Initial Plan

Internet of Things
Security Penetration Testing

CM3203 - One Semester Individual Project - 40 Credits

Author: Maria Carolina Roberts
Supervisor: Dr Yulia Cherdantseva

School of Computer Science and Informatics
Cardiff University

2021

Contents

Description

The Internet has become extremely available in a short amount of time and the cost of connecting devices to the internet is decreasing. Wi-Fi capable devices and sensor costs are also decreasing, and smartphone penetration (usage rate) is increasing with more than four out of every ten people in the world currently equipped with a smartphone. This links into the implementation of Internet of Things (IoT) which refers to the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment. The use of IoT has increased rapidly in the past couple of years as consumers eagerly adopt these objects into their lives due to their attractive utility, features and simplicity. IoT, therefore, tends to attract the likes of hackers and cybercriminals since they are highly used and therefore would be valuable to attack. You could ask how much valuable data will a hacker get by infiltrating your home smart plug or lightbulb? But that point of entry can get them access to your home network, enabling them to steal private information like usernames and passwords, or even banking information, etc.

I will be looking at IoT smart home devices, more specifically the WeMo Wi-Fi Smart Plug which I will be purchasing as a personal item and will be using it for the project. Recently, vulnerabilities have been found with the plug with the WeMo plugs allowing hackers to possibly compromise entire networks with an unreported buffer overflow. Due to this, it can create a gateway for potential hackers to compromise an entire home Wi-Fi network and can become a malware target.

These vulnerabilities of IoT devices can be identified using penetration testing and during this project I plan to implement a systematic penetration test on the Smart Plug which I have chosen so that I can identify its weaknesses. Factors that significantly may amplify the chance of a successful attack include port protocols, product architecture, entry points, software versions, and Information about technologies. DNSMap, Network Mapper (Nmap), Arp-scan, SSLsplit are just some of the technologies that can achieve this. I then would analyse its vulnerabilities from this scan as vulnerability make the system prone to cyberattacks and this can be done with tools such as APT2, BruteXSS etc. Finally, sniffing and spoofing traffic would be the last step as understanding how specific hosts and devices communicate on a target network is critical for proper penetration testing which can be done with many tools such as Wireshark, DNSChef, MITMf etc.

This will allow me to able to suggest some improvements which can therefore, in future, keep the device safe and secure and to do this I will be using a machine running Kali Linux to implement the penetration test which I will run on my machine with the operating system downloaded using VirtualBox on my Windows system in order to achieve a virtual machine.

Overall, I hope to gain a greater understanding on security aspects of IoT devices and ethical hacking and have the opportunity to be able to help others in the future gain knowledge on the area by delivering a project which I would be happy to publish.

Project Aims and Objectives

For this section I will be talking about what I am setting out to achieve when completing my project.

- Background research on attacks.
    - Background research on different types of IoT attacks on the IoT devices, including case studies on the most relevant/interesting.
    - Specifications of the IoT devices to identify hardware or software issues.
    - This is in order to collate research surrounding different types of attacks into a concise manner which is easy for people so read and find.

Resulting in a section of the report which contains background information on the device and which attacks are most common amongst them.

- Implement attacks on the device.
    - Research some of the best penetration software used by hackers and pick the most appropriate for the smart plug.
    - Set up the device for penetration testing using an appropriate penetration software.
    - Design the attack and carefully plan out what vulnerabilities I will be targeting for full exploit.
    - Attempt to successfully compromise the device and find vulnerabilities.
    - This is in order to show how dangerous it can be to leave devices unprotected, showing that a hacker could gain access to their personal data with simple tools and knowledge.

Resulting in a section of the report which contains the main attack and how this was implemented (including all steps and justifications)

- Monitor network.
    - Understanding tools and some background research on the software.
    - Using sniffing and spoofing tools to assist in analysing the networks, their problems, and possible vulnerabilities in relation to the attack conducted on the device.
    - This is in order to show the use of intrusion detection systems to complement the attack that I have carried out.

Resulting in a section of the report which contains vulnerabilities detected using a software that detects intrusions.

