Modelling Cyberattacks in Internet of Things Environments

- Initial Plan -

Author: Thomas Jack Stevens

Supervisor: Prof Omer Rana

Project Description

The aim of this project is to better understand the types of cyberattacks which take place within the Internet of Things (IoT) devices. Specifically, I will be investigating attacks which can be performed on, and using, a Libelium Waspmote device. The Waspmote is designed to be a sensor node, used as part of a sensor network. It gains information on its surroundings, such a light levels and temperature, through the use of removable sensors. This information is then sent through the sensor network using removable wireless modules. These modules allow the Waspmote to communicate over a variety of wireless technologies. The Waspmote includes a variety of features, but two which I believe will be particularly relevant to this project are Over the Air Programming (OTA) and multiple encryption libraries.

There are two types of attack I am going to investigate. These two types are, attacks which can be initiated through IoT devices, and attacks which can be targeted to IoT devices. The first type of attack involves using the IoT device to exploit vulnerabilities in the sensor network. The second type involves trying to exploit the IoT device itself. As part of this investigation, I will discuss the potential implications of different vulnerabilities, such as the disruption they could cause for the public and businesses.

Both types of attacks will likely involve wireless communication as this is often the only practical way to interface with these devices. Therefore, wireless communication will be a significant focus for the project. There are many modules available for the Waspmote which allows it to utilise different wireless communication protocols. As a result I will need to gain an understanding on how different wireless protocols work, and types of vulnerabilities they are susceptible to.

After investigating the types of vulnerabilities that IoT devices are susceptible to, I intend on exploiting at least one of them, myself. I will discuss any vulnerabilities which I have not implemented and how someone might go about preforming them.

The final part of my project will be a discussion of what I have found. As a conclusion for the project, I plan to discuss how to defend against attacks. There are two areas I would like to discuss. Firstly, I would like to talk about the specific things which can be done to protect against known exploits. Secondly, I would like to talk about general good practices which can be followed to mitigate the chances of a successful attack. This is the section where I would also like to discuss further work which could be done to investigate the types of vulnerabilities which can be found in IoT devices.

Aims and Objectives

- Gain a good understanding of the types of vulnerabilities found in IoT devices and sensor networks.
- Develop a working knowledge of how IoT devices operate, with a focus on the Libelium Waspmote.
- Gain a good understanding of the different protocols used for wireless communication, including strengths and weaknesses.
- Perform a demonstration of at least one attack on an IoT device using the Waspmote and an attached wireless modules.
- Discuss the implications of any vulnerabilities found, e.g. how they could be used to disrupt companies and the public.
- Discuss how different vulnerabilities can be mitigated and what can be done to protect against them.

Work Plan

Week	Objective
Week 2	- Preform a literature review on the types of vulnerabilities which have been found in IoT devices and sensor networks.
Week 3	- Research the basic workings of IoT devices and sensor networks, i.e. When, where, why, and how they're used. - Read through Waspmote documentation, including technical, networking and programming guides.
Week 4	- Research different wireless technologies and protocols. Likely done through the use of books on the topics and RFCs. - Make notes on the specific strengths of weaknesses of different technologies/protocols.
Week 5	- Take a more in depth look at the features of the Waspmote which relate to common security flaws in IoT devices. - This step will involve having an in depth look at the areas of the Waspmote API which interact with these features, as well as reading any specific guides. - Make notes on how the weaknesses for different wireless technologies and protocols could affect the Waspmote.
Week 6 Week 7 Week 8	- Perform at least one attack on/using the Waspmote. Ideally multiple attacks will be performed, at least one on and one using the Waspmote. - A significant amount of time will likely go towards analysing code in the Waspmote API for potential vulnerabilities. - Document successful and failed attacks, as well as attacks I did not have time to carry out.
Week 9 Week 10	- Write discussion on the implications of any vulnerabilities found. - Write discussion on how vulnerabilities can be mitigated and defended against. - Draw overall conclusions from the project.

	- Compile all previous work into report, including any tables, diagrams and appendices.
Week 11	- Proof read and finalise report.

I also plan on having weekly meetings with my supervisor to discuss the project's progress.