.

Cardiff University

School of Computer Science and Informatics

CM3203 - One Semester Individual Project

Initial Plan – IoT Security

Author: Peter Ghawi

Date Due: 3rd February 2020 at 23:00
Module Leader: Frank C Langbein
Supervisor: Philipp Reinecke
Moderator: Richard Booth
Credits Due: 40

Academic Year: *2019/20*

Description

When discussing the Internet of Things it encapsulates the billions of physical devices connected to the internet collecting and sharing data around the world. Due to affordable processors and wireless connection capabilities, it has become possible to modify practically anything, from a pill that notifies medical patients to take their medication, to aeroplanes that produce data to predict maintenance requirements or improve flight and fuel efficiency. This adds a level of digital intelligence to any device, enabling the device to communicate real-time data without any human interaction. However, although these devices ease the daily life of the user, they come with irrefutable security risks, which make them vulnerable to a array of cyber-attacks. This project will focus on designing and implementing attacks against an IoT device provided by the university, followed by emulating network traffic to seem as an attack to evaluate the effectiveness of various types of IDS. An Intrusion Detection System is a software application or hardware that monitors traffic on networks in search of suspicious activity and known threats. Alerting information includes information about the source of the intrusion, the target address and type of attack that is suspected.

Aims and Objectives

This section will illustrate the main aims and objectives of the proposed project throughout the project timeframe.

1. To describe and justify the use of a series of attacks on the TP-Link Cloud Camera.
    - Setup IoT device and required environment for pen-testing.
    - Produce a datasheet for the device listing camera, video, audio, etc. specifications.
    - Research common vulnerabilities published for IoT devices then specifically for the device provided and other camera IoT devices.
    - Search for previous exploits that have been published for the device and what the attacker could have achieved after the exploit was successful.

The result of this aim will be a report containing the most vital information collected during the process.

2. Attempt the attack with the highest probability of success to exploit the device.
    - Produce a list of possible attacks and which of these attacks have the highest probability of success.
    - Devise a method to compromise the device.
    - Implement the method to attempt compromising the device.

The result of this aim will be a report outlining the tools and steps taken to implement the potential attack on the device.

3. Inject attack symptoms into the network and see if an IDS (Intrusion Detection System) can detect them.
    - Monitor the network to understand how the traffic is shown during an attack.
    - Write a module to emulate the traffic of an actual attack in an IDS.

