ICS 442 – Penetration Testing

Project Proposal

IoT Security Analysis & Countermeasures

Dr. Emad Ramadan

Yahya Althubaity 201650160

Osama Bujwaied 201661700

Ridha Alismail 201687160

Table of Contents

1. Introduction

Internet of Things (**IoT**) is a network of physical objects that have technologies allowing them to connect and exchange data with other devices over the internet. IoT became one of the most important topics currently in the modern world. It contains complex network that comprise huge number of smart devices that are connected together to achieve great purpose. IoT application range from smart-home, smart-city, cars, manufacturing, e-healthcare, smart control system, transportation and much more.

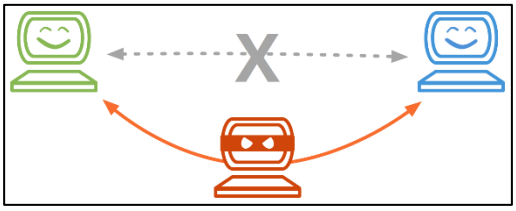
1.1 Problem

Unfortunately, the more complex IoT networks becomes harder to integrate the system together, so the system will have many vulnerabilities. There are several numbers of attacker that trying to exploit IoT network for their own self-benefits. These include stealing people sensitive information, banks accounts, mentoring the system, or controlling IoT system. This report will discuss some attacks threatening IoT networks, what data could be exposed, and ways to defend against these attacks.

1.2 Most Common IoT Attack

- https://www.globalsign.com/en/blog/five-common-cyber-attacks-in-the-iot
  - Botnets
  - **Man-In-Middle**
  - Data & Identity Theft
  - Social Engineering
  - **Denial of Service**
- https://www.channelfutures.com/best-practices/iot-insecurity-6-common-attacks-and-how-to-protect-customers
  - Privilege escalation
  - **Eavesdropping**
  - Brute-force password attacks
  - Malicious node injection
  - Firmware hijacking
  - **DoS**
  - Physical tampering

2. IoT Man-In-Middle Attack (Osama)



Man-in-Middle Attack is a concept of hacker who breach and interrupt 2 different systems. It is dangerous because attacker can alter the message that where send by these systems when they belief the are communication with each other. According to Lea (2016), several cases already have been reported about this area in hacking vehicles and smart home devices. These explosions can be used to get private information for the people, or even making a disaster.

2.1 Countermeasure

There are several techniques that can be used to prevent man-in-middle attack. We will discuss some of them below.

2.2.1 Digital Certifications

The most important technique to prevent man-in-middle is to use Digital Certifications. It will use advanced encryption technique between the 2 system to make sure there is no one in the middle that can spy or modify in their connection. that can be achieved by checking the client Digital Certification by the server before establishing the connection. IoT devices manufacturers are trying to install Digital Certification in all of these their devices. The problem is that they might need to assign hundreds of thousands of these certificates to each of these devices. This Diagram will illustrate how the Digital Certification will work in the system

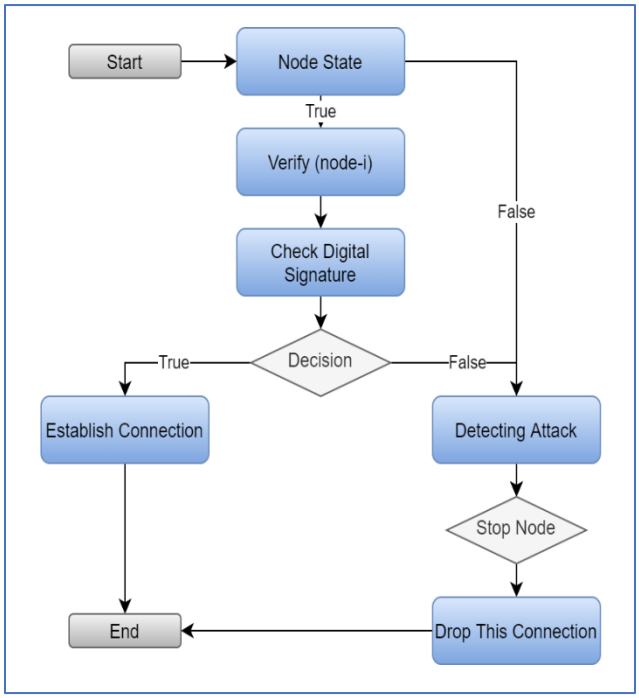


Figure 1. Digital Certification Mechanism.