- Conclude and recommend.
    - Research on the specific vulnerabilities found and how these can be made more secure.
    - This is in order to make sure the project has a clear section including ways that people can avoid their devices being hacked in order to help them in the future.

Overall, my project aims to show how common devices, which are used in many homes, can be vulnerable to attackers if they have the right tools and expertise and if the right security measures are not taken by the manufacturers and/or the individual buying the device. It is needed and important to make light of these situations using ethical hacking in order to avoid exploitation in the future. I will be meeting with my supervisor, Dr Yulia Cherdantseva, every 2 weeks for a longer meeting so that my progress can be monitored and to make sure that I am on track with my work.

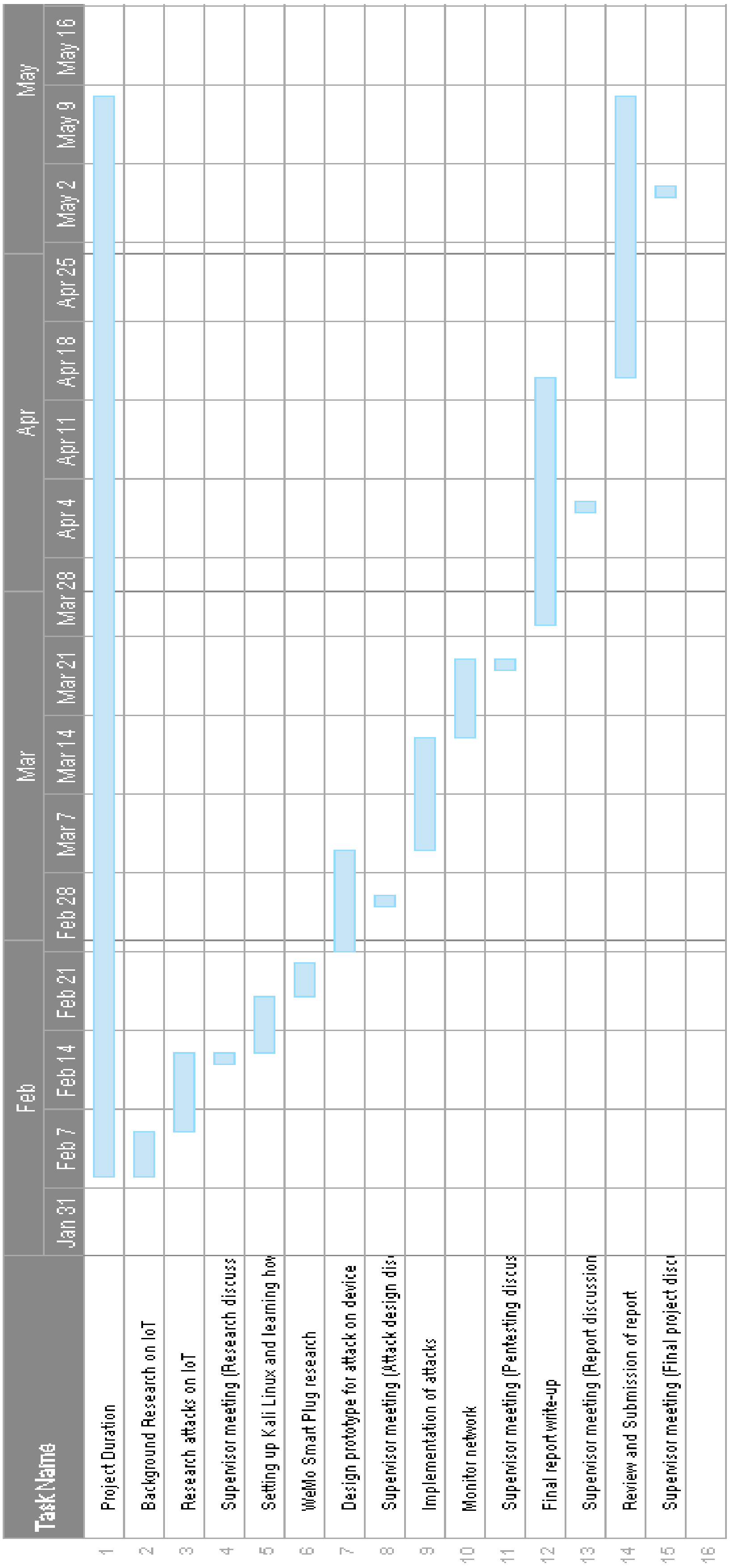
Work Plan

In this section I will be talking about the schedule I will be following in order to assess my progress. By splitting the weeks of the project up, I can keep track of milestones and be able to effectively sort out my time management throughout the project. Below I have listed some important milestones and I have included a Gantt chart to visually represent my schedule.

Milestones

- IoT attacks researched.
- WeMo Smart Plug researched
- Vulnerabilities found for WeMo Smart Plug using Pen Testing.
- Compromise the device.
- Sniffing and spoofing traffic
- Recommended improvements for security
- Final report draft
- Final report reviewing and proofreading.
- Submit final report.

Gantt Chart


Task Name
Feb
Mar
Apr
May
Jan 31
Feb 7
Feb 14
Feb 21
Feb 28
Mar 7
Mar 14
Mar 21
Mar 28
Apr 4
Apr 11
Apr 18
Apr 25
May 2
May 9
May 16
1 Project Duration
2 Background Research on IoT
3 Research attacks on IoT
4 Supervisor meeting (Research discuss
5 Setting up Kali Linux and learning hov
6 WeMo Smart Plug research
7 Design prototype for attack on device
8 Supervisor meeting (Attack design dis
9 Implementation of attacks
10 Monitor network
11 Supervisor meeting (Pentesting discus
12 Final report write-up
13 Supervisor meeting (Report discussion
14 Review and Submission of report
15 Supervisor meeting (Final project disc
16

Gantt Chart Timeline Explanation

Project duration

- I will be working on the main part of the project from the submission of the initial plan (08/02/2021) to the submission date of the final report (14/05/2021).
- This will allow me to have some time during the project for any unforeseen circumstances or commitments that I have listed.

