Yoochan Lee / Ph.D Student

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

Phone: (+82) 10-5264-4225 | Mail: yoochan10@snu.ac.kr | Homepage: link | Lab: CompSec at SNU

Research Interests

In general, my research area is **System and Software Security**. I focus on evolutionizing exploition technique such as combining exploitation technique and side-channel attacks. I mainly focus on doing research that is of interest to academia and industry.

Education

Seoul National University Sep 2019 - Present
Seoul, South Korea

M.S/Ph.D. in Electrical and Computer Engineering (Advisor: Byoungyoung Lee)

Hanyang University Mar 2012 - Feb 2018
Seoul, South Korea

B.S. Computer Science and Engineering

Experience

- **Raon WhiteHat, Security Team**, Seoul, South Korea (February 2017 - August 2017)
  Security Intern: Penetration Testing
- **Naver Labs, Security Team**, Gyeonggi-do, South Korea (April 2016 - June 2016)
  Security Intern: Finding web browser vulnerabilties in Naver Whale
- **ETRI, Network Security Team**, Gyeonggi-do, South Korea (January 2015 - February 2015)
  Intern

Publications

- **Diagnosing Kernel Concurrency Failures with AITIA**
  Dae R. Jeong, Minkyu Jung, Yoochan Lee, Byoungyoung Lee, Insik Shin, and Youngjin Kwon
  In ACM EuroSys Conference (EuroSys) 2023
- **Pspray: Timing Side-Channel based Linux Kernel Heap Exploitation Technique**
  Yoochan Lee, Jinhan Kwak, Junesoo Kang, Yuseok Jeon, and Byoungyoung Lee
  In 31st USENIX Security Symposium (SEC), Aug 2023
- **ExpRace: Exploiting Kernel Races through Raising Interrupts**
  Yoochan Lee, Changwoo Min, and Byoungyoung Lee
  In 30th USENIX Security Symposium (SEC), Aug 2021

Publications (Industiral Conferences)

- **Privilege Escalation Exploit using DOP in x86-64 macOS**

  Yoochan Lee, Sangjun Song, Junoh Lee, and Jeongsu Choi
  Hack In The Box Amsterdam 2023

- **Perfect Spray: A Journey From Finding a New Type of Logical Flaw at Linux Kernel To Developing a New Heap Exploitation Technique**

  Yoochan Lee, Jinhan Kwak, Junesoo Kang, Yuseok Jeon, and Byoungyoung Lee
  BlackHat Europe 2022

- **Exploiting Kernel Races through Taming Thread Interleaving**

  Yoochan Lee, Changwoo Min, and Byoungyoung Lee
  BlackHat USA 2020

Honor and Awards

- **The 3rd place** in DEFCON 30 CTF (StarBugs), Las Vegas, USA, Aug. 2022
- The 4th place in DEFCON 29 CTF (StarBugs), Las Vegas, USA, Aug. 2021
- The 11th place in DEFCON 28 CTF (Star-Bugs), Las Vegas, USA, Aug. 2020
- The 15th place in DEFCON 27 CTF (CGC), Las Vegas, USA, Aug. 2019
- The 11th place in Seccon CTF (GYG), Tokyo, Japan, Dec. 2018
- **The 1st place** in Cyber Conflict Excercise and Contest 2018 (GYG), Jeju, South Korea, Oct. 2018
- The 13th place in DEFCON 26 CTF (C.G.K.S), Las Vegas, USA, Aug. 2018
- The 8th place in Midnight Sun CTF, Stockholm, Sweden, June. 2018
- The 9th place in Codegate CTF (GYG), Seoul, South Korea, Apr. 2018
- The 5th place in Cyber Conflict Excercise and Contest 2017 (GYG), Seoul, South Korea, Nov. 2017
- The 3rd place in Belluminar POC 2017, Seoul, South Korea, Nov. 2017
- The 9th place in DEFCON 25 CTF (RRR), Las Vegas, USA, Aug. 2017
- Encouragement Award in Samsung CTF 2017, Seoul, South Korea, Aug. 2017
- The 6th place in Nuit Du Hack 2017 (GYG), Paris, France, June. 2017
- The 12th place in Seccon CTF 2017 (GYG), Tokyo, Japan, Jan. 2017
- **The 1st place** in Secuinside Capture The Bug (Minionz), Seoul, South Korea, July. 2016
- The 6th place in Codegate CTF (teambob), Seoul, South Korea, May. 2016
- **Top 10** in Best Of the Best 4th, Mar. 2016

Reported Vulnerabilities (selected)

- **CVE-2021-31077: macOS:** Kernel heap overflow leads to Local Privilege Escalation.
- **Solidly:** Drain tremendous funds using invalid type casting.
- **CVE-2018-4417: macOS:** Kernel Information Leakage.
- **CVE-2018-4338: macOS:** Kernel Information Leakage.
- **CVE-2018-4084: macOS:** Kernel Information Leakage.
- **CVE-2017-7014: macOS:** Arbitrary Kernel Code Execution.