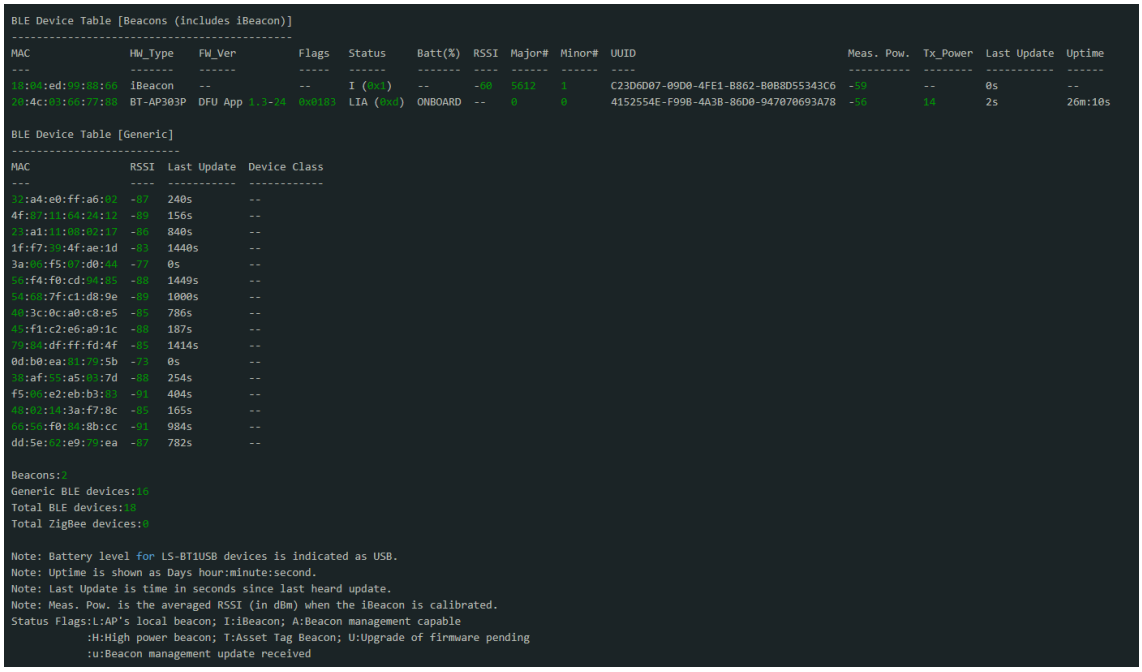
Figure 22. Network Monitored Hosts.

In the Network monitored hosts, the users are able to check and manage the nested devices as the Figure 22. All the nested devices have their own attributes, e.g, Address, Name, Vendor, and Protocol.

The data are stored in the Cloud for up to 7 days that means the BLE devices had been seen by that AP can accumulate and be stored on the Cloud and can access anytime, anywhere The module can do the query in a period of time (e.g., in the 60s). At the time of testing, the module retrieved more than 225 devices and more than 200 Wi-Fi networks around.

4.3.2 Aruba Access Point

Once the command has been executed, the AP returns the results immediately, the results vary depends on the time of querying the command. At the time of testing, the AP returned 18 BLE devices and 61 Wi-Fi networks in total (Figure 23 – 24).