Background research on IoT

- I will spend a few days researching IoT devices and common attacks on them, making notes for my final report as I go along.

Supervisor meeting

- Meeting with supervisor to discuss progress on research conducted.

Setting up Kali Linux and learning how to use tools.

- Self-learning by reading book on Kali Linux (Kali Linux Revealed) in order to understand tools and testing these tools out to get used to the software.

WeMo Smart Plug research

- A few days research on smart plug chosen and learning about previous exploits not only on this smart plug device (WeMo Smart Plug), but devices similar to it.

Design prototype for attacks on device

- Visual design for attacks I will be implementing, tools and hardware used, protocols used, networks used etc.

Supervisor meeting

- Meeting with supervisor to discuss progress on attacks research and design.

Implementation of attacks

- Conduct the attacks on the smart plug and write down what I have found and create a systematic methodology which I followed in order to include it in my final report.

Monitor network.

- Using sniffing and spoofing tools, monitor the network traffic of device.

Supervisor meeting

- Meeting with supervisor to discuss progress on the attacks I have conducted and what I have found so far.

Final report write-up

- Using all the information that I have collected during my project, create a report draft which may include an introduction, all the research I have found, the plan and design I have made, the methodologies that I followed to conduct the attacks, what I found when monitoring the network, my overall findings, my recommendations and any future work I would like to conduct, etc.

Supervisor meeting

- Meeting with supervisor to discuss how I am doing on my final report draft.

Review and submission of final report

- Proofreading and final touches on the final report and getting it ready for submission.

Supervisor meeting

- Meeting with supervisor to discuss the final reports final draft which I will send in advance of the deadline. After this meeting, take into consideration all feedback given by supervisor.

Other Commitments

Here I will mention any other commitments that I have that may hinder the timeline to a certain extent, such as examinations, group meetings, etc. Dates for these submissions and meetings are currently unknown but I will be able to factor them into my work plan accordingly when the information becomes available.

- CM3202: Emerging Technologies Portfolio
- CM3202: Emerging Technologies Group Meetings