AVRS: Emulating AVR Microcontrollers for Reverse Engineering and Security Testing

Michael Pucher, Christian Kudera, Georg Merzdovnik

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

Problem & Motivation

Background

AVR 8-bit microcontrollers are used in automotive applications, sensor nodes and IoT devices, while also being popular with hobbyists. They are the basis for most boards of the Arduino product line, which in turn is used in a variety of projects, like data logging [5] or control and measurement systems [3].

Due to weak processing power, security can become an afterthought:

- Data received from peripherals is untrusted user input.
- Simple vulnerabilities persist, e.g., stack buffer overflows.
- AVR devices cannot be monitored efficiently during execution.

Problems

- While there is a wealth of different tools for analyzing firmware for architectures that are common to standard hardware, such as Arm [2, 1], the AVR ecosystem did not receive a similar treatment.
- Muench et al. [2] have shown the need for full-system emulators for developing potent security analysis techniques.
- Existing emulators, e.g., Avrora [4], are intended to be used as part of the development process and thus unfit for use on unknown firmware.

Need: Emulators specifically designed for security analysis.

Methodology

- **Analysis of Existing Emulators.** Analyze existing open-source AVR emulators and document shortcomings
- **AVRS.** Implement a new emulator, compensating existing shortcomings
- **Evaluation of all Emulators.** Compare emulators regarding performance and completeness, examine AVRS improvements
- **Fuzzing AVR Firmware.** Build fuzzing support on top of AVRS

AVRS

Designed to reuse existing approaches of other emulators, improve on lacking monitoring features and performance

- **Instruction Decode.** Decode all instructions upfront, use internal intermediate representation (IR)
- **Instruction Emulation.** Emulating IR optimizes to jump table
- **Device Differences.** Architectural differences are decided at compile-time, using procedural Rust macros
- **Peripherals and Monitoring.** Provide Rust and RPC API for peripheral implementation, API can hook MMU for monitoring memory access.

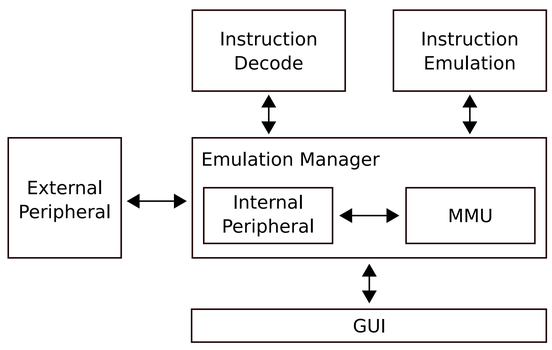

Figure 1: Overview of AVRS Architecture

Fuzzing

- **Implementation.** Use *boofuzz* as input generator, AVRS as emulator
- **Crash Detection.** Use heuristics presented in [2] to detect crashes
- **Example Programs.** Test fuzzer using serial protocol on ATtiny104 and ATmega328p, providing fuzzing cores and peripheral implementations

