Cheolwoo Myung / Ph.D Student

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

Phone: (+82) 10-5500-9036 | Mail: cwmyung@snu.ac.kr | Lab: CompSec at SNU

Research Interests

I am interesed in **system security**, especially the issues in **hypervisor** and **OS kernel**. Currently, my research focus is **software testing**, e.g., designing and implementing fuzzing system to detect vulnerabilities.

Publications

MundoFuzz: Hypervisor Fuzzing with Statistical Coverage Testing and Grammar Inference

Cheolwoo Myung, Gwangmu Lee, and Byoungyoung Lee

*The 31st USENIX Security Symposium (**Security**), August 2022. [to appear]*

Projects

Research on hypervisor device driver vulnerability analysis technology Apr 2021 – Oct 2021
National Security Research Institute of Korea (NSR)

- Design a fuzzer to detect vulnerabilities of para-virtualized (PV) back-end device driver
- Target: Hyper-V

Research on hypervisor vulnerability analysis technology Apr 2020 – Oct 2020
National Security Research Institute of Korea (NSR)

- Design a fuzzer to find vulnerabilities of virtual device provided by hypervisor
- Target: QEMU

Research on race condition vulnerability analysis technology Apr 2019 – Oct 2019
National Security Research Institute of Korea (NSR)

- Design a fuzzer to detect data race bugs in OS kernel
- Target: Windows7, 10

Reported Vulnerabilities (selected)

1. **CVE-2020-35506**: QEMU: Use-after-free in virtual SCSI device (am53c974) CVSS.v3: 6.7
2. **CVE-2020-35503**: QEMU: Null-pointer dereference in virtual SCSI device (megasas-gen2) CVSS.v3: 6.0
3. **CVE-2020-28916**: QEMU: Denial-of-Service in virtual network controller (e1000e) CVSS.v3: 5.5

Education

Seoul National University Sep 2018 - Present
Seoul, South Korea

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

Handong Global University Mar 2012 - Aug 2018
Pohang, South Korea

B.S. in Mechanical and Control Engineering

Technical Skills

Languages

- *Knowledgeable:* C, Go
- *Have an experience with:* C++, Python, Rust

Frameworks: AFL, syzkaller, QEMU