Jaewon Hur

Ph.D. Student
Dept. of Electrical and Computer Engineering
Seoul National University, South Korea
CompSec Lab

Email: *hurjaewon@snu.ac.kr*
GitHub: *https://github.com/JaewonHur*

About Me

I'm a Ph.D. student at Seoul National University (SNU), working in the CompSec lab. My research area is in systems/hardware security. I am interested in defining and finding new types of vulnerabilities particulary through leveraging fuzzing techniques. My current focus is on finding vulnerabilities in CPU hardware such as transient execution vulnerabilities. In addition to the vulnerability finding, I'm interested in various security issues such as trusted execution environments and kernel security.

Publications

1. **R2Z2: Detecting Rendering Regressions in Web Browsers through Differential Fuzz Testing**
   Suhwan Song, **Jaewon Hur**, Sunwoo Kim, Philip Rogers, and Byoungyoung Lee
   *IEEE/ACM International Conference on Software Engineering (**ICSE**) 2022*
2. **DifuzzRTL: Differential Fuzz Testing to Find CPU Bugs**
   Jaewon Hur, Suhwan Song, Dongup Kwon, Eunjin Baek, Jangwoo Kim, and Byoungyoung Lee
   *IEEE Symposium on Security and Privacy (**SP**) 2021*
3. **Push yoUr Password: Secure and Fast WiFi Connection for IoT Devices**
   Junyoung Choi, **Jaewon Hur**, and Saewoong Bahk
   *IEEE Wireless Communications and Networking Conference (**WCNC**) 2021*
4. **EV-CAST: Interference and Energy-Aware Video Multicast Exploiting Collaborative Relays.**
   Yeonchul Shin, **Jaewon Hur**, Gyujin Lee, Junyoung Choi, SungJu Lee, and Sunghyun Choi
   *IEEE International Conference on Mobile Ad Hoc and Sensor Systems (**MASS**) 2019*

(In submission)

5. **SpecDoctor: Differential Fuzz Testing to Find Transient Execution Vulnerabilities**
   Jaewon Hur, Suhwan Song, Sunwoo Kim, and Byoungyoung Lee
   *Submitted to IEEE Symposium on Security and Privacy (**SP**) 2022*

Research Projects

1. **Embedded secure platform verification.**
   In this project, we build a framework for emulating and verifying firmware running on a secure embedded processor.
   Seoul National University and Samsung LSI, 2021.

2. **CPU RTL fuzzing to find transient execution vulnerabilities.**

   We developed a fuzzer framework to find end-to-end transient execution vulnerabilities in a given CPU RTL. As a result, we found several variants of transient execution vulnerabilities.

   Seoul National University, 2020-2021.

3. **RTL fuzzing to find CPU bugs.**

   We applied a differential fuzzing technique on CPU RTL verification. With the fuzzer, we found several unknown CPU bugs on various open-source CPUs. We open-sourced the implementation in https://github.com/compsec-snu/difuzz-rtl.

   Seoul National University, 2019-2020.

Reported Hardware Bugs

- **OpenRISC Mor1kx**
  1. CVE-2020-13453: Misaligned swa raises exception when reservation is not set.
  2. CVE-2020-13454: Jump to link register does not assert illegal instruction exception.
  3. CVE-2020-13455: Reservation is not cancelled when there is snopping hit between lwa and swa.
  4. Issue #99: `eear` register does not save virtual address on illegal instruction exception.
  5. Issue #114: `l.fl1, l.ff1` instructions are incorrectly decoded.
- **RISC-V Rocket**
  1. Issue #2345: Instruction retired count does not increase on ebreak.
- **RISC-V Boom**
  1. CVE-2020-13251: Source field in `ProbeAckData` does not match the sink field of `ProbeRequest`.
  2. CVE-2020-29561: Misaligned `lr` instruction on a cached line set the reservation.
  3. Issue #454: `FS` in `mstatus` register is set after `fle.d` instruction.
  4. Issue #458: Floating point instruction which has invalid `rm` field does not raise exception.
  5. Issue #492: when `frm` is `DYN`, floating point instruction with `DYN` and does not raise exception.
  6. Issue #493: Rounding mode in `fsqrt` instruction does not work.
  7. Issue #503: `invalid operation` flag is not set after invalid `fdiv` instruction.
  8. Issue #577: New type of **transient execution attack** using implementation bug in Boom.
- **RISC-V Spike**
  1. CVE-2020-13456: Misaligned `lr.d` should not set load reservation.
  2. Issue #426: Faulting virtual address should not be written to `mtval` when `ebreak`.
  3. Issue #2390: Reading `dpc` register should raise exception in machine mode.

Education

- **Seoul National University (SNU)**, *South Korea*

  Ph.D. Course in Electrical and Computer Engineering (2017 - *Current*)

  Advisor: Prof. Byoungyoung Lee
- **Pohang University of Science and Technology (POSTECH)**, *South Korea*

  B.S. Electrical Engineering (2013 - 2016)

Skills

Language

Knowledgable: *C, Scala, Python, Chisel*
Have an experiance with: *Rust, Go, C++, Verilog*

Framework

RISC-V Boom, FIRRTL, Spike, Keystone, QEMU

Reference

Byoungyoung Lee

Assistant professor
Dept. of Electrical and Computer Engineering
Seoul National University, *South Korea*

Email: *byoungyoung@snu.ac.kr*
Homepage: *https://lifeasageek.github.io*