

# Yoochan Lee

## Postdoctoral Researcher

Max Planck Institute for Security and Privacy  
Bochum, Germany

Phone: (+82) 10-5264-4225 | Mail: [yoochan.lee@mpi-sp.org](mailto:yoochan.lee@mpi-sp.org) | Homepage: [leeyoochan.github.io](https://leeyoochan.github.io) | LinkedIn: [Profile](#)

### RESEARCH INTERESTS

---

My research advances **offensive security methodologies** to fundamentally strengthen system resilience. By developing **novel exploitation techniques** and precise **exploitability metrics**, I aim to uncover critical ‘blind spots’ that defensive-centric approaches often overlook. Specifically, my work demonstrates the practical severity of vulnerabilities previously dismissed as low-risk, providing defenders with the insights needed to **prioritize remediation efforts** effectively.

### EDUCATION

---

#### Seoul National University

*M.S./Ph.D. in Electrical and Computer Engineering*

Advisor: Prof. Byoungyoung Lee

Seoul, South Korea

*Sep 2019 – Aug 2025*

#### Arizona State University

*Visiting Scholar*

AZ, USA

*Mar 2024 – Jun 2024*

#### Hanyang University

*B.S. in Computer Science and Engineering*

Seoul, South Korea

*Mar 2012 – Feb 2018*

### PUBLICATIONS

---

- **GHost in the SHELL: A GPU-to-Host Memory Attack and Its Mitigation**

Sihyun Roh, Woohyuk Choi, Jaeyoung Chung, [Yoochan Lee](#), Suhwan Song, and Byoungyoung Lee  
*In IEEE Symposium on Security and Privacy (S&P), May 2026*

- **DirtyFree: Simplified Data-Oriented Programming in the Linux Kernel**

[Yoochan Lee](#), Hyuk Kwon, and Thorsten Holz  
*In Network and Distributed System Security Symposium (NDSS), Feb 2026*

- **PeTAL: Ensuring Access Control Integrity against Data-only Attacks on Linux**

Juhee Kim, Jinbum Park, [Yoochan Lee](#), Chengyu Song, Taesoo Kim, and Byoungyoung Lee  
*In ACM Conference on Computer and Communications Security (CCS), Oct 2024*

- **Pspray: Timing Side-Channel based Linux Kernel Heap Exploitation Technique**

[Yoochan Lee](#), Jinhan Kwak, Junesoo Kang, Yuseok Jeon, and Byoungyoung Lee  
*In USENIX Security Symposium (USENIX Security), Aug 2023*

- **Diagnosing Kernel Concurrency Failures with AITIA**

Dae R. Jeong, Minkyu Jung, [Yoochan Lee](#), Byoungyoung Lee, Insik Shin, and Youngjin Kwon  
*In European Conference on Computer Systems (EuroSys), May 2023*

- **ExpRace: Exploiting Kernel Races through Raising Interrupts**

[Yoochan Lee](#), Changwoo Min, and Byoungyoung Lee  
*In USENIX Security Symposium (USENIX Security), Aug 2021*

## PUBLICATIONS (UNDER SUBMISSION)

---

- **Heap Localization: Cache Side-Channel based Linux Kernel Heap Exploit Techniques**  
Yoochan Lee, Sihyun Roh, Hyuk Kwon, Byoungyoung Lee, and Thorsten Holz  
*Submitted to IEEE Symposium on Security and Privacy (S&P), 2026*

## PUBLICATIONS (INDUSTRIAL 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*

## ACADEMIC APPOINTMENTS

---

- **Max Planck Institute for Security and Privacy (MPI-SP)**, Bochum, Germany  
Postdoctoral Researcher (Advisor: Prof. Thorsten Holz)  
Nov 2025 – Present

## TEACHING & MENTORING EXPERIENCE

---

- **White Hat School**, Seoul, South Korea  
Lead Mentor  
Sep 2023 – Sep 2025
- **Best of the Best (BoB)**, Seoul, South Korea  
Mentor  
Jul 2023 – Present

## INDUSTRY EXPERIENCE

---

- **Raon WhiteHat**, Seoul, South Korea  
Security Intern: Penetration Testing  
Feb 2017 – Aug 2017
- **Naver Labs**, Gyeonggi-do, South Korea  
Security Intern: Browser Vulnerability Research (Naver Whale)  
Apr 2016 – Jun 2016
- **ETRI**, Daejeon, South Korea  
Intern, Network Security Team  
Jan 2015 – Feb 2015

## HONORS AND AWARDS

---

- **3rd Place**, DEFCON 30 CTF (Team StarBugs), Las Vegas, USA, Aug 2022
- **4th Place**, DEFCON 29 CTF (Team StarBugs), Las Vegas, USA, Aug 2021
- 11th Place, DEFCON 28 CTF (Team Star-Bugs), Las Vegas, USA, Aug 2020
- 15th Place, DEFCON 27 CTF (Team CGC), Las Vegas, USA, Aug 2019
- 1st Place, Cyber Conflict Exercise and Contest 2018 (GYG), Jeju, South Korea, Oct 2018
- 13th Place, DEFCON 26 CTF (Team C.G.K.S), Las Vegas, USA, Aug 2018
- 9th Place, DEFCON 25 CTF (Team RRR), Las Vegas, USA, Aug 2017
- 1st Place, Secuinside Capture The Bug (Team Minionz), Seoul, South Korea, July 2016
- **Top 10**, Best Of the Best 4th Generation, Mar 2016

## SELECTED VULNERABILITY DISCOVERIES

---

- **CVE-2021-31077 (macOS)**: Kernel heap overflow leading to Local Privilege Escalation.
- **Solidly Smart Contract**: Critical vulnerability allowing unauthorized fund withdrawal (Tremendous funds drained).
- **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.

## REFERENCES

---

**Available upon request.**