[[1]](#footnote-1)

A Survey of Internet of Things (IoT) Security Practices and Vulnerabilities

Harry Alan Frank, Jr

*Abstract*—This paper will focus on the current security protocols and vulnerabilities surrounding the Internet of Things (IoT).

*Index Terms*—Internet of Things (IoT), Denial of Service, Distributed Denial of Service (DDoS) Attack, RFID

# INTRODUCTION

I

n this document, we will explore the Internet of Things technology, implementations, and some common security practices and vulnerabilities. Since its inception, smart homes, lights, cameras, door locks, and many, many other systems have been created and sold to be used out in the world. However, many of them have been sent out without adequate security measures put into place. This allows for many different ways for attackers to take advantage and exploit these devices.

Unfortunately, corporate and individual consumers of IoT devices may not currently possess the technical expertise to evaluate the cost/benefit of purchasing more expensive devices which may be secured more properly. [1]

## Defining the Internet of Things

The internet of things is made up of many different types and styles of devices, from different fields. This can include (but is not limited to)

1. Mobile Computing (MC)
2. Wireless Sensor Networks (WSN)
3. Radio Frequency Identification (RFID)

For the purposes of this paper, IoT will be defined as follows:

*Internet of Things (IoT): a wired or wireless network of uniquely identifiable connected devices which are able to process data and communicate with each other with or without human involvement.[2]*

# Turn this section into overview

In section III, I will cover IoT technologies, interactions and implementations. In section IV, I will cover some common security protocols which are used in IoT. In section V, I will cover some vulnerabilities that are inherent in the technology.

# Internet of Things Technology, Interactions, and Implementations

The main objective of the internet of things is to allow two or more devices to automatically exchange information without any human interaction. The communication takes place over some specific communication technologies and standards, which are defined below.

## Wireless Sensor Network (WSN)

A WSN generally is described as a network of nodes that cooperatively sense and control the environment, enabling interaction between persons or computers and the surrounding environment. [3] They are comprised of a series of *nodes* where each node is connected to several other nodes. Each network typically has several main parts:

1. Radio Transceiver
2. Microcontroller
3. Memory
4. Battery or power source
5. Sensor

Each node can vary in size from shoebox sized, down to nearly the size of a grain of sand. Due to the limitations of the radio transmissions, information travels in a multi-hop relay, from sensor to sensor before reaching the primary *sink node* to be sent to the base station. Through the base station, the user can control and configure the WSN and collect the monitored data.

## Radio Frequency Identification (RFID)

Radio Frequency Identification technology is used mainly in information tags which act as small transponders to send information wirelessly to a reader, typically an autoID (Automatic Identification) which is characterized by data forms that are machine readable [4]. RFID tags differ from other autoID forms because they can be read without direct line of sight to the reader, and often have a higher read distance (feet rather than inches).

RFID tags are based on two main technologies:

### RFID Tags (Transponders)

### An RFID tag consists of:

#### A microchip, which can be as small as 0.4mm by 0.4mm. The smaller the chip, typically the higher cost. These chips are typically factory programmed with an ID number which will be picked up by the reader when scanned.

#### A chip antenna, for either magnetic or electromagnetic fields.

Typically, there are two types of RFID tags.

#### Active tags: this type of tag has an internal battery, which allows it to communicate remotely within a limited distance[5]

#### Passive tag: this type of tag has no internal battery, and so transmission occurs only when activated by an external reader. Without an internal power supply, it relies on the electromagnetic signal of the reader to activate.[5]

### RFID Readers (Transceivers)

Typically contains a radio frequency receiver and on occasion a transmitter, depending if the unit is designed to be read-only or read-write. Most are designed to operate on only a single channel or frequency.

# Security Issues

## Security Issues in Wireless Sensor Networks (WSN)

DDOS Attacks: Recently, DDoS attacks have been conducted in large scale by armies of poorly protected IoT devices that have become zombie systems in massive global campaigns [6]. Because most IoT devices typically have far more networking power than is necessary for their intended task, it is possible for them to be used in a botnet causing massive congestion on home networks, or targeting other systems with a DDoS attack.

There is no particularly good way to reduce the malicious traffic from these systems aside from squelching it at the source. [6] These devices should have no need to be able to send floods of ICMP messages, and it should be strictly throttled on the device, either through hardware limitations or kernel-side bandwidth limitations. This would reduce the device’s capabilities down to a level commensurate to it’s needs, making it more difficult to be utilized in an attack, even if compromised.

## Security Issues in RFID technology

Since RFID technology is mainly used for automatic exchange of information, there is no threat of a DDoS attack from them. However, there are vulnerabilities from which RFID technology can suffer. The four most common RFID attacks are as follows:

#### Unauthorized Tag Disabling: The tags themselves are vulnerable to a DoS attack to either temporarily or permanently incapacitate the tag.

#### Unauthorized Tag Cloning: If one captures the information from the RFID tag through a reader, it can be mimicked and cloned onto another tag. This gives the attacker access to anything that may have been secured by the RFID tag’s unique indentifier.

#### Replay Attacks: Much like cloning the tag, a tag’s identifier can be intercepted on route to the reader, and replayed back later in order to mimic having properly passed authentication

# Conclusion

References

1. G. Corser, G. Fink, M. Aledhari, J Bielby, R. Nighot, *Internet of Things (IoT) Security Best Practices*, IEEE, p. 1
2. G. Corser, G. Fink, M. Aledhari, J Bielby, R. Nighot, *Internet of Things (IoT) Security Best Practices*, IEEE, p. 2
3. S. Yinbiao, K. Lee, P. Lanctot, *Internet of Things: Wireless sensor networks,* p. 19
4. IEEE, *The State of RFID Implementation and its Policy Implications,* p. 2
5. IEEE, *The State of RFID Implementation and its Policy Implications,* p. 9
6. G. Corser, G. Fink, M. Aledhari, J Bielby, R. Nighot, *Internet of Things (IoT) Security Best Practices*, IEEE, p. 6

**Harry A Frank, Jr,** a senior at Radford University, graduating in May 2018

1. Manuscript received December 6, 2017.

   H. A. Frank, Jr is a senior at Radford University, studying Computer Science with focuses in Database and Networks, Radford Virginia, 24141; email [hfrank3@radford.edu](mailto:hfrank3@radford.edu) [↑](#footnote-ref-1)