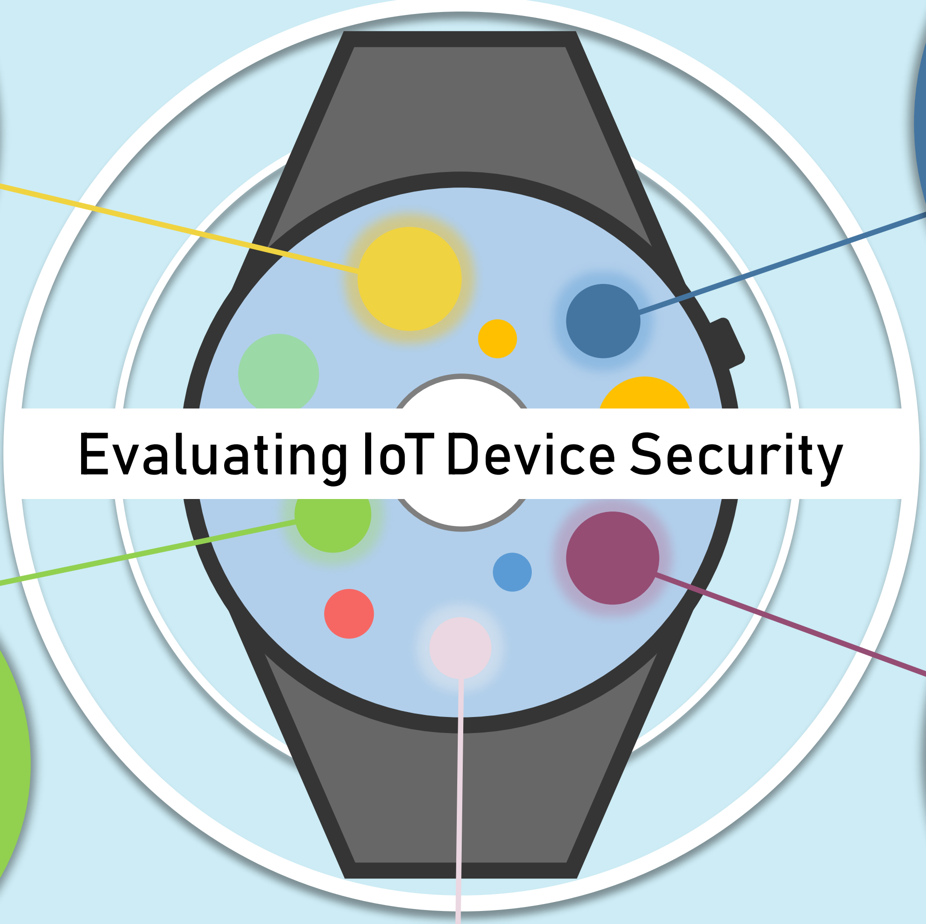
2nd Marker
Naghmeh
Moradpoor

Student
Fraser
Dumayne

Supervisor
Liam
Bell

Evaluating IoT Device Security



Introduction

The Internet of Things is an increasingly relevant concept in the computing world in which non-smart objects can become intelligent through the addition of devices which help them connect to the Internet. These 'things' can then be used to perform every day tasks and enhance productivity. Unfortunately, the enhancement of these devices can cause them to become vulnerable to attacks.

Objectives

Security is a huge weakness in IoT device manufacturing as cheap components and vulnerable software are used to keep costs low. The objective of the investigation was to perform device analysis to prove how insecure IoT devices can be and how easily they can be hacked.

Methodology

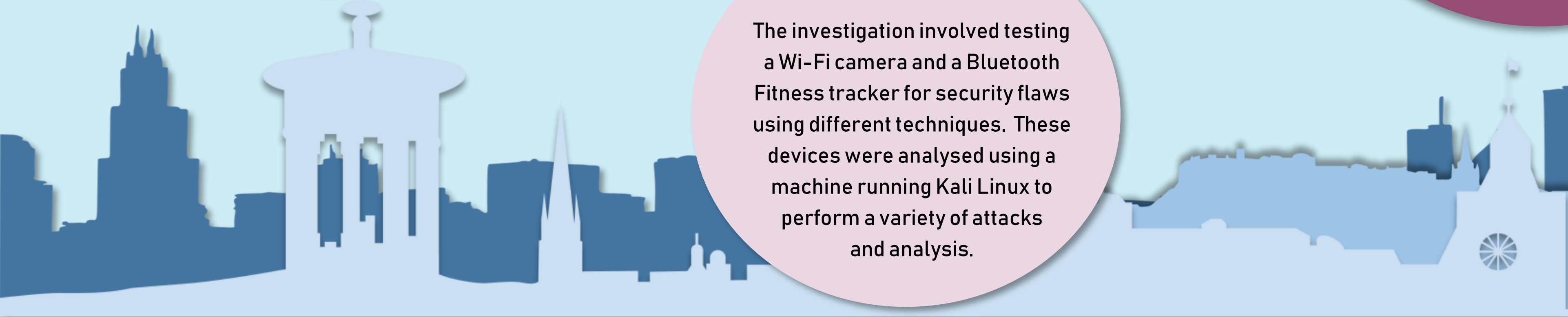
The investigation involved testing a Wi-Fi camera and a Bluetooth Fitness tracker for security flaws using different techniques. These devices were analysed using a machine running Kali Linux to perform a variety of attacks and analysis.

Results

Several vulnerabilities were found in the Wi-Fi camera including missing web application encryption causing openly available credentials, and a weak setup process potentially allowing attackers to gain control of the device, The Bluetooth fitness tracker maintained a solid foundation in terms of security as the device paired with the mobile application and denied further communications despite several attack attempts.

Further Work

The Internet of Things is a huge area in computing and therefore the work could be enhanced by taking on a larger sample size of devices with varying protocols to understand what the most frequently occurring vulnerabilities are and how manufacturers may be trying to solve them.



Edinburgh Napier
UNIVERSITY