Automated Emulation of IoT Device Firmware

Christian Kudera, Sebastian Dietz, Georg Merzdovnik

COMET
Competence Centers for Excellent Technologies
www.ffg.at/comet

SBA Research

Background & Motivation

Security in the IoT Ecosystem

Achieving security in the IoT ecosystem is a challenging task. According to Kaspersky [1], over 100 million attacks against the IoT were identified in the first half of 2019.

Compromised IoT devices are misused for:

- Distributed denial-of-service (DDoS) attacks
- Spamming and cryptocurrency mining
- Proxy agents or VPN pools

Problems

- The IoT market is rapidly growing, whereby the devices are characterized by heterogeneity due to different architectures and protocols [2].
- The emulation of IoT devices is rather limited, especially if the firmware doesn't contain a Linux operating system [3].
- Due to the lack of suitable tools, the security analysis of IoT devices is challenging, time consuming, and not well supported [4, 5].

Need: Framework that automatically builds emulated IoT devices from firmware samples without any further knowledge.

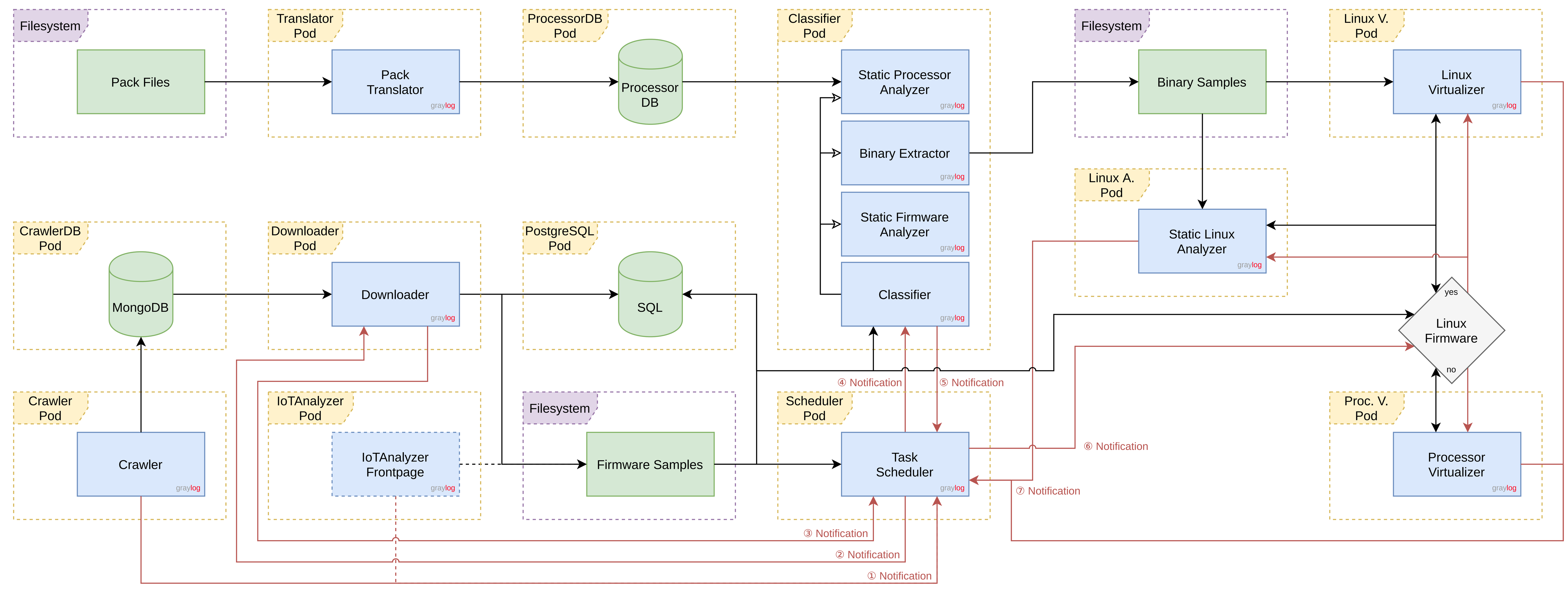

Figure 1: Automated Emulation of IoT Device Firmware Architecture

Methodology

Figure 1 illustrates the architecture of the framework and its corresponding components:

- **Crawler & Downloader**: The Internet is constantly monitored for new firmware samples. Identified samples are downloaded for an analysis.
- **Task Scheduler:** Coordinates the tasks for all components, with all intermediate results being stored in a database.
- **Classifier:** Classifies the samples and extracts as much information as possible through a modular approach. For example, the *Static Processor Analyzer* uses previously gained knowledge about different processors (e.g., base address, memory size) to determine the processor family and peripherals.
- **Processor & Linux Virtualizer:** Uses the knowledge gained from the classifier to create suitable virtualization instances. Lacking knowledge is complemented through dynamic analyses (e.g., identifying appropriate processors and peripherals).
- **Static Linux Analyzer:** Extracts additional knowledge from the Linux file system (e.g., installed software, password hashes).
- **IoT Analyzer Frontpage:** In the future, we will provide a website, where firmware samples can be uploaded. The firmware sample will be analyzed and the uploader receives a report.

Outlook

IoT Firmware Fuzzing & Symbolic Execution

- Dynamically probe the firmware for security issues
- Analyze the behaviour of the firmware in different scenarios

IoT Honeypots

- Collect IoT-relevant malicious empirical data
- Formulate IoT-centric attack signatures
- Generate IoT-specific technical threat intelligence

IoT Device Characteristics Database

- Manufacturer name and device model
- Open ports and running services
- Device fingerprints and application banners
- Device interaction information

Large-scale Identification of Exploited IoT Devices

- Use the gained knowledge to identify compromised IoT devices in the Internet
- Inform national and global CERT teams about ongoing threats

[1] IoT under fire: Kaspersky detects more than 100 million attacks on smart devices in H1 2019, 10 2019.
[2] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose. SoK: Security Evaluation of Home-Based IoT Deployments. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1362–1380, 2019.
[3] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh. IoT Security: Ongoing Challenges and Research Opportunities. In *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, pages 230–234, Nov 2014.
[4] J. Wetzels. Ghost in the Machine: Challenges in Embedded Binary Security. Usenix Enigma, February 2017.
[5] M. Muench, J. Stijohann, F. Kargl, A. Francillon, and D. Balzarotti. What you corrupt is not what you crash: Challenges in fuzzing embedded devices. In *NDSS 2018, Network and Distributed Systems Security Symposium, 18-21 February 2018, San Diego, CA, USA*, 2018.

This research is funded by the FFG under the BRIDGE Young Scientists program (grant no. 872664) and the industrial PhD program (grant no. 878784).

SBA Research (SBA-K1) is a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.