Internet of Things (IoT) Penetration Testing Toolset

Sarunas Iljeitis (si1g16)

Supervised by Dr Julian Rathke (jr2)

1. Problem:

Nowadays people tend to use more and more low-end consumer-based electronics. Such sensor based or smart-devices are used to create highly automated networks (IoT networks) that assist humans in performing various tasks. Unfortunately, product manufacturers are driven by ever-increasing demand for highly functional affordable gadgets, because of that security is usually not their top priority. The current IoT gadget market is filled with low-quality inexpensive devices that implement poor security standards. Some security vulnerabilities could be easily prevented by device users simply following mutual security standards guidelines. As consumers are usually negligent to properly secure their new gadgets and device manufacturers are more concerned about minimizing the production cost such devices become favorable targets for attackers wishing to compromise owner's network.

2. Goal:

Penetration testing is an essential aspect of any modern device, application or network development. It is the single most effective way of finding security breaches before the actual attack happens. The goal of this project is to provide a set of tools that can be automatically applied to IoT networks or individual devices to scan for common IoT vulnerabilities. The toolset is intended to be used to find vulnerable devices which use different communication methods, apply customizable vulnerability tests and provide test results in a report. The toolset would follow most common IoT device testing methodology and vulnerability testing best practice.

3. Scope:

This project cannot possibly find all existing IoT device vulnerabilities nor address specific device level implementation details; thus, it will only check for most frequent IoT device weak points. The toolset will concentrate on testing mutual device properties providing a certain level of configuration for different tests following common testing patterns. It will not however be able to expand over bigger IoT infrastructures as it concentrates on testing singular devices or a small set of devices on the same network.