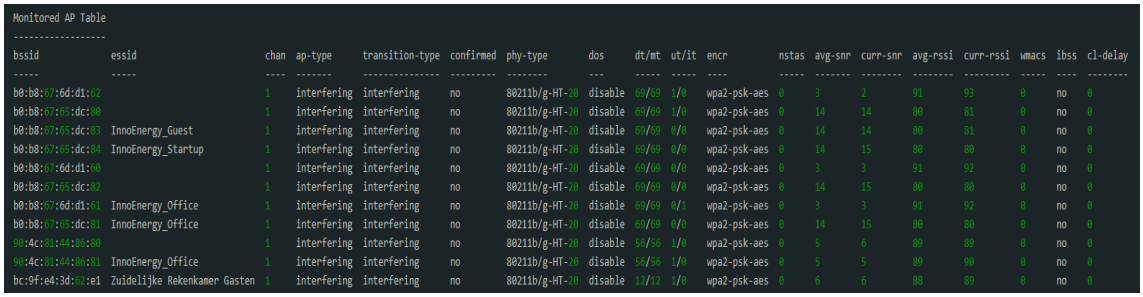
```
BLE Device Table [Beacons (includes iBeacon)]
-----------------------------------------------
MAC               HW_Type    FW_Ver          Flags   Status     Batt(%)  RSSI  Major#  Minor#  UUID                                  Meas. Pow.  Tx_Power  Last Update  Uptime
---               -------    ------          -----   ------     -------  ----  ------  ------  ----                                  ----------  --------  -----------  ------
18:04:ed:99:88:66  iBeacon    --              --      I (0x1)    --       -60   5612    1       C23D6D07-09D0-4FE1-B862-B0B8D55343C6  -59         --        0s           --
20:4c:03:66:77:88  BT-AP303P  DFU App 1.3-24  0x0183  LIA (0xd)  ONBOARD  --    0       0       4152554E-F99B-4A3B-86D0-947070693A78  -56         14        2s           26m:10s

BLE Device Table [Generic]
---------------------------
MAC               RSSI  Last Update  Device Class
---               ----  -----------  ------------
32:a4:e0:ff:a6:02  -87   240s         --
4f:87:11:64:24:12  -89   156s         --
23:a1:11:08:02:17  -86   840s         --
1f:f7:30:4f:ae:1d  -83   1440s        --
3a:06:f5:07:d0:44  -77   0s           --
50:f4:f0:cd:04:85  -88   1449s        --
54:60:7f:c1:d8:9e  -89   1000s        --
40:3c:0c:a0:c8:e5  -85   786s         --
45:f1:c2:e6:a9:1c  -88   187s         --
79:04:df:ff:fd:4f  -85   1414s        --
0d:b0:ea:81:70:5b  -73   0s           --
38:af:55:a5:03:7d  -88   254s         --
f5:06:e2:eb:b3:83  -91   404s         --
48:02:14:3a:f7:8c  -85   165s         --
66:56:f0:84:8b:cc  -91   984s         --
dd:5e:62:e9:70:ea  -87   782s         --

Beacons:2
Generic BLE devices:16
Total BLE devices:18
Total ZigBee devices:0

Note: Battery level for LS-BT1USB devices is indicated as USB.
Note: Uptime is shown as Days hour:minute:second.
Note: Last Update is time in seconds since last heard update.
Note: Meas. Pow. is the averaged RSSI (in dBm) when the iBeacon is calibrated.
Status Flags:L:AP's local beacon; I:iBeacon; A:Beacon management capable
           :H:High power beacon; T:Asset Tag Beacon; U:Upgrade of firmware pending
           :u:Beacon management update received
```

Figure 23. The results for BLE command.



```
Monitored AP Table
------------------
bssid             essid                        chan  ap-type      transition-type  confirmed  phy-type       dos      dt/mt  ut/it  encr          nstas  avg-snr  curr-snr  avg-rssi  curr-rssi  wmacs  ibss  cl-delay
-----             -----                        ----  -------      ---------------  ---------  --------       ---      -----  -----  ----          -----  -------  --------  --------  ---------  -----  ----  --------
b0:b8:67:6d:d1:62                              1     interfering  interfering      no         80211b/g-HT-20 disable  69/69  1/0    wpa2-psk-aes  0      3        2         91        93         0      no    0
b0:b8:67:65:dc:40                              1     interfering  interfering      no         80211b/g-HT-20 disable  69/69  1/0    wpa2-psk-aes  0      14       14        80        81         0      no    0
b0:b8:67:65:dc:83  InnoEnergy_Guest            1     interfering  interfering      no         80211b/g-HT-20 disable  69/69  0/0    wpa2-psk-aes  0      14       14        80        81         0      no    0
b0:b8:67:65:dc:84  InnoEnergy_Startup          1     interfering  interfering      no         80211b/g-HT-20 disable  69/69  0/0    wpa2-psk-aes  0      14       15        80        80         0      no    0
b0:b8:67:6d:d1:60                              1     interfering  interfering      no         80211b/g-HT-20 disable  69/69  0/0    wpa2-psk-aes  0      3        3         91        92         0      no    0
b0:b8:67:65:dc:82                              1     interfering  interfering      no         80211b/g-HT-20 disable  69/69  0/0    wpa2-psk-aes  0      14       15        80        80         0      no    0
b0:b8:67:6d:d1:61  InnoEnergy_Office           1     interfering  interfering      no         80211b/g-HT-20 disable  69/69  0/1    wpa2-psk-aes  0      3        3         91        92         0      no    0
b0:b8:67:65:dc:41  InnoEnergy_Office           1     interfering  interfering      no         80211b/g-HT-20 disable  69/69  0/0    wpa2-psk-aes  0      14       15        80        80         0      no    0
90:4c:81:44:86:80                              1     interfering  interfering      no         80211b/g-HT-20 disable  56/56  1/0    wpa2-psk-aes  0      5        6         89        89         0      no    0
90:4c:81:44:86:81  InnoEnergy_Office           1     interfering  interfering      no         80211b/g-HT-20 disable  56/56  1/0    wpa2-psk-aes  0      5        5         89        90         0      no    0
bc:9f:e4:3d:62:e1  Zuidelijke Rekenkamer Gasten 1     interfering  interfering      no         80211b/g-HT-20 disable  12/12  1/0    wpa2-psk-aes  0      6        6         88        89         0      no    0
```

