Initial Report

Investigating Security vulnerabilities in Internet of Things Devices

CM3203 - One Semester - 40 Credits

James L. Grant - Author
Irene Anthi - Supervisor

February 3, 2019

Contents

Chapter 1

Project Description

1.1 Abstract

The popularity of Internet of Things (IoT) devices (e.g. amazon echo, smart bulbs, smart cameras, smart sensors) has significantly increased over the past few years. This is due to their ubiquitous connectivity, allowing them to exchange information with other technologies and their decision-making capabilities to invoke actions. This provides seamless user experiences which significantly enhance people's everyday lives and is demonstrated by how prominent IoT is today. Nevertheless, although these concepts support the tasks of everyday life, they come with tremendous security risks. The insufficient security measures and lack of dedicated security systems for these devices make them vulnerable to a range of cyber-attacks. The project will focus on designing and implementing attacks against IoT devices in our lab, following by the student trying to implement methods/tools, to help mitigate them.

1.2 Description and Preamble

Within the last five years, the popularity of networked embedded devices within the home has surged dramatically, allowing homeowners to alter the heating controls, switch lights on and off around the home, and even order fresh groceries through simple interfaces. These devices, collectively known as Internet of Things (IoT) devices, can be utilised to automate daily life through the collection and exchanging of data with traditionally dumb devices. An example of these devices can be found in the "Nest" smart thermostat. The Nest device is design to learn common patterns in heating usage and adapt the thermostat according to these patterns along with weather predictions gained via the internet.

Due to the nature of these devices and specifically the access they hold over the house (some smart meters can remotely shut off gas/electric), there is the real threat that devices could be compromised in such a way that the data may be extracted by an unauthorised third party, or that the functionality of the device is compromised resulting in potential harm for the victim (having gas/electric completely shut off). These risks produce a need to keep the devices secure from malicious parties through regularly patched software and other modern security practises such as encrypted communication methods. Sadly in many devices this is not the case and serves as the groundwork for this project.

The overall aim of this project is to investigate the security properties of a number of IoT devices by designing and implementing a series of cyber-attacks on each device. When these attacks have been developed, I will then proceed with designing and creating a management tool for these attacks to help with automation for the end user. By developing these attacks, I hope to gain an understanding on the fundamental vulnerabilities that surround them, with a potential to extend the knowledge into developing mitigation's and protections against these vulnerabilities.

Chapter 2

Project Aims and Objectives

As this project is rooted in the research and exploitation of specific vulnerabilities, my aims are not strictly to develop a large portion of code but more to demonstrate the effectiveness of the chosen attack vectors on a collection of IoT devices. These aims are a broader look at the project and require clarification on just how I am going to identify, design, and implement the exploits. For each of the aims below, I have also produced a series of objectives that would allow me to fulfil my aims. Below are my listed aims (labelled with numbers) with a sub list of objectives required to complete each aim:

1. To Investigate a series of attack vectors for a set of IoT devices.
   (a) Produce a specification sheet for each device listing main components, firmware, communication methods etc.
   (b) Research common vulnerabilities published for both the devices and the underlying technology.
   (c) Search for previous exploits that have been published for each given device.
   (d) Produce a list of possible attack vectors for which to explore/develop into a full exploit.
2. To develop at least one attack vector into a full exploit which can compromise the system.
   (a) Evaluate each method from the list of attacks and select the one with the highest probability to be successful.
   (b) Design an exploit based upon the chosen vector and create a payload for compromising the system.
   (c) Implement the exploit so that it can functionally compromise the system.
3. To find produce a series of findings on the state of security implementations based upon the success of the previously mentioned exploits.
   (a) Identify which exploits worked and the extent of the damage that could be caused by these exploits along with how feasible it would be for a malicious 3rd party to perform this attack on someone.
   (b) Produce potential conclusions on how these attacks could be improved and potential mitigation's against these attack vectors such as patching firmware, using encrypted traffic etc.

