Initial Plan - Can IoT Devices be Identified Through Their Device Fingerprint?

Author: Rachel Keyte
Supervisor: George Theodorakopoulos
Module number: CM3203
Module title: One Semester Individual Project
Credits: 40

Contents Page

Project Description

Internet of Things (IoT) devices are becoming increasingly common with the demand for efficiency, accuracy and cost saving whilst reducing the need for human involvement of everyday processes. The overall aim of IoT devices is to have the physical objects around us connected to the internet and controllable remotely. Some examples of IoT devices can include light bulbs, fridges, cameras, insulin pumps and smart meters.

However these new devices have brought about many security risks which can range from attackers being able to turn your lights on and off to being able to spy into your home; moving security risks from online threats to physical ones.

In this project I will be looking into the possibility of determining a device type fingerprint for various IoT devices using a Wifi Pineapple.
The WiFi Pineapple is an access point that can be used to capture network traffic and execute various network attacks as it was originally created for penetration testing. Its capabilities will allow me to intercept the network activity of the IoT devices by exploiting the automatic connections to known access points specified by SSID.
A device type fingerprint will take into account multiple different factors to determine the type of device with some level of certainty. It will involve recording factors such as the transmission rate and how much data is transmitted over a network.

Once I have collected information from the devices available in the IoT lab at the university I will use the data to create a classification/ clustering algorithm.
Following this, I will aim to perform 'blind attacks' where I intercept an unknown device from the ones I have previous data for and using the classification/ clustering algorithm, determine what type of device was intercepted.

The significance of knowing the device type can have potential positive and negative impacts.
From a company's perspective, they may want to see what devices they have connected to their network to help detect unauthorised access.
From the perspective of an individual, concerns are that a Wifi Pineapple could be used to 'check' people's homes. If it can be concluded that this house has an expensive IoT device such as a smart TV then it may result in people's homes being burgled. Furthermore there have been cases of people hacking into baby monitors and being able to view the room and speak through the device.
In terms of the medical field the functionality of determining a device type may be useful if a patient is unable to communicate. The medical professionals will be able to determine if the patient has a device such as a pace maker or insulin pump.

Project Aims and Objectives

Core Objectives:

- Research areas of vulnerability in IoT device security, previous research into device fingerprinting that has been done and the WiFi Pineapple.
- Intercept IoT devices using the WiFi Pineapple.
    - Perform man in the middle attacks on different IoT devices in the IoT lab.
- Discover whether device type fingerprints for certain IoT devices can be determined with the use of a WiFi Pineapple.
    - Collect data that will be useful in determining the device type fingerprint.
    - Create a suitable classification algorithm.
- Discover whether the type of IoT device can be determined without prior knowledge of what type of device it is.
    - Perform 'blind attacks' when the device is unknown and determine what it is using the algorithm

Desirable Objectives:

- Discuss how any vulnerabilities can be mitigated or prevented.

Work Plan

I have created a work plan to outline the tasks that I aim to achieve each week and the deliverables for them. I have also included the key review meetings however it is likely that additional meetings will be required on a more regular basis.

WEEK 1 29th Jan - 2nd Feb

Write initial plan for the project detailing the work plan, aims and objectives and project description.

Initial meeting with supervisor to discuss the project and clarify aims/ objectives.

Some initial research.

Deliverable: Initial Plan.

WEEK 2 5th Feb - 9th Feb

Background research:

- IoT device security.
- Previous research.
- Machine learning
    - Common classification algorithms used.
- Wifi Pineapple:

- How it works.
- What its used for

WEEK 3 — 12th Feb - 16th Feb

Continue background research.

Milestones: Research finished

Deliverables: Introduction and background sections of the report.

WEEK 4 — 19th Feb - 23rd Feb

Decide on an approach to the problem (how I will intercept, extract and compare the information I need)

- Compare solutions already available.
- Describe what my approach will be.
- Explain why I have chosen the approach.
- What information will be extracted.

Perform initial attacks - intercept some IoT devices using the Wifi Pineapple to practise collecting data, and become confident using the Wifi Pineapple.

Adjust the approach if necessary.

WEEK 5 — 26th Feb - 2nd Mar

Continue performing initial attacks.

Complete the approach section in the report.

Review meeting.

Milestones: First review meeting.

Deliverable: Approach section of report.

WEEK 6 — 5th Mar - 9th Mar

Perform more attacks on different devices to collect some IoT data.

- Locate and record the information that will constitute the device type fingerprint.

WEEK 7 — 12th Mar - 16th Mar

Continue performing attacks to collect data and extracting device fingerprint information.

Milestone: Device information collected from multiple IoT devices.

Deliverable: Collected data.

WEEK 8 — 19th Mar - 23rd Mar

Design a classification algorithm.

- Find an appropriate way to classify the data by device type taking into account all the variables that will make up the device type fingerprint.

WEEK 9 — 26th Mar - 30th Mar

Build the algorithm to determine the device type.

WEEK 10 — 2nd Apr - 6th Apr

Continue building the algorithm.

Start to test the algorithm with some of the data that I collected (training data).

WEEK 11 — 9th Apr - 13th Apr

Complete final tests on algorithm with the remaining unseen test data and alterations made.

