

Coursework Title: Artefacts (AS2) Securing ‘things’ in a network

Feedback Method: via Email and Canvas

Programmes: Computer Security, Computing and Information Systems, Policing and Cybercrime

Introduction

The Internet of Things (IoT) is not a new paradigm; the technological capabilities of society have enabled its immense progression and increased utilisation. Increasingly, there are applications of these varying Internet-enabled ‘things’ in everyday life including automation of many day-to-day operations, healthcare, data analytics, smart buildings, and wearable technology. Worryingly, with IoT devices, practically anything can be connected to the Internet or to another ‘thing’– in many instances we are creating our own problems and a larger attack surface with inherent underlying security issues. For security, “one size fits all” does not work for the complex IoT ecosystem - interoperability issues are important. Secure by Design, Default and in Deployment is imperative in future implementations of such interconnected ‘things’.

You are introducing a new smart device into your network but want to ensure the current network has no vulnerabilities. You are to design and implement a security application to find out information about the network that may be useful for an attacker, and then create a security policy for the network. Device security, network security and introducing future ‘things’ should be considered.

Learning Outcome to be assessed

1. Critically evaluate a complex computer security problem.
2. Apply complex skills relating to security techniques and tools to secure a computer system.

Details of the task

Part 1: Implementation

In order to assess the viability of the network in its current form, create a program (in Java) that comprises the following functionality:

- Allows the user to scan for devices on the network
- Identifies port information and socket information (e.g. domain, type, protocol, hostname)
- Saves all information to a file that is encrypted/decrypted with a password
- Include guidance for user of the program

Part 2: Design

- Detail your design and implementation choices including encryption method used
- Consider ways upon which your tool could be extended to include further features

Part 3: Security policy

- A Security policy is a statement that partitions the states of a system into a set of authorized or secure states and a set of unauthorized or non-secure states. Now that you have created a program that can find out network information, create a security policy to ensure the network information found by the program are secure, and also focus on ensuring future 'things' being introduced into the network are secure.

Marking Scheme/Assessment Criteria

Assessment Criteria	% Weighting for each problem part
Implementation	45
Scan for devices on the network	10
Identified port and socket information	10
Saves all information to a file that is encrypted/decrypted with a password	10
Demonstration of program	10
Guidance for user of the program	5
Rationale	25
Design and implementation choices	20
Further work	5
Security Policy	30
Device security	10

Network security	10
Future 'things'	10
Total	100

What you should hand in:

Submission via Canvas. Please submit a single .ZIP file containing all the code, the report and an executable version of your application (**convert .jar file to an executable version for windows: .exe file**).

Recommended reading

Reading list is on Canvas.