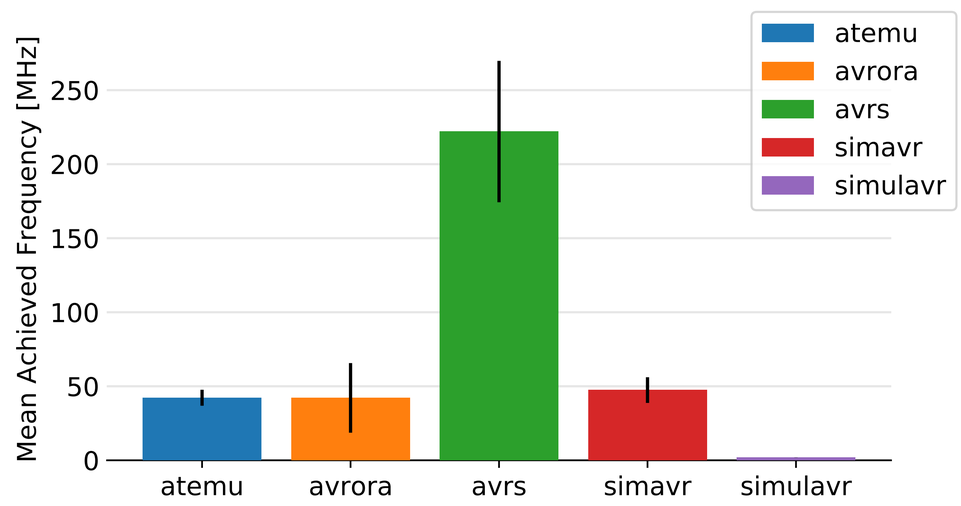

Figure 2: Achieved emulator frequencies across all benchmarks

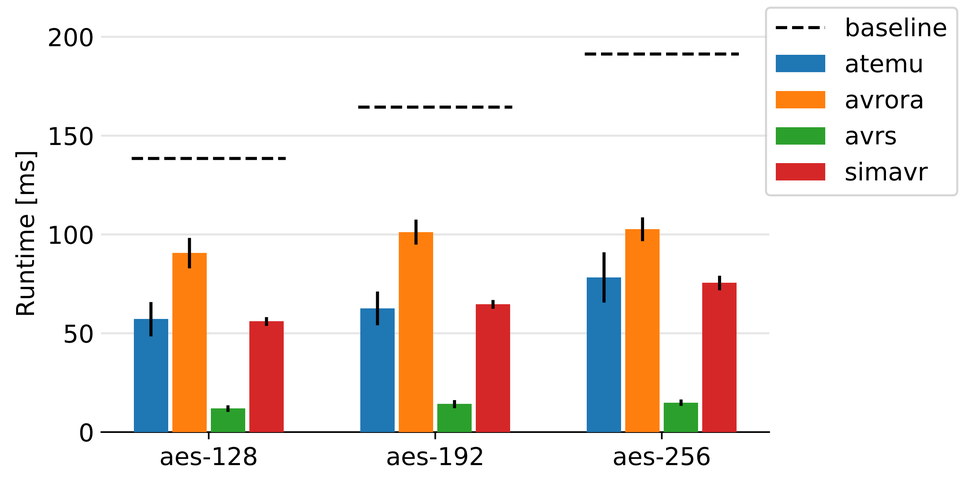

Figure 3: Performance of AES operations in emulators, slower than baseline omitted

Conclusions & Outlook

- Existing emulators lack completeness with respect to implemented instructions, even in mature, actively-developed emulators.
- Open-source toolchain support for ATtiny and ATxmega is error prone.
- AVRS can achieve competitive performance, as highlighted by figures 2 and 3, while also providing support for missing instructions.
- Fuzzing example shows ease of implementing analysis on top of AVRS.
- Use AVRS in future projects to evaluate symbolic execution/taint tracking on AVR devices, decode to IR allows exploring static analysis on AVR as well.

[1] Marius Muench, Dario Nisi, Aurélien Francillon, and Davide Balzarotti. Avatar2: A multi-target orchestration platform. In *Proc. Workshop Binary Anal. Res.(Colocated NDSS Symp.)*, volume 18, pages 1–11, 2018.
[2] Marius Muench, Jan Stijohann, Frank Kargl, Aurélien F rancillon, and Davide 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*, S an Diego, UNITED STATES, 02 2018.
[3] Isaías González Pérez, Antonio José Calderón Godoy, Manuel Calderón Godoy, and Juan Félix González González. Survey about the utilization of open source arduino for control and measurement systems in advanced scenarios. application to smart micro-grid and its digital replica. In *ICINCO*, 2019.
[4] Ben L. Titzer, Daniel K. Lee, and Jens Palsberg. Avrora: Scalable sensor network simulation with precise timing. In *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks*, IPSN '05, Piscataway, NJ, USA, 2005. IEEE Press.
[5] Andrew Wickert, Chad Sandell, Bobby Schulz, and G.-H Ng. Open-source arduino-derived data loggers designed for field research. *Hydrology and Earth System Sciences Discussions*, pages 1–16, 12 2018.

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG Forschung wirkt.
wirtschaftsagentur wien Ein Fonds der Stadt Wien
Europäische Kommission
FWF Der Wissenschaftsfonds.
netidee OPEN INNOVATIONS

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.