Investigating Radio Frequency Vulnerabilities in IoT (Using a HackRF)

Initial Plan

Author: Sam Mantle
Supervisor: Eirini S Anthi
Moderator: Kirill Sidorov

Module Code: CM3203
Module Title: One Semester Individual Project
40 Credits

Project Description

The significant increase in Internet of Things (IoT) devices, which routinely collect sensitive information, is demonstrated by their prominence in our daily lives. Although such devices have simplified and automated every day tasks, they have also introduced tremendous security flaws. The insufficient security measures that are currently being employed to defend these smart devices make IoT the 'weakest' link to breaking into a secure infrastructure, and therefore an attractive target for cyber-attacks. This project will focus on investigating Radio Frequency vulnerabilities on IoT devices and mechanisms to defend against them.

Throughout the project I will be carrying out attacks against IoT devices while using a HackRF One from Great Scott Gadgets to capture and analyse the radio signals. The HackRF tool is a Software Defined Radio peripheral capable of transmission or reception of radio signals from 1 MHz to 6 GHz[1]. I will be testing a range of IoT devices which can be found in a typical smart household today, including (but not limited to):

- TP-Link NC200 WiFi Camera
- TP-Link HS100 UK WiFi Wall Plug Adapter
- Amazon Echo Dot
- Withings Bluetooth Blood Pressure Monitor

The aim of the project is to test the IoT devices against a variety of attacks while recording their radio frequency signals for any change. There are a range of attacks that can be done against WiFi and Bluetooth devices, and while more devices are becoming 'smart' devices, the attack surface also increases. I will investigate any existing known vulnerabilities with these devices and any exploits available for attacking these devices wirelessly. I will also carry out common attacks.

This project will aim to cover the opportunities to use the device's RF signals as a way to identify or "fingerprint" the devices, this could provide insight into automated RF based device scanning which is one of the first steps of reconnaissance (stage 1 of the cyber kill chain). Once we discover how the devices can be fingerprinted, a small program could be developed to use captured RF signals as a signature rule set for determining what device a given signal belongs to (in real-time, near real-time or by providing a capture as input).

The project will also explore what methods are possible for identifying the devices and comparing the potential advantages and disadvantages of these methods. Existing research in this field may exist and there are already many organisations using spectrum signatures of existing media to identify or classify an input media (such as Shazam[2]). I will investigate the opportunity to use methods that are yet to be introduced to the mainstream cyber-security field.

Various attacks while be carried out against these devices while analysing the RF signals for any changes and examine whether these changes are consistent during the same attack and how the signals change throughout different attacks. Depending on the results, it may be possible to identify an attack took place based on the RF signals and possibly categorise the attacks. If this can be done, there is an opportunity to create a system like an IDS (Intrusion Detection System) which can detect these attacks.

The reason behind investigating IoT Radio Frequencies in particular comes down to lack of focus in that particular area in general. Although RF based security research is becoming increasingly popular (especially in fields such as automotive security) there is still less focus in this area compared to other vulnerability research. A lot of research appears to focus on the hardware, firmware/software and network exploitation where attacks take place within the network or against publicly accessible or internet facing devices. These types of attacks are more common than pure RF based attacks which require the attacker to target the device directly using RF (such as replay attacks, signal jamming and deauthentication).

As more homes and organisations adopt smart devices into their ecosystem it increases their exposure and attack surface. This will eventually boost motive to use RF based attacks or any attacks which can be difficult to detect with typical IDSs (Intrusion Detection Systems) which are either heuristic or signature based. This is one reason for exploring the idea of fingerprinting devices and detecting attacks based on their RF signals within thie project. Identifying abnormalities or unexpected behaviour within RF activity and being able to identify attacks in the RF signals could improve attack detection, although this could also result in many false positives which will be investigated.

