Security of the LoRaWAN protocol

Onderzoeksmethoden 1 - Research Proposal

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 need some kind of agreement on how to communicate to each other. Such an agreement is called a protocol. Many new protocols have been designed to let IoT devices communicate. 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 ran by companies across the globe such as Sigfox[1] or Lor[2]. An example of a protocol used for this kind of communication is LoRaWAN. LoRaWAN is a community made 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 devices connected to the Internet such as your smart phone. The LoRaWAN protocol is one of the popular IoT protocols around these days, it is also already rolled out nation wide in the Netherlands. Before we all adopt our IoT devices to this protocol, we need to make sure it is safe to use and can not be tempered with by potential attackers.

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. They relied upon trust in the users of the protocols. In the earlier days, this was not a big deal because not a lot of important data was transported via the Internet. Nowadays, we do our banking online, order goods online and text with each other online. If we did not change all old protocols, these things would not be possible because attackers could have just tampered with our important data and, for example, wire funds to their own account. These days, it is important to design a protocol from the ground up with security in mind because changing a protocol that is already widely used is not an easy job. A new standard for a protocol gets adopted very slowly because updates have to be rolled out for every single different piece of hardware. Sometimes even hardware needs to be replaced. This is a time consuming and costly job so it is vital that we design new protocols with security in mind. We could compare the IoT network to the Internet in its earlier days. A lot of people are coming up with new protocols and ideas on how devices could communicate over an IoT network. One of the more popular protocols is LoRaWAN. It is already used nation-wide in the Netherlands. We need to look at the security of this protocol to prevent a repeat in history.

[1] https://www.sigfox.com/
[2] https://www.loriot.io/

Motivation

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[3][4][5][6]. 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 thus 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 questions

We will asks ourselves the following questions:

- Is it safe to use the LoRaWAN protocol (version 1.1)[7] nation wide in the Netherlands?
  - How does the LoRaWAN network function?
  - What security vulnerabilities were already discovered in LoRaWAN and can still be used in the newer version of the LoRaWAN protocol.
  - 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 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 considered "safe" if no vulnerabilities are found within 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 we had and the scope that we considered in the research.

Literature

As already stated, a couple of other people have already found vulnerabilities in the LoRaWAN protocol. These vulnerabilities form a basis for finding new vulnerabilities in the protocol. Also, research that looked at other protocols similar to LoRaWAN (for example [8]) will be used to identify vulnerabilities in the LoRaWAN protocol.

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.

Methodology

The finding of vulnerabilities is not trivial. We will use action research as our main strategy to complete this research. We need a very structured approach for analyzing and exploiting the LoRaWAN protocol or otherwise we might not find or be able to exploit vulnerabilities. The method we will be using to find vulnerabilities will be based upon an approach described by J. Thuraisamy[9]. We will use this approach because it has a lot in common with the FMA approach

described in Researching Information Systems and Computing[10]. The method we will be using covers three steps:

1. Enumerate entry points
2. Identify insecure states in the protocol
3. Use the entry points to reach the insecure states

This structured method helps us to keep track of all discoveries made when analyzing the specification of LoRaWAN. We will prioritize the found vulnerabilities based upon the ease of exploitation. This ensures us that we can exploit the easier (and most of the times faster) vulnerabilities first.

Data generation method

For generating vulnerabilities, we will analyse the LoRaWAN specification and other papers related to LoRaWAN vulnerabilities. Our data generation is primarily these documents. Finding vulnerabilities in these documents is not formal work. We will thus try to describe found vulnerabilities as clear as possible. Vulnerabilities will get found by using the method of J. Thuraisamy above.

Data analysis

When an exploit is analysed and the insecure state that we are trying to achieve with the exploit is determined we will create a vulnerability cause graph[11]. This will give a good overview over how we want to exploit the protocol to reach the insecure state and will also allow others to have a quick look at the attack without reading the literature associated with it. The exploiting of the vulnerability on a real network will be done less structural because real world situations might not behave as they should theoretically. This means that we will try to write pieces of code that exploit the vulnerability. This is also used as validation of the found vulnerabilities. When a vulnerability is successfully exploited we will label it a valid vulnerability. Otherwise we will label it a theoretical vulnerability.

