FIRMALYZER

Automated bare-metal and monolithic firmware security analysis for IoT devices

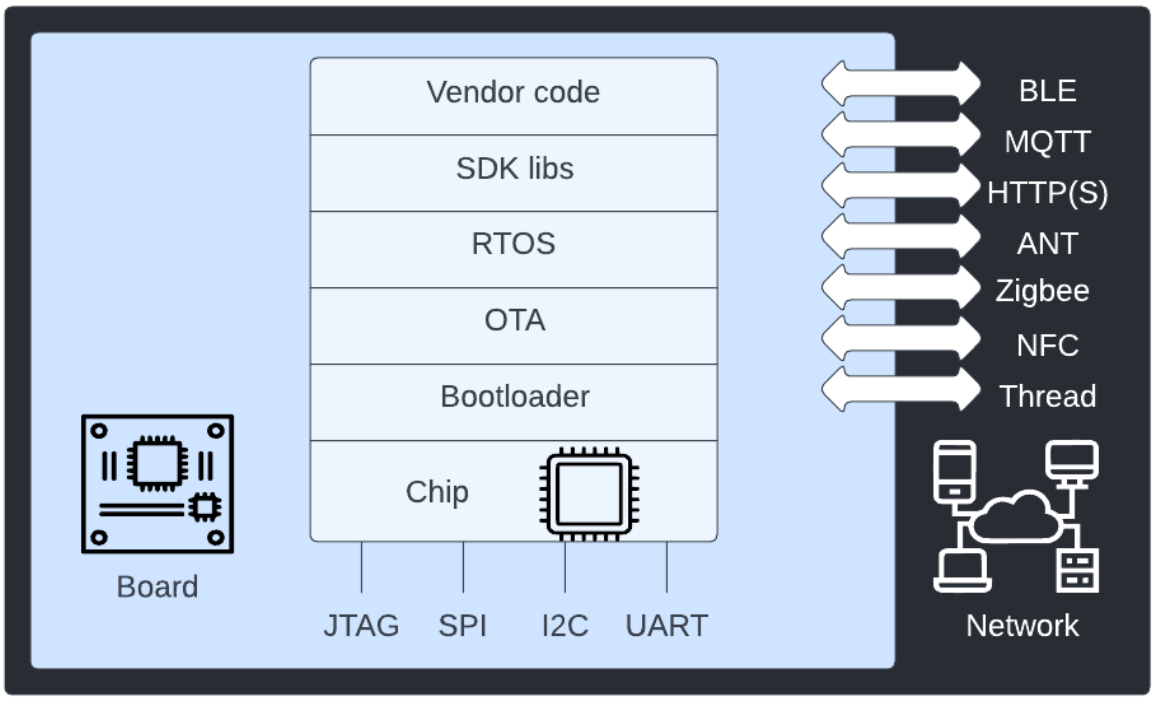
THE CHALLENGE

General purpose Linux is currently still the dominant operating system used in IoT devices, with 22% market share in 2017, but this trend is currently shifting towards use of embedded OS and monolithic firmware specially in low power devices in which the application directly runs on the hardware without an operating system. A number of open-source tools have been published to facilitate manual static analysis of non-Linux embedded firmware specifically for automating the annotation of memory-mapped peripherals in the disassembled binary code. These tools are intended for IoT security researchers with intermediate level knowledge of an ARM architecture and binary reverse engineering in manual code audit engagements. Determining the attack surface of the target firmware binary and discovering vulnerabilities targeting those vectors are still manual and expensive tasks that are not scalable for an IoT device vendor with multiple product lines.

FIRMALYZER FIRMWARE SECURITY ANALYSIS ENGINE

Firmalyzer analysis engine for bare-metal and monolithic firmwares enables device manufacturers and security testing labs to perform automated security analysis without access to the firmware source code. With a combination of static code analysis and targeted code emulation, Firmalyzer can discover the following classes of vulnerabilities:

- *Insecure use of vendor SDK APIs such as Bluetooth Low Energy functions*
- *Potential memory corruption vulnerabilities such as buffer overflows, out-of-bounds read and writes and format string bugs*
- *Integer overflow and underflow issues*
- *Use after free and double free vulnerabilities*
- *Insecure use of cryptographic algorithms*
- *Insecure privileged mode services*
- *Disabled SoC/MCU security features such as secure-debug and secure-boot*
- *Outdated vendor SDK or RTOS*



Attack surfaces analyzed by Firmalyzer

CONTACT DETAILS

Web: *https://firmalyzer.com/*
Email: *contact@firmalyzer.com*
Address: *Brusselstraat 51 2018 Antwerp Belgium*