Figure 24. The results for Wi-Fi command.

4.4 Comparison between Meraki and Aruba Access Point

In general, Meraki MR30H is outweighed by Aruba 303P. Meraki gives more advantages to the Cost of operation as well as performance.

For Bluetooth Asset Inventory, Meraki MR30H gives a better result of the BLE devices than Aruba 303P, for both devices the data can be stored on the cloud with a flexible subscription which helps easy to manage. There is one disadvantage of Meraki is that Meraki only supports cloud-based which means all the actions need to perform via the Cloud, the IDS requires an active internet connection which is not always describable on

the ICS network. On the other hand, Aruba seems suitable for use in the IDS more than Meraki, because it can operate locally instead of interact over the cloud.

	Meraki MR30H	Aruba 303P
BLE Antena in AP	• Single integrated Omni-directional BLE antenna. • Additional 3rd party battery-powered BLE beacons required for coverage.	• Single integrated Omni-directional BLE antenna. • Additional Aruba battery-powered BLE beacons required for coverage.
Location Algorithm	• Dependent on accurate map placement.	• Dependent on accurate map placement.
Location analytics	• Wi-Fi and Bluetooth standard. • Data stored on the Cloud.	• Support ALE (Analytics and Location Engine). • Data not stored on the local devices. Possible to store on the Aruba Central Cloud.
Asset tracking	• Using Signal Strength and Placement of AP. • 3rd party RealTime Location Services (RTLS) solutions from Meraki technology partners such as Ekahau to enable tracking of non-WiFi assets.	• Tracking of Aruba BLE asset tags supports from Aruba 3xx model APs with integrated BLE beacon.
Asset Result	• Name • MAC address • Vendor/Model • RSSI • InSight/OutSight alert • Connectivity History (first & last)	• MAC address • RSSI • Last update

Figure 25. Comparison between Meraki and Aruba Access Point.

5 CONCLUSION

The thesis aimed to provide Bluetooth visibility and to leverage Cisco Meraki and Aruba access points in order to improve the visibility of IoT protocols, to study threat scenarios arising from the use of IoT in the enterprise, and to examine how to extend a commercial IDS. The goals of the thesis were achieved during the internship period at Forescout Technologies Inc by conducting research in various technology magazines to collect a wide range of IoT protocols, developing a threat modeling, and implementing the Bluetooth asset inventory project within the company. The Bluetooth project can be used to identify the assets, the first important phase in Threat modeling. Identifying the assets allows the enterprise to better understand the IoT device visibility, in preparation to develop the IDS efficiently.

Eventually, the Bluetooth asset inventory was a small part of the Intrusion Detection System (IDS) which was to identify the assets in the threat modeling plan. The Bluetooth project can be tested in the SilentDefense and the intrusion researchers were able to retrieve the BLE devices with full information such as the device's name, vendor/model, MAC address, RSSI, and connectivity history. The overall results of the Bluetooth project have met the requirements planned out from the beginning that provide detailed information of all IoT devices in the network system.

Nevertheless, there is a limitation since the Bluetooth asset inventory is a part of the SilentDefense, it requires monitoring and captures the network traffic locally in the network system. However, the results can only be retrieved by querying over the cloud which is less convenient, has less privacy, and is less secure. For further development, the Bluetooth asset inventory can be implemented by using SNMP, an efficient means to monitor the local traffic. By properly implementing the identity assets, this project could be a success, more secure, and could be used as the first important stage of the IDS.

REFERENCES

Aruba Central, 2020. *Aruba Central Datasheet*. [ebook] Aruba, p.1. Available at: <https://www.arubanetworks.com/assets/ds/DS_ArubaCentral.pdf> [Accessed 16 June 2020].

Arubanetworks, 2020. *Aruba Instant 8.3.0.X*. [online] Available at: <https://www.arubanetworks.com/techdocs/Instant_83x_WebHelp/Content/PDFs/Aruba%20Instant%208.3.0.x%20User%20Guide.pdf> [Accessed 16 June 2020].