Project Aims and Objectives

Throughout this project I will be working towards the following objectives, aiming to answer these questions respectively:

Core Objectives:

1. Investigate what security issues and vulnerabilities currently pose a threat to IoT devices
   (a) Which ones relate to RF based attacks (such as sniffing, Deauthentication, Replay attacks, ultrasound 'silent' commands and DoS)
   (b) Which devices have known vulnerabilities? Do the test devices have known vulnerabilities?
2. Investigate whether we can identify or "fingerprint" devices based on their radio signals.
3. Investigate which methods are available for identifying these devices based on the RF signals.
   (a) Are there any unconventional methods or techniques not used in this industry but used elsewhere? (such as techniques used to identify music).
4. Attempt to carry out attacks on the devices. Both successful and unsuccessful attacks will provide valuable data which I will further analyse.
   (a) Are these attacks evident while analysing the radio signals? Are the differences consistent with every attack and are all the devices affected in a similar manner?
   (b) Attempt a variety of attacks including direct RF attacks without being connected to the same network.

Desirable Objectives:

1. Can we identify the attacks based on the RF signals and in what way can we classify these attacks? (such as aggregating based on specific device or detecting an attack which affects multiple devices in a similar manner)
   (a) Are there ways to detect these attacks in real time or prevent them? (Potential for RF based Intrusion Detection and Prevention Systems)

Work Plan:

Initial plan (Week 1):

- Initial meeting with supervisor
- Find out what devices I will be using
- Complete Initial Report

Deliverable: Initial Report.

Background Research (Weeks 1-3):

- Research background on IoT Communication technology and Security
- Read up on any existing research around 'fingerprinting' IoT devices
- Research any previous/existing RF based vulnerabilities, bugs and exploits.
- Research how to use the HackRF to capture Radio signals and analyse them

Deliverable: Background section of the report

Prepare Devices and Test Environment (Weeks 3 – 5):

- Setup devices, network, operating system (likely Kali Linux) and other software
- Due to sharing the devices they will likely stay on the IoT testbed in the Lab, if the opportunity arises to take a device home then appropriate network setup will be configured including a separate router for WIFI devices.
- Attempt to Isolate the device by switching other devices off, ensuring we avoid any background noise from other devices
- Potential for a faraday cage if I can acquire one.

Document Devices and Test Environment (Weeks 3 – 5):

- Document the hardware, software and environment/configuration I will be using during this project in the report.

Deliverable: Documentation for the devices and environment for approach section of the report

Research/Document Analysis Techniques (Weeks 5 – 6):

- Research ways to capture and analyse the radio signals
- This may include looking at methods and techniques used by other industries used for other types of application
- Research any previous material linked to analysing the same devices I will be using

Milestone 1: Research and preparation complete.
Deliverable: Complete approach section.

Initial RF Capture/Analysis (Weeks 6 – 7):

- Start capturing radio signals and analysing them
- Analysis can include comparing the results from the different devices and comparing them during normal usage.

Deliverable: RF Capture data, figures and results for the start of implementation

Device Fingerprinting/Identification (Weeks 7 – 9):

- Analyse the captured radio signals further to see if the devices can be fingerprinted/identified consistently and investigate how background noise may affect this.
- Depending in the results, create a small program (likely in python) to identify these devices in the area.
- The program will either record real time or take in a capture as input and output devices which match the signal.

Deliverable: Further results and conclusion from RF Analysis and a small program for identifying devices.

Attack Devices (Weeks 9 – 11):

- Use a variety of tools to carry out attacks against the devices and record the results.
- These attacks can either be exploits while on the same network as the device or direct RF based attacks targeting the device directly.

Analyse RF Signals from Attacks (Weeks 9 – 12):

- The attacking stage will overlap the analysis task as the attacks I decide to carry out may be influenced by the previous results.
- Analyse the results to determine how the devices are affected during an attack and whether we notice a difference in the radio signals.

Milestone 2: RF capture and analysis stages complete.

Finalise Attack Results and Conclusions (Weeks 12 – 15):

- Document these results in the report and come up with a conclusion.

