Come Join the CAFSA - Continuous Automated Firmware Security Analysis

Collin Mulliner
August 2019

Modern devices are complex and their firmware often consists of multiple parts that together make up the software stack of the final product. Securing firmware is hard work since firmware changes over time and engineering focus shifts to different aspects like prototyping, development, testing, and finally production. Shipping 'bad' firmware can have a ripple effect on the entire product line and infrastructure, possibly preventing security controls from being properly implemented, potentially costing millions due to recalls. Preventing this ripple effect will ultimately save you money and keep your product reputation intact.

This project is about processes and tools that we designed, built, and deployed in the last couple of years while working on securing devices at multiple companies, most notably in my current role at Cruise Automation. We determined that well engineered simple, yet powerful, processes integrated into the development and release flow can achieve great victories.

Our approach is centered around FwAnalyzer, a tool for analyzing firmware images, specifically filesystem images. The tool provides an automated way to model and check the security properties of files and file content. Checks can be as simple as flagging suid executables or world writable files and as complex as ensuring that a release build contains production CAs signed with production keys. Our approach is vastly different and more impactful compared with traditional tools such as vulnerability scanners, that try to identify insecure code or artifacts, based on CVEs within in your software stack.

One core component of the process deals with reporting and further processing of information extracted and gathered during the analysis and checking phase. All steps generate machine readable reports that allow integration in continuous development environments as well as extending the process and tools to new targets. We open sourced FwAnalyzer together with a library of checks for various targets.

FwAnalyzer

The source for FwAnalyzer, supporting scripts, and examples are available on GitHub:

http://fwanalyzer.io