Arubanetworks.com. 2020. *Aruba Datasheet*. [online] Available at: <https://www.arubanetworks.com/assets/ds/DS_AP303Series.pdf> [Accessed 20 May 2020].

Barry, Peter and Crowley, Patrick, 2012. *Modern Embedded Computing | Sciencedirect*. [online] Sciencedirect.com. Available at: <https://www.sciencedirect.com/book/9780123914903/modern-embedded-computing> [Accessed 28 May 2020].

Cheshire, Stuart, 2013. *RFC 6762 - Multicast DNS*. [ebook] Internet Engineering Task Force (IETF), p.1-33. Available at: <https://tools.ietf.org/pdf/rfc6762.pdf> [Accessed 16 April 2020].

Cisco Meraki MR30H, 2020. *Cisco Meraki Cloud Managed Wireless Products*. [online] Available at: <https://meraki.cisco.com/products/wireless/mr30h> [Accessed 13 May 2020].

Cisco Meraki, 2020. *The Cisco Meraki Dashboard API*. [online] Available at: <https://documentation.meraki.com/zGeneral_Administration/Other_Topics/The_Cisco_Meraki_Dashboard_API> [Accessed 16 June 2020].

Dameff, Christian and Radcliffe, Jay, 2018. *Black Hat USA 2018*. [online] Blackhat.com. Available at: <https://www.blackhat.com/us-18/briefings/schedule/> [Accessed 15 May 2020].

Doss Robin, Piramuthu Selwyn and Zhou Wei, 2015.[book] *Future Network Systems And Security*. Springer International Publishing Switzerland, p.75.

Engineers Garage. 2018. *Service Delivery Protocols - DNS-SD, Mdns, Upnp And Simple Discovery Service Protocol : IOT Part 10*. [online] Available at: <https://www.engineersgarage.com/tutorials/service-delivery-protocols-dns-sd-mdns-upnp-and-simple-discovery-service-protocol-iot-part-10/> [Accessed 16 June 2020].

Express, Pwnie, 2017. *Pwnieexpress/Blue_Hydra*. [online] GitHub. Available at: <https://github.com/pwnieexpress/blue_hydra> [Accessed 18 May 2020].

Farahani, Shahin, 2008. *Zigbee Wireless Networks And Transceivers*. [ebook] Elsevier, p.265. Available at: <https://books.google.com/books?id=m5NYbUpqXY0C&pg=PA265&lpg=PA265&dq=zigbee+65536+nodes&source=bl&ots=9jN5xva-

bl&sig=ACfU3U3M92zDZESxMpjBDlj6BTHZvv0SBg&hl=en&sa=X&redir_esc=y#v=onepage&q=65536&f=false> [Accessed 16 April 2020].

Ficco, Massimo and Palmieri, Francesco, 2017. *Security And Resilience In Intelligent Data-Centric Systems And Communication Networks*. Elsevier, p.217.

Forescout. 2020. Forescout Technologies - IoT Security Company In San Jose, CA. [online] Available at: <https://www.forescout.com/company/> [Accessed 14 April 2020].

Forescout.com. 2020. *Silent Defense*. [online] Available at: <https://www.forescout.com/company/resources/silentdefense-datasheet/> [Accessed 14 May 2020].

GitHub. 2017. *Greatscottgadgets/Ubertooth*. [online] Available at: <https://github.com/greatscottgadgets/ubertooth/wiki/Getting-Started> [Accessed 18 May 2020].

GitHub, 2020. *Meraki/Dashboard-Api-Python*. [online] Available at: <https://github.com/meraki/dashboard-api-python/> [Accessed 16 June 2020].

Greenberg, Andy, 2020. *The Untold Story Of Notpetya, The Most Devastating Cyberattack In History*. [online] Wired. Available at: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> [Accessed 15 May 2020].

Hasan, Mehedi, 2020. *Top 15 Standard Iot Protocols That You Must Know About | Ubuntupit*. [online] UbuntuPIT. Available at: <https://www.ubuntupit.com/top-15-standard-iot-protocols-that-you-must-know-about/#comments> [Accessed 26 April 2020].

Haataja, Keijo, 2009. *Security Threats And Countermeasures In Bluetooth-Enabled Systems*. [online] Epublications.uef.fi. Available at: <https://epublications.uef.fi/pub/urn_isbn_978-951-27-0111-7/urn_isbn_978-951-27-0111-7.pdf> [Accessed 16 June 2020].