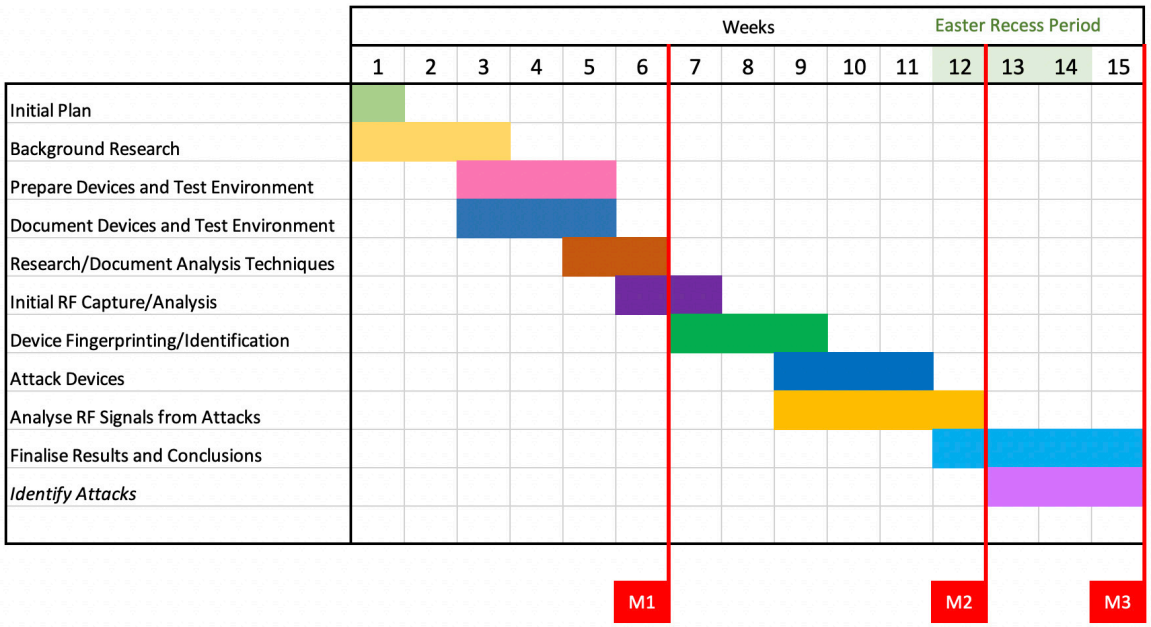
Deliverable: Results and conclusion from RF Analysis during attacks for results section.

Identify Attacks (Weeks 13 – 15) *Desirable Objective*:

- A desirable task at the end depending on time frame
- Attempt to identify types of attacks against the devices
- This may include creating a small program similar to the one mentioned previously where we attempt to identify an attack against devices where rules will determine whether a radio signal pattern matches an attack.
- Given a capture over a period of time, attempt to analyse evidence of an attack. Even if this cannot be automated during the project time frame it would be useful to have the documentation and knowledge to be able to analyse the radio signals and determine whether an attack likely took place.

Milestone 3: Project Complete
Deliverable: Final Report Complete.

Gantt Chart:



Ethics

After checking the University's Ethical Approval guide[3] and discussing with my supervisor I will not need ethical approval for this project as I will not be collecting data from other people. These devices will remain in a secure confined environment (in the IoT lab or my own isolated network) and any processes involving my own participation does not involve sensitive or personal data. This includes situations such as sending voice commands to Amazon Alexa. Any demonstrations or other practical activity with the devices will be done without using, collecting or processing personal or sensitive data.

References

[1] Great Scott Gadgets. *HackRF One*. URL: `https://greatscottgadgets.com/hackrf/` (visited on 01/02/2019).

[2] Shazam. *Company - Shazam*. URL: `https://www.shazam.com/gb/company` (visited on 01/02/2019).

[3] *Computer Science and Informatics Ethics*. URL: `https://www.cs.cf.ac.uk/ethics/` (visited on 01/02/2019).