Appendix D:

IoT Vulnerabilities

1 Introduction

There are an estimated 31 billion devices currently in use. As these devices are being adopted in all aspects of life - from home devices, medical devices, industrial devices - there are valid concerns raised about the security capabilities of these devices.

2 IoT Device Resources

Internet of Things devices are typically low-power devices and sensors. These devices are network connected, and often interact with a users personal information. As an affect of the low power resources used on these devices, the devices critical functions take precedence in terms of memory or processing performance. This leaves little availability in terms of available resources for aspects such as security.

3 OS Security Features

Non-resource constrained, "fully fledged" operating systems which run on consumer PCs and enterprise server hardware have a number of security features which can be implemented to protect against attack. These range from firewall and packet filtering software, to firmware verification software.

3.1 UEFI Secure Boot

Secure boot is a security mechanism used to verify that software being run on a system is from a trusted source. The vendors whose software has been granted permission to run on the system are stored in firmware. This allows for any software being loaded onto the device at boot time can be verified by comparing the vendor signature agains the keys which are stored in firmware.

Secure boot is compatible with the x64 platform, and is enabled by defautl on Windows and most Linux distributions.

3.2 IPtables

4 Conclusion