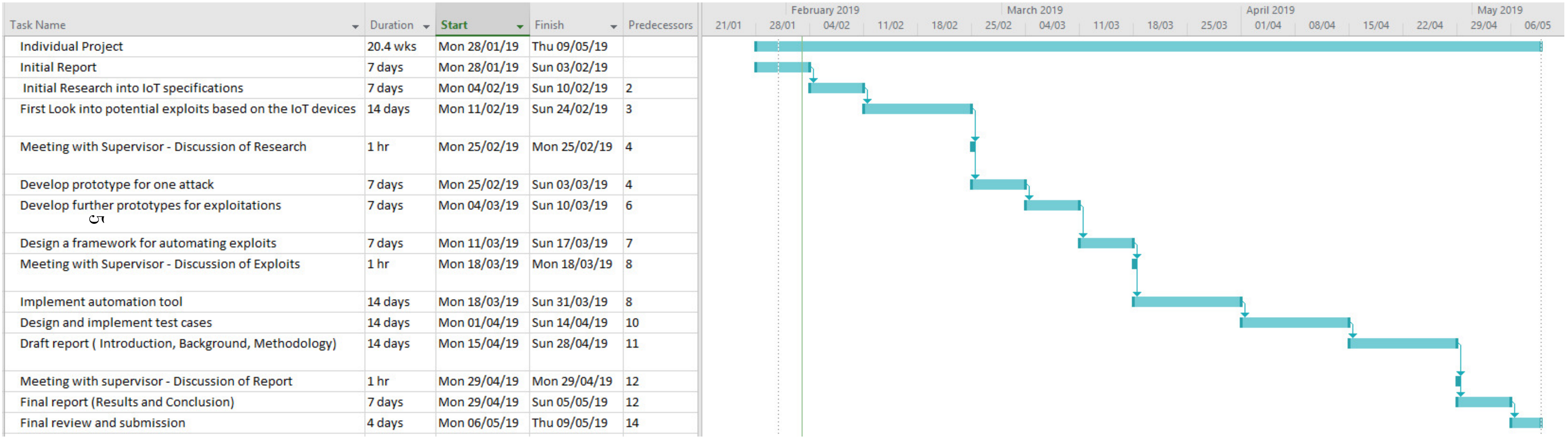
Chapter 3

Work Plan

In order for me to complete the project within the specified time, it is imperative for me to abide by a work plan consisting of a schedule for each week of the project and a set of milestones for which I can assess my progress throughout. Below is a list of milestones that I have deemed to signal significant progress through my project and then further below is a Gantt chart that will outline my schedule for the project.

3.1 Milestones

- Exploit found for each device
- Vulnerability exploited in such a way that I have compromised one device.
- Exploit other vulnerabilities to achieve the same results of compromised system for all devices.
- Develop tool to automate one attack
- Further develop tool to select target and attack vector
- Produce a series of tests surrounding the automation tool to ensure stability etc.
- Draft Report - Intro, Research, Methods
- Final Report prior to submission
- Submission



Task Name	Duration	Start	Finish	Predecessors
Individual Project	20.4 wks	Mon 28/01/19	Thu 09/05/19	
Initial Report	7 days	Mon 28/01/19	Sun 03/02/19	
Initial Research into IoT specifications	7 days	Mon 04/02/19	Sun 10/02/19	2
First Look into potential exploits based on the IoT devices	14 days	Mon 11/02/19	Sun 24/02/19	3
Meeting with Supervisor - Discussion of Research	1 hr	Mon 25/02/19	Mon 25/02/19	4
Develop prototype for one attack	7 days	Mon 25/02/19	Sun 03/03/19	4
Develop further prototypes for exploitations	7 days	Mon 04/03/19	Sun 10/03/19	6
Design a framework for automating exploits	7 days	Mon 11/03/19	Sun 17/03/19	7
Meeting with Supervisor - Discussion of Exploits	1 hr	Mon 18/03/19	Mon 18/03/19	8
Implement automation tool	14 days	Mon 18/03/19	Sun 31/03/19	8
Design and implement test cases	14 days	Mon 01/04/19	Sun 14/04/19	10
Draft report (Introduction, Background, Methodology)	14 days	Mon 15/04/19	Sun 28/04/19	11
Meeting with supervisor - Discussion of Report	1 hr	Mon 29/04/19	Mon 29/04/19	12
Final report (Results and Conclusion)	7 days	Mon 29/04/19	Sun 05/05/19	12
Final review and submission	4 days	Mon 06/05/19	Thu 09/05/19	14