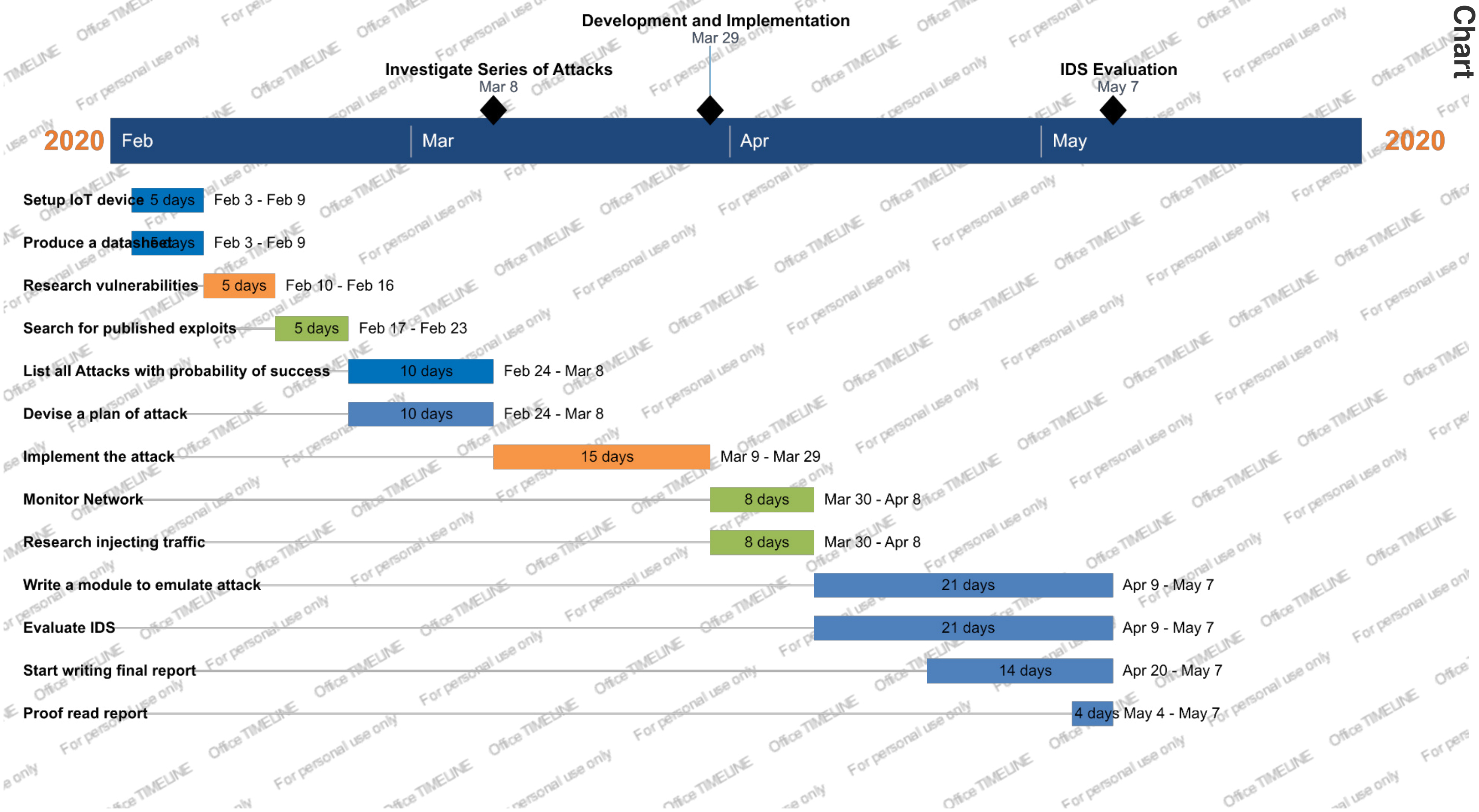
A meeting with the supervisor will be taking place every week to discuss the project’s progress.

Risk Assessment

Risk	Risk Level	Likelihood of event	Solution
Data loss	High	Somewhat Likely	Have multiple backups of the project stored which are updated at each step of the project.
Falling behind on the work plan	Medium	Somewhat Likely	Start tasks according to the Gantt Chart and provide time in the following week to finish any tasks left over in case of falling behind.
Hardware failure	Medium	Unlikely	Ensure similar device are available in the case of failure.
Illness	Low	Somewhat Likely	Make sure that tasks are given enough time to be complete and make them spaced out enough so that in the event of falling behind schedule tasks are still manageable.

Gantt Chart

IoT Security


Development and Implementation
Mar 29
Investigate Series of Attacks
Mar 8
IDS Evaluation
May 7
Feb
Mar
Apr
May
Setup IoT device
5 days
Feb 3 - Feb 9
Produce a datasheet
5 days
Feb 3 - Feb 9
Research vulnerabilities
5 days
Feb 10 - Feb 16
Search for published exploits
5 days
Feb 17 - Feb 23
List all Attacks with probability of success
10 days
Feb 24 - Mar 8
Devise a plan of attack
10 days
Feb 24 - Mar 8
Implement the attack
15 days
Mar 9 - Mar 29
Monitor Network
8 days
Mar 30 - Apr 8
Research injecting traffic
8 days
Mar 30 - Apr 8
Write a module to emulate attack
21 days
Apr 9 - May 7
Evaluate IDS
21 days
Apr 9 - May 7
Start writing final report
14 days
Apr 20 - May 7
Proof read report
4 days
May 4 - May 7