Abstract

The Internet of things is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. This being said, IoT is the next big thing that will change the way we communicate and exchange data. Every day thousands of IoT devices are coming into the market. Most of these devices collect and exchange data over the cloud. Not much effort has been put into securing the IoT devices, thus understanding the security of IoT devices and their communication is of utmost importance.

If one has a close look at any IoT Network, there are many components to be secured. Some of them are listed below –

- Network
- Radio and wireless communication
- Embedded applications and web services
- Mobile (Android & Ios)
- Cloud, API
- Firmware (UEFI,bootloader,filesystem)
- Hardware (chips,eproms,uart pins,connectors,RTM modules,uart cables)

For the scope of this project we will be covering firmware analysis and fuzzing of binaries for vulnerabilities. Firmware is a software program programmed on a hardware device. It provides the necessary instructions on how the device communicates with the other computer hardware.

Firmware

The following firmware’s would be analysed for the scope of this project:

- Damn Vulnerable Router Firmware
- IoTGoat
- DLink WiFi Day & Night DCS - 932L Camera Firmware

Proposed Methodology

Sr. No	Test Case	Description
1	Information gathering and reconnaissance	Acquire all relative technical and documentation details pertaining to the target device's firmware
2	Obtaining firmware	Attain firmware using one or more of the proposed methods listed
3	Analyzing firmware	Examine the target firmware's characteristics
4	Extracting the filesystem	Carve filesystem contents from the target firmware
5	Analyzing filesystem contents	Statically analyze extracted filesystem configuration files and binaries for vulnerabilities
6	Emulating firmware	Emulate firmware files and components
7	Dynamic analysis	Perform dynamic security testing against firmware and application interfaces
8	Runtime analysis	Analyze compiled binaries during device runtime
9	Binary Exploitation	Exploit identified vulnerabilities discovered in previous stages to attain root and/or code execution

Referenced from: https://owasp.org/www-project-internet-of-things/