3.2 Time-line Breakdown

Above is the schedule for this presentation (Landscape oriented for ease of insertion into the document). Because of space restraints, I decided to keep the descriptions of each task as concise as I could and then proceeded to list some of the entries below, with the intent to expand upon specific nodes with the method I intend to use to complete them.

1. Individual Project
    - This is the time dedicated for the entire project, including the Easter holiday season.
2. Initial Report
3. Initial Research into IoT specifications
    - As I have no prior knowledge on IoT as a general field and due to the fact that IoT devices run a range of different specifications, it will be necessary for me to first produce a specification sheet for the devices.
    - After I have done this, I can then start to look for documentation on details of the devices such as the protocols for communication, any firmware that is published (either fully open source or partially in cases such as GPL compliance), or debugging information.
4. First Look into potential exploits based on the IoT devices
    - This is when I will begin to look into specific exploits that are related to the devices (protocol weaknesses/known firmware exploits etc).
    - While this will be my primary research into exploits for use in the project, it is very possible that a vulnerability can be released (published or leaked) at any time and as such, it is possible that different vulnerabilities may be used instead of or in addition to the ones gathered at this stage.
5. Meeting with Supervisor - Discussion of Research
    - This will be the first major discussion with my supervisor and will target the usefulness of my research, the attack vectors I have chosen to exploit for each IoT device, and whether they are feasible in the time frame I have been given.
    - While I do not have prior experience in this area, my supervisor is currently studying a PhD in the field and because of this, this would be a good point for my supervisor to suggest any potential alterations to my project.
6. Develop prototype for one attack
7. Develop further prototypes for exploitation of vulnerabilities
8. Design a framework for automating exploits
    - When discussing the idea of a framework with my supervisor, two possible avenues were discussed.
    - The first is the idea of a framework system similar to the popular tool Metasploit, that would allow myself or others to create further exploit scripts that could all be controlled from one application.
    - The other possible alternative is closer to the research that my supervisor is working on and may be a smarter choice for me to take as my supervisor has prior experience. This idea is to create a tool that will look at the firmware of a device to look for potential vulnerabilities (a common route for exploits to take). While this is a great idea and would be a fantastic opportunity to produce, I have to consider the time-frame that I have to produce all my work and the report at the end of the project.

9. Meeting with Supervisor - Discussion of Exploits

    - In the second major meeting with my supervisor, I hope to be able to show proof of exploits that I have developed, along with my methodology for producing said exploits.
    - By this point I will have discussed with my supervisor the route that the automation tool will take, and a suitable design process for its development

10. Implement automation tool

11. Design and implement test cases

    - Since the tool will be designed to have full user input, I need to ensure that it is durable and will execute successfully on a consistent basis.

12. Draft report (Introduction, Background, Methodology)

13. Meeting with supervisor - Discussion of Report

    - In the final major meeting with my supervisor, I will have the draft of a report to show, along with reproducible tests for each of the exploited devices. I will discuss my personal thoughts on the outcome of the project, along with any progression that could be made given more time; and will ask for their opinion on what could be expanded upon.
    - Using this information, I will then go away and finish the report, stating both mine and my supervisors opinion on the future of the project.

14. Final report (Results and Conclusion)

15. Final review and submission