


Hacking Lab




Contact information
Email: insuyun@kaist.ac.kr TEL : 042-350-7469
Lab. : ITC Building (N1) 812
Website : <https://hacking.kaist.ac.kr>

Current state of the Lab. (in 2025 Spring Semester)
Postdoctoral Fellows : 0 PhD Students: 5 Master's Student: 9

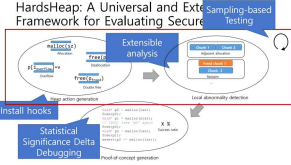
Research Areas: Understanding hacking in a scientific manner!

Automatic bug finding:
How do hackers find vulnerabilities?




BaseComp: A Comparative Analysis for Integrity Protection in Cellular Baseband Software (Security '23)

Automatic exploit generation:
How do hackers build exploits?



HardsHeap: A Universal and Extensible Framework for Evaluating Secure Allocators. (CCS '21)

Offensive research:
What do real hackers do?




Renderer RCE on both Google Chrome and Microsoft Edge (Pwn2Own 2024)

Recent research achievements ('21~)

32	▼ KAIST		11.4	13
<i>Faculty</i>				
Yongdae Kim	SECURITY		8	1.3
Soeul Son	SECURITY, ML, WEB, IR		6	1.6
Seungwon Shin 0001	NLP, SECURITY		6	1.2
Insu Yun	SECURITY		6	1.1

2nd in tie (based on csrcrankings for KAIST security research)

Developing AI-powered hacking system!



AIxCC finalists (20M dollars awarded!)

News!

- [06/04/2025] Security analysis of mandatory security software in South Korea is accepted to USENIX Security '25!
- [04/28/2025] FirmState is accepted to WiSec '25!
- [03/31/2025] CPMM-Exploiter is accepted