Rajat Sethi

CPSC 8580

**Paper Summary 8 - FIRM-AFL: High-Throughput Greybox Fuzzing of IoT Firmware  
via Augmented Process Emulation**

Fuzzing is the act of inputting random values into a system to determine its behavior. This especially includes error-inducing behavior, which could reveal overly specific error messages, and unintended behavior, which could reveal vulnerabilities. In this paper, the research team developed a form of greybox-fuzzing, a lightweight testing methodology, to find exploits in IoT systems.

The main novelty of this paper is Firm-AFL, their greybox-fuzzer. Using *Augmented Process Emulation* to simulate a kernel-mode and user-mode emulation, the team was able to simulate an IoT firmware. In addition, the team was also able to emulate memory address and paging tables to analyze the firmware attacks on a low-level. Using this emulation, Firm-AFL tested several inputs and system calls to find a number of 0-day and 1-day vulnerabilities. Also, these vulnerabilities were found quite quickly, with the throughput reaching 8.2x times faster at finding 1-day vulnerabilities.

One of the main weaknesses of this paper is their unrestricted and unexplained use of jargon. In several sections, the researchers would drop acronyms and terminologies, but not explain what they were or what relation it had with the research project. This was especially a problem when they were introducing QEMU, a commonly used fast processor emulator. The paragraph was filled with OS terminology and there was very little mention of Firm-AFL, their contribution. In future works, I would hope that the research team pays more attention to the quality of their writing.

As mentioned in the “Discussion” section, there were two main points of improvement. First, Firm-ALF only works on MIPS and ARM-based architectures. More research needs to be done for the project to work on other architectures. In addition, more work must be done to support other IoT firmware. Currently, Firm-AFL works on primarily Linux-based systems. Supporting other operating systems and IoT firmware could take a large quantity of resources and time.