2.2.2 Virtual Private Network (VPN)

Other way to prevent Man-in-Middle is to use Virtual Private Network. It will make secure communication tunnel between 2 devices a by encrypting everything that go in and out of the device. This encryption will not make the attacker be able to examine the data that send between the communication. This can be achieved by pair of public and private keys for each of the end node device. These keys will be swapped during the communication in the handshake. By this way the information remains secure till it arrives to its destination.

3. IoT Eavesdropping (Ridha)

3.1 Attack

IoT is a growing field and has many aspects in our life. Today as IoT systems and networks become bigger and more complex, attackers have found some vulnerability in them. One of the attacks is called eavesdropping. Which is stealing the information as it is transmitted over the network between computers, sensors, smartphones, servers,…..etc. It is one of the simplest attacks that can be performed. By listing to the communication between two points. after that, the hacker can get data from it and decrypt the message if needed.

3.2 Counter measure

One of the solutions proposed by Gang Liu and his teammates[3] is programming protocol-independent packet processors (P4)-based network immune scheme (P4NIS). P4NIS is a protocol made specifically to mitigate eavesdropping attacks. It uses three lines of defense.

1) **The first line of defense**

It contains three parts the first part is multipath defense. Multipath defense is augmenting the promiscuous and stateful forwarding policy by having multiple alternative options, the first line of P4NIS manages multiple heterogeneous paths in which the packets are difficult to be entirely eavesdropped. For example, P4NIS is equipped with three 4G LTE modules to forward packets through wireless links. The second part, Multiprotocol Defense is having various alternative network protocols, the first line of defense has the traditional IPv4 and IPv6 network protocols. Besides, a novel VLI datagram header called VLI. finally, Programmable Forwarding Defense which is combining the first two. It will cause multiple paths with each one will have multiple protocols. As a result of doing so, it will be harder to detect and reassemble the packets of the message.

2) **The second line of defense**

The second line of defense has a programmable cryptographic design to support various encryption algorithms. Using the design, operators could customize different cryptographic algorithms and encrypt packets from one stream to split them into different streams. In that case, eavesdroppers are difficult to classify the encrypted packets into streams correctly.

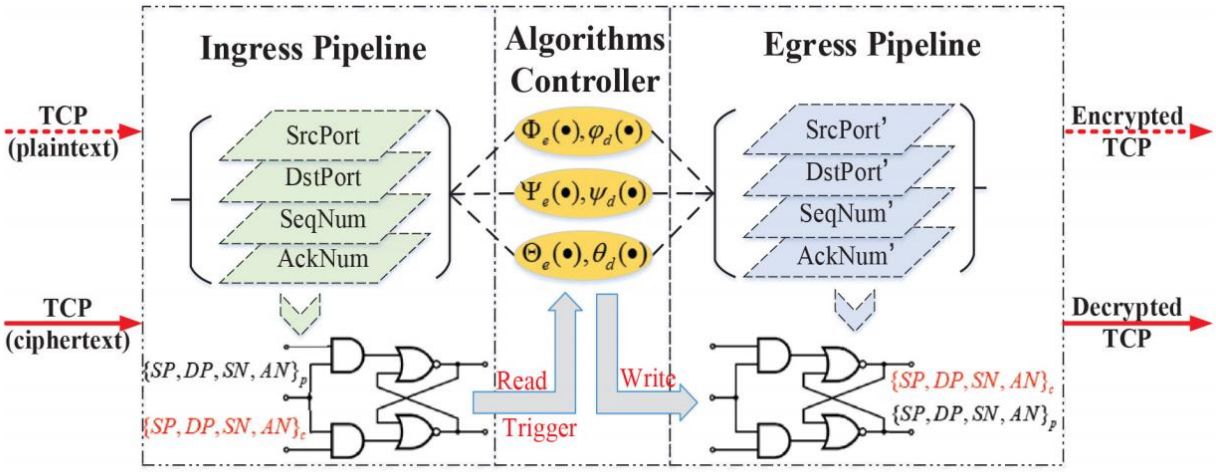


Figure 2 Programmable cryptographic design.