Milestone: Algorithm completed

Deliverable: Functional classification algorithm

WEEK 12 — 16th Apr - 20th Apr

Design Section:

- Requirements
- Description of solution
- Justification

Build Section

Test Section:

- Does it meet requirements

Deliverables: Design, build and test sections in the report completed.

WEEK 13 — 23rd Apr - 27th Apr

Perform attacks on unseen devices and determine what they are just on information extracted and using the algorithm to classify them.

Results

- Findings from classification of unknown devices

Milestone: 'Blind attacks' completed

Deliverable: Results section.

WEEK 14 30th Apr - 4th May

Evaluation

- How the project has addressed the problem
- Why I chose to do the project in this way
- Functional fulfilment
- Strengths and Weaknesses of the project

Future Work

- How I would continue to work on the project
- Potential future improvements
- How to further develop the solution

Reflection

- Why I initially decided to do this area
- Changes made
- Challenges faced
- Personal reflection
- How happy I am with the results/ project in general

Final review meeting.

Deliverables: Evaluation, future work and reflection sections.

Milestone: Final review meeting

WEEK 15 7th May - 11th May

Conclusion

- The significance of the findings and their impact.

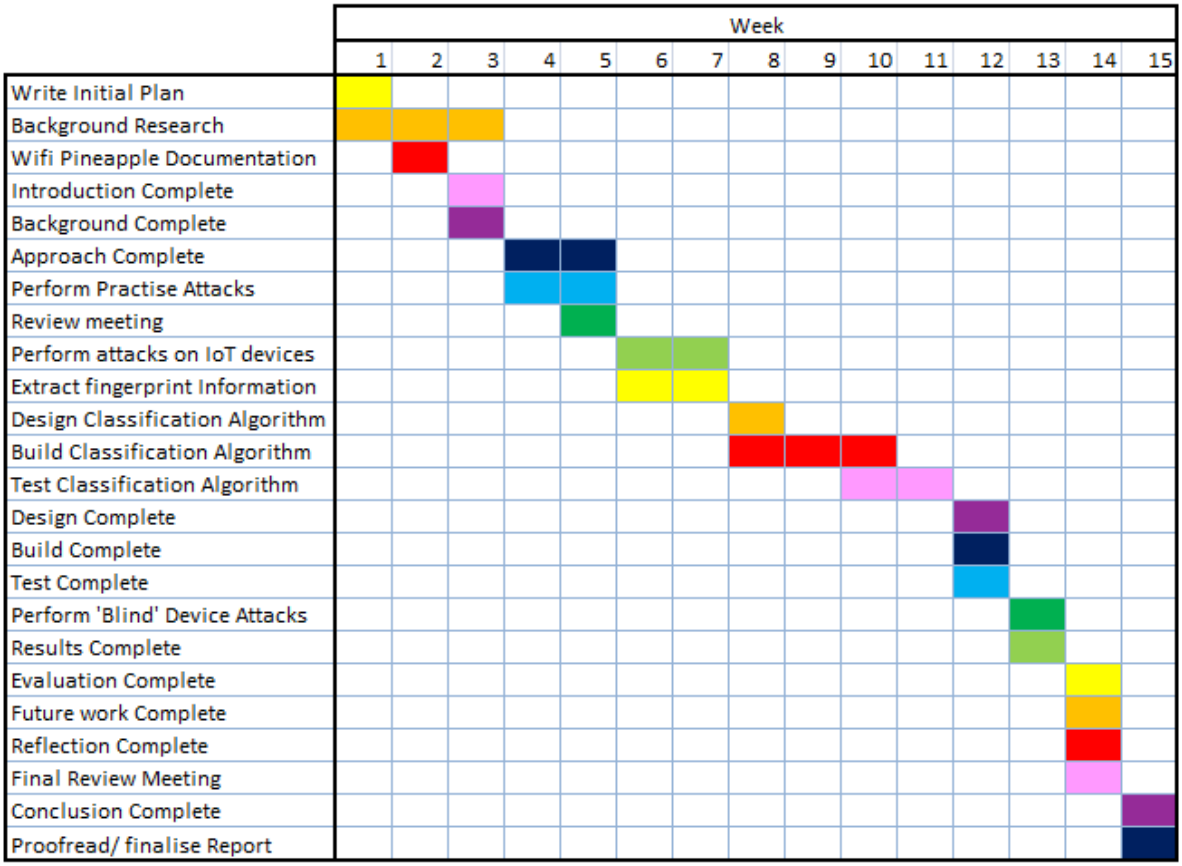
Proofread and finalise the project.

Deadline 11/05/2018 - upload final report

Deliverables: Conclusion section and final report.

Milestones: Final report completed.

Gantt Chart



Ethical Approval

Having consulted the ethical approval guide [1], I have ensured that there are no ethical problems with the research for the project and do not need to seek approval of the ethics board in order to complete this project. This is because I am not accessing any sensitive data and the devices are confined to the Cardiff University IoT lab.

References

[1] Cardiff University. *Computer Science and Informatics Ethics* [Online]. Available at: https://www.cs.cf.ac.uk/ethics/ [Accessed: Jan. 31st, 2018].

[2] N. Dhanjani. 2015. *Abusing the Internet of Things*. O'Reilly.

[3] Hak5. 2018. *WiFi Pineapple - Home* [Online]. San Francisco. Available at: https://www.wifipineapple.com/ [Accessed: 02 February 2018].