Huawei, 2020. *Application Scenarios For Mdns Relay - S12700 V200R013C00 Configuration Guide - IP Service - Huawei*. [online] Available at: <https://support.huawei.com/enterprise/en/doc/EDOC1100065646/a238a14d/application-scenarios-for-mdns-relay> [Accessed 16 June 2020].

Knight, Shawn, 2018. *700-Series Z-Wave Chipset Will Enable Sensors With 10-Year Battery Life*. [online] TechSpot. Available at: <https://www.techspot.com/news/72652-700-series-z-wave-chipset-enable-sensors-10.html> [Accessed 16 June 2020].

Lerner, Steven, 2018. *Medical Device Flaws Shine Light On Security And Iot Issues*. [online] Enterprise Mobility Exchange. Available at: <https://www.enterprisemobilityexchange.com/eme-security/news/medical-device-security-iot> [Accessed 24 April 2020].

Lua.org. 2020. *Lua Programming Language*. [online] Available at: <http://www.lua.org/about.html> [Accessed 16 June 2020].

Maayan, G.David, 2020. The Iot Rundown For 2020: Stats, Risks, And Solutions - Security Today. [online] Security Today. Available at: <https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.aspx> [Accessed 14 April 2020].

Majkowski, Marek, 2017. *Stupidly Simple Ddos Protocol (SSDP) Generates 100 Gbps Ddos*. [online] The Cloudflare Blog. Available at: <https://blog.cloudflare.com/ssdp-100gbps/> [Accessed 16 June 2020].

Mitchell, Bradley, 2019. *How Far Will Your Wi-Fi Reach?*. [online] Lifewire. Available at: <https://www.lifewire.com/range-of-typical-wifi-network-816564> [Accessed 16 June 2020].

Mitchell, Bradley, 2020. *802.11 Wifi Standards Explained*. [online] Lifewire. Available at: <https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553> [Accessed 15 April 2020].

Microsoft Azure, 2017. *Iot Security Architecture*. [online] Available at: <https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture> [Accessed 16 June 2020].

Myers, Lisa, 2020. *Lock Down Personal Smart Devices To Improve Enterprise Iot Security*. [online] Security Intelligence. Available at: <https://securityintelligence.com/articles/lock-down-personal-smart-devices-to-improve-enterprise-iot-security/> [Accessed 15 May 2020].

Nawijn, Bram, 2019. *Iot Connectivity Benefits An Enterprise-Oriented Environment*. [online] Tjip.com. Available at: <https://www.tjip.com/en/publications/iot-connectivity-benefits-enterprise-oriented-environment> [Accessed 16 June 2020].

Shelby, Zach, 2014. *RFC 7252 Constrained Application Protocol (Coap)*. [ebook] Internet Engineering Task Force (IETF), p.1. Available at: <https://tools.ietf.org/pdf/rfc7252.pdf> [Accessed 16 April 2020].

Seri, Ben and Vishnepolsky, Gregory, 2017. *Blueborne Technical White Paper*. 1st ed. [ebook] ARMIS, p.5. Available at: <https://www.armis.com/resources/iot-security-research/blueborne-technical-white-paper/> [Accessed 19 May 2020].

Sensor and Actuator Network, 2018. *Security Vulnerabilities In Bluetooth Technology As Used In Iot*. 1st ed. [ebook] Sensor and Actuator Networks, p.8-15. Available at: <https://www.mdpi.com/journal/jsan> [Accessed 26 May 2020].

Taylor, Twain, 2019. *6 Most Commonly Used Iot Communication Protocols*. [online] TechGenix. Available at: <http://techgenix.com/iot-communication-protocols/> [Accessed 16 June 2020].

Tech Wire Asia. 2019. *Applying Iot To The Enterprise World And Why It Matters - Tech Wire Asia*. [online] Available at: <https://techwireasia.com/2019/01/applying-iot-to-the-enterprise-world-and-why-it-matters/> [Accessed 16 June 2020].

Triggs, Robert, 2018. *A Quick History Of Bluetooth*. [online] Android Authority. Available at: <https://www.androidauthority.com/history-bluetooth-explained-846345/> [Accessed 25 January 2021].

Woolley, Martin. *Bluetooth 5 Go Faster. Go Further.*. [ebook] bluetooth.com, p.5. Available at: <https://www.bluetooth.com/wp-content/uploads/2019/03/Bluetooth_5-FINAL.pdf> [Accessed 14 April 2020].