the design (as shown in Fig. 1) has three main parts: 1) ingress pipeline 2)algorithms controller and 3) egress pipeline. In the ingress pipeline, a TCP packet, whether it is in the type of plaintext or ciphertext, is used to extract the fields of source port, destination port, sequence number, and acknowledge number. The four fields can be combined together and stored in the local registers. After finishing the storage, the algorithm controller is triggered to encrypt/decrypt the fields using selected algorithms

3) The third line of defense

The third line of defense is the traditional cryptographic mechanism, such as RSA2048 to encrypt packet payload.

4. IoT Denial of Services (Yahya)

4.1 DoS attack

A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Using sensors that IoT systems have, IoT can collect large amount of data from the environment, the data collected needs to be stored, processed, and presented in a seamless form. Security and Privacy issues may arise in IoT systems, because IoT devices need to be connected to the internet and other IoT devices to communicate and exchange data, these connections could be exploited and flooded with malicious traffic if the network has no proper security mechanisms (Chen et all,. 2018).

4.2 Counter measures

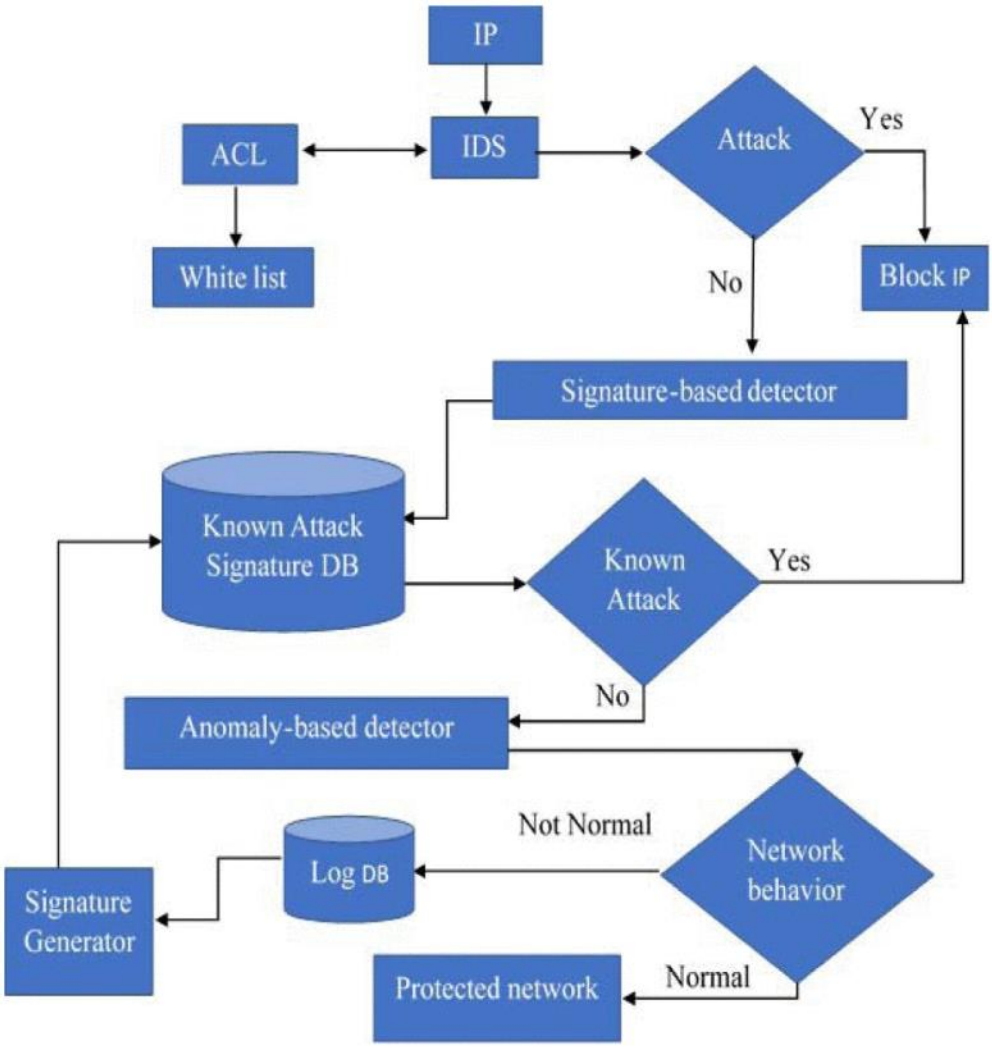
Intrusion Detection System (IDS) can be classified into two categories: signature-based and behavior-based detection systems. In signature-based detection, attacks are detected by comparing network traffic with well-known attack signatures, if there is a match, the detection system will generate an alarm. In behavior-based detection, the behavior of network traffic will be compared against previous normal traffic behavior, any anomaly or abnormal behavior is a sign of a potential attack. Both types of IDS has its own advantages and disadvantages that are shown in Table1.

