Jaewon Hur / Post Doctoral Researcher

Dept. of Electrical and Computer Engineering
Seoul National University
South Korea

Phone: (+82) 10-2284-1687| Mail: jwhur19@gmail.com | Lab: CompSec at SNU

About Me

I am currently working as a **post doctoral researcher** at **Computer Security Lab** of **Seoul National University**. I received **Ph.D** at **Computer Security Lab**, advised by professor **Byoungyoung Lee** from 2019 to 2023. Before then, I studied at **multimedia wireless network lab**, advised by professor **Sunghyun Choi** since 2017 until 2019.

I'm interested in the issues of **system security** in general, but I focused on two topics during my Ph.D: **fuzzing**, and **confidential computing**. As a research, I developed an RTL fuzzer for RISC-V CPUs, named **DifuzzRTL**, and presented it at **IEEE S&P 2021**. In the following research, I developed the first RTL fuzzer that finds transient execution vulnerabilities, named **SpecDoctor**, presenting it at **ACM CCS 2022**. After that, I moved to work on **confidential computing**, especially applying it to solve the issues of data privacy and sovereighty in machine learning. Accordingly, I developed **DLBox** (will be presented at **NDSS 2025**), which systematically protects the data from untrusted machine learners. In addition, I have guided several research projects about cloud security, such as **TeeMate** (i.e., efficient confidential serverless computing), and **Laputa** (i.e., secure policy enforcement in Spark), etc. Currently, I am working on virtualization (i.e., KVM), emulating TDX machines.

As above, **I have studied the topics in system security across the various fields, and I am always open to new security issues**. Besides, I generally like programming and solving the problems on my own, so I developed **MumeParrot**, which automatically trades stocks for me, and **Kandl**, which is a ChatGPT based course recommendation bot.

Publications

- **DLBox: New Model Training Framework for Protecting Training Data**
  Jaewon Hur, Juheon Yi, Cheolwoo Myung, Sangyun Kim, Youngki Lee, and Byoungyoung Lee
  The 32nd Network and Distributed System Security (NDSS), Feb, 2025.
- **Laputa: Secure Data Analytics in Apache Spark with Fine-grained Policy Enforcement and Isolated Execution**
  Byeongwook Kim, Jaewon Hur, Adil Ahmad, and Byoungyoung Lee
  The 32nd Network and Distributed System Security (NDSS), Feb, 2025.
- **TeeMate: Fast and Efficient Confidential Container using Shared Enclave**
  Chulmin Lee, Jaewon Hur, Sangho Lee, and Byoungyoung Lee
  Arxiv
- **Graminer: Fuzz Testing Gramine LibOS to Harden the Trusted Computing Base**
  Jaewon Hur, and Byoungyoung Lee
  The 6th Workshop on System Software for Trusted Execution (SysTex), May. 2023.
- **SpecDoctor: Differential Fuzz Testing to Find Transient Execution Vulnerabilities**
  Jaewon Hur, Suhwan Song, Sunwoo Kim, and Byoungyoung Lee
  The 29th ACM Conference on Computer and Communication Security (CCS), Nov. 2022.
- **FuzzOrigin: Detecting UXSS Vulnerabilities in Browsers through Origin Fuzzing**
  Sunwoo Kim, Youngmin Kim, Jaewon Hur, Suhwan Song, and Byoungyoung Lee
  The 31st Usenix Security Symposium (SEC), Aug. 2022.

- **R2Z2: Detecting Rendering Regression in Web Browsers through Differential Fuzz Testing**
  Suhwan Song, Jeawon Hur, Sunwoo Kim, and Byoungyoung Lee
  The 44th International Conference on Software Engineering (ICSE), Nov. 2022.
- **DifuzzRTL: Differential FuzzTesting to Find CPU Bugs**
  Jeawon Hur, Suhwan Song, Dongup Kwon, Eunjin Baek, Jangwoo Kim, and Byoungyoung Lee
  The 42nd IEEE Symposium on Security and Privacy (S&P), May, 2021.
- **Push Your Password: Secure and Fast WiFi Connection for IoT Devices**
  Junyoung Choi, Jaewon Hur, and Saewoong Bahk
  The 17th IEEE Wireless Communication and Networking Conference (WCNC), April, 2021.
- **EV-CAST: Interference and Energy-Aware Video Multicast Exploiting Collaborative Radio**
  Yeonchul Shin, Jaewon Hur, Gyujin Lee, Jonghoe Koo, Junyoung Choi, Sung-ju Lee, and Sunghyun Choi
  The 16th IEEE international Conference on Mobile Ad-Hoc and Smart Systems (MASS), November, 2019.

Projects

- **Emulating Intel TDX Machines** Sep. 2024 – Now
  - Used language: C
  - Used framework: KVM, QEMU, Gramine LibOS
- **ChatGPT based course recommendation bot (Kandl)** May. 2023 – Aug. 2023
  - Used language: TypeScript, React
  - Used framework: ElasticSearch, Redis, Figma, Next.js
- **Fuzzing Gramine LibOS** Feb. 2023 – May. 2023
  - Used language: Go, C
  - Used framework: Syzkaller, Gramine LibOS
  - **Actively used by Intel engineers**
- **Automated stock trading app (MumeParrot)** Sep. 2022 – Now
  - Used language: Kotlin
  - **Currently available in Android play store**
- **Secure policy enforcement in Apache Spark** May. 2022 – Dec. 2023
  - Used language: Scala
  - Used framework: Spark
- **Efficient confidential serverless framework** May. 2022 – Dec. 2023
  - Used language: C, Scala
  - Used framework: Gramine LibOS, OpenWhisk
- **Secure machine learning platform for data protection** Mar. 2022 – Apr. 2023
  - Used language: Python
  - Used framework: PyTorch, grpc, QEMU-KVM, vfio, AMD-SEV
  - Running normal Nvidia GPUs in SEV-SNP VMs
- **CPU fuzzing to find transient execution vulnerabilities** May. 2021 – Dec. 2022
  - Used language: Scala, Chisel
  - Used framework: RISC-V Boom, RISC-V NutShell, Firesim, Firrtl
- **Firmware fuzzing to find bugs in Samsung secure element** Mar. 2021 – Feb. 2022
  - Used language: C
  - Used framework: QEMU-KVM
- **Differential fuzz testing to find CPU bugs** Sep. 2019 – May. 2021
  - Used language: Scala, Chisel
  - Used framework: RISC-V Boom, RISC-V Rocket, Firrtl

Education

- **Seoul National University** Mar. 2017 - Sep. 2023
  Seoul, South Korea

  Ph.D. in Electrical and Computer Engineering (Advisor: Byoungyoug Lee)

- **Pohang University of Science and Technology** Mar.2013 - Feb. 2017
  Pohang, South Korea

  B.S. in Electronical Engineering

Technical Skills

Languages

- *Knowledgeable:* C, Python, Scala
- *Have an experience with:* Go, C++, Kotlin, Java, TypeScript

Frameworks: AFL, syzkaller, QEMU, kvm, Docker, Kubernetes, Git, Linux, PyTorch, React