Validation of the research question

All valid vulnerabilities will also be labelled a threat category by using the Common Vulnerability Scoring System[12]. This system provided us with a score from one to ten. We will define the protocol secure if no valid vulnerabilities with score four or higher are found. This means that if we only find theoretical vulnerabilities or vulnerabilities with a score lower than four we will define the protocol safe because the Common Vulnerability Scoring System uses the impact of a vulnerability on a system as scoring basis. If we only find vulnerabilities with a low impact this means that these vulnerabilities "typically do not yield valuable information but may point at other possible vulnerabilities"[13].

Timeline

We will divide the available time into research phases. Each phase will have a goal to help us to answering the research question. After the phases have been explained, a time line will be showed to divide the available time between all different phases.

Phase 1, LoRaWAN specification

Before the research can start, the LoRaWAN specification must be read and completely understood. In this phase we will thoroughly read and note possible attack vectors we find in the specification. The result of this phase will be a list with possible vulnerabilities in the LoRaWAN protocol and a security-wise summary of important aspects in the LoRaWAN protocol.

Phase 2, Attacks

In this phase, we will filter out the attacks found in the previous phase and search for other (already found) attacks in other papers. We will prioritize attacks based upon how likely and easy it is to execute a specific attack. We will also try to find as much documentation as possible on attacks that were found. The result of this phase will be a list of prioritized attacks that we can exploit in the next phase.

Phase 3, Attacking LoRaWAN

In this phase we will execute the found vulnerabilities from the prioritized list. If an attack succeeded, the possible impact of this attack is documented such as how the attack was executed. The result of this phase is a list of valid attacks with a ranking and a way of how to exploit the attack.

Phase 4, Final steps

This phase is focused upon the results of the research. We will analyze the results and create a final version of the research document. This step focuses mainly upon a nice presentation of the done research.

These four phases will be the global setup of this research. Phases three and four will be repeated a couple of times for each found vulnerability. Therefor, phase three and four will have one timespan in the following diagram:

- Phase 1: 10 weeks
- Phase 2: 2 weeks
- Phase 3: 18 weeks
- Phase 4: 8 weeks

References

[1] Smart Parking project in Montpellier to relieve traffic congestion and reduce car parking search, October 24th, 2017. http://www.libelium.com/smart-parking-project-in-montpellier-to-relieve-traffic-congestion-and-reduce-car-parking-search.

[2] Smart City project in Castellon: a platform to control water usage and waste management, April 19th, 2016. http://www.libelium.com/smart-city-project-in-castellon-a-platform-to-control-water-usage-and-waste-management.

[3] E. van Es. LORAWAN VULNERABILITY ANALYSIS, March 2, 2018.

[4] Xueying Yang. LORAWAN: VULNERABILITY ANALYSIS AND PRACTICAL EXPLOITATION, July 21, 2017.

[5] Simone Zulian. Security threat analysis and countermeasures for LoRaWAN joining procedure, 2015.

[6] Piers Lawrence Emekcan Aras, Gowri Sankar Ramachandran and Danny Hughes. Exploring the security vulnerabilities of LoRa.

[7] A. Yegin N. Sornin. *LoRaWAN 1.1 specification.* LoRa Alliance, October 11, 2017.

[8] D. Kaleshi P. Thomas G. Margelis, R. Piechocki. Low Throughput Networks for the IoT: Lessons Learned From Industrial Implementations.

[9] Jackson Thuraisamy. High-Level Approaches for Finding Vulnerabilities. http://jackson.thuraisamy.me/finding-vulnerabilities.html.

[10] Briony J. Oates. *Reseraching Information Systems and Computing*. November 2005.

[11] Nahid Shahmehri David Byers, Shanai Ardi. Modeling Software Vulnerabilities With Vulnerability Cause Graphs.

[12] Inc. FIRST. Common Vulnerability Scoring System. http://www.first.org/cvss/.

[13] Yashwant K. Malaiya Omar H. Alhazmi, Sung-Whan Woo. Security vulnerability catagories in major software systems.