Table 1 comparisoin between signature-based and behavior-based IDS

	Advantages	Disadvantages
Signature-based	- Low false positive rate - Fast detection period - Based on well-known DoS attack patterns	- Weak protection against new attacks - No alarm is set for authorized traffic - Updated on regular bases before securing a network
Behavior-based	- Monitors unknown behavior - Detects unknown attacks - Decrease limitation problems	- Produces high false positive rates - Time-consuming in means of doing exhaustive monitoring due to the amount of resources used

Defending against DoS attacks requires a hybrid IDS that benefits from each type's advantages and eliminate their weaknesses. "if an attack passed the IDS network sensors without detection (in case it is a new IP), and reached the signature-based detector without detection, then it does not match any of the signature-based attacks stored in (KAS-DB). The behavior of the attack is already traced and carefully monitored be the anomaly-based detector, and because of collaborative efforts of previous actions regardless they detected the attack or not, it will monitor the attacks behavior of byte patterns along the outcome processes of each of the IDSs and the signature-based detector output. Based on our assumptions, if the network behavior is normal during IP request time, it well be announced as a legitimate IP and approved to enter the secure network. On the other hand, if an abnormal behavior is detected in any stage, the IP will be blocked" (Shurman et all,. 2019). Figure 1 is a flow chart representing the hybrid approach.

Figure 3 Hybrid IDS



2 (Shurman et all,. 2019)

5. Conclusion

In conclusion, the IoT industry needs a lot of work in security. Especially it is involving very sensitive aspects in our life. It could cause a very cruel action such as shut down the traffic lights or electricity network. The startup companies do not seem to take cybersecurity very seriously especially because they want to produce the product as fast as possible. So there's a lot of work to do in securing IoT devices and networks.

6. References & Work Distribution

[1] Q. Chen, H. Chen, Y. Cai, Y. Zhang and X. Huang, "Denial of Service Attack on IoT System," 2018 9th International Conference on Information Technology in Medicine and Education (ITME), 2018, pp. 755-758, doi: 10.1109/ITME.2018.00171.

[2] M. M. Shurman, R. M. Khrais and A. A. Yateem, "IoT Denial-of-Service Attack Detection and Prevention Using Hybrid IDS," 2019 International Arab Conference on Information Technology (ACIT), 2019, pp. 252-254, doi: 10.1109/ACIT47987.2019.8991097.

[3] G. Liu et al., "Softwarized IoT Network Immunity Against Eavesdropping With Programmable Data Planes," in IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6578-6590, 15 April15, 2021, doi: 10.1109/JIOT.2020.3048842.

Table 2. Work Distribution.

Osama Bujwaied 201661700	Ridha Alismail 201687160	Yahya Althubaity 201650160
Managing Teamwork. Man-Middle Attack Design the Report.	**Eavesdropping**	**Denial of Services**