Security of the LoRaWAN protocol

Onderzoeksmethoden 1 - Research Idea

x

September 1, 2018

Introduction

A couple of years ago the Internet of Things started to gain a lot of attention from companies, governments and other people. This attention resulted from the convergence of a lot of technologies that are now components of the Internet of Things. The applications of this network are almost infinite, most of which having something to do with information collection. IoT devices are perfect for doing this kind of work because they all work on low power. IoT devices are now already used for monitoring parking space availability[1], controlling water usage[2], smart lighting and have many more uses. These IoT devices make use of many new protocols to communicate to each other or to a server that is connected to the Internet. These protocols are designed to function on low power hardware and to transmit via low throughput waves. A couple of these Internet of Things networks are run by companies across the globe such as Sigfox or Lor. An example of a protocol used for this kind of communication is LoRaWAN. LoRaWAN is a MAC layer protocol that provides specifications for communication between IoT devices connected to the LoRaWAN network. This network also has devices capable of connecting to the Internet. These devices are called LPWAN gateways. By communicating to such a gateway, IoT devices can send data to our devices (through the Internet). We will focus upon the LoRaWAN protocol.

Problem formulation

At the earlier days of the Internet, a lot of protocols were designed for structured communication. These protocols were only designed with normal usage in mind. Nowadays, we still use these protocols and know that a lot of these protocols were not designed securely. For example, someone could just tamper with ARP messages and steal (or modify) data going over Ethernet or WiFi. Security is very important when designing a protocol for communication. Without security, possibilities for malicious attackers are endless and could result in, for example, a Denial of Service or stolen personal data. Fortunately, we have learned something from the past and have been busy designing new protocols with security in mind. The state of the IoT network nowadays is almost like the Internet in its early days. A lot of people are trying to come up with protocols to provide a way for devices on an IoT network to communicate with each other. One of these protocols, LoRaWAN, is very popular and thus widely used. The Netherlands has the first nationwide LoRaWAN network setup right now. To prevent a repeat in history, we must now look at the security aspects of newly developed protocols. This can ensure us that the protocol that was designed is future proof.

Previously done research

This is not the first time that research is being done upon the security aspects of LoRaWAN. A couple of other researchers have already tried to break the protocol and have succeeded. It is however important to research the security of LoRaWAN even more. This because of the fact that the research that has been done upon the security of LoRaWAN is based upon an older specification of the LoRaWAN protocol (version 1.0.2). Also, not all aspects of the LoRaWAN protocol have been looked into. The research that has already been done is not complete. We still need to look into the fully updated specification of the protocol and research the security of all aspects of the protocol.

Research question

We will asks ourselves the following questions:

- Is it safe to use the LoRaWAN protocol nation wide in the Netherlands?
  - How does the LoRaWAN network function?
  - What security vulnerabilities were already discovered in LoRaWAN?
  - Are these vulnerabilities fixed in the new version of LoRaWAN?
  - Are there undiscovered security vulnerabilities in the LoRaWAN protocol?

A complex enough system will always have certain vulnerabilities and (most likely) will never be one-hundred percent solid. This means that we have to define the word ”safe” in the main research question. We will define this word while using the other research questions. Two of these research questions refer to vulnerabilities. In this context, vulnerabilities are weaknesses in software or protocols. The LoRaWAN protocol will be stated as ”safe” if no vulnerabilities are found in the scope of this research and if none of the previously found vulnerabilities are discovered in this research. We must be careful though, this does not mean that no vulnerabilities exist in the LoRaWAN protocol, only that we were unable to find any in the time span that we had in this research.

Motivation

A couple of people have already suggested or tried out attacks on the LoRaWAN network and succeeded. This proves that this network is not fully secured. The developments in the IoT landscape are going very fast, it is thus a must that researchers should look at the security of the protocols used by IoT devices to prevent that we are stuck with protocols that are not secure in the future (just like with some protocols nowadays). Also, the first nationwide LoRa network is available in the Netherlands and a lot of companies are looking into this network to try to come up with ways in how they could use it to improve their business. The LoRa network is growing fast and it is very important that, before the LoRa network gets to big, possible security issues are fixed. As previously stated, some people have already accomplished attacks against LoRaWAN. Since then, the LoRa community have published a revised specification (version 1.1). It is important that this newer specification is also tested security-wise.

Theoretical framework

For answering the research question(s), we need a theoretical framework to build our research upon. One of the building blocks of our theoretical research will be the LoRaWAN specification [3]. As already stated, some papers have already been written upon an older version of the specification for LoRaWAN networks. Two of these papers can be used in this research, namely [4] and [5]. These two research papers both address security issues in version 1.0.2 of the specification for the LoRaWAN protocol. These two papers will be used to review the security status of the old vulnerabilities discussed in the research questions. Both of these papers are very recent and maybe still applicable with the new version of the LoRaWAN specification. An older report on the LoRaWAN security status is [6]. This report covers a very in-depth security view upon the join procedure of the LoRaWAN protocol. A more global view on the security of LoRaWAN can be read from [7]. This report covers a general view upon the security of LoRaWAN and an in-depth analysis of the network stack used by LoRa devices. Possible attacks can be obtained from these papers. They might not be fixed yet or might work if tweaked a little bit.

Scope

The scope of the research question must be defined in order to answer the research question. As stated earlier, this research will focus upon the LoRaWAN specification version 1.1. Also, we are looking at the security aspects of the protocol. Information leakage due to implementations are out of scope of this research. This means that side-channel attacks are also out of scope.

References

[1] "Smart parking project in montpellier to relieve traffic congestion and reduce car parking search." http://www.libelium.com/smart-parking-project-in-montpellier-to-relieve-traffic-congestion-and-reduce-car-parking-search Empty.

[2] "Smart city project in castellon: a platform to control water usage and waste management."

[3] A. Y. N. Sornin, *LoRaWAN 1.1 specification.* LoRa Alliance.

[4] E. van Es, "Lorawan vulnerability analysis."

[5] X. Yang, "Lorawan: Vulnerability analysis and practical exploitation."

[6] S. Zulian, "Security threat analysis and countermeasures for lorawan joing procedure."

[7] P. L. Emekcan Aras, Gowri Sankar Ramachandran and D. Hughes, "Exploring the security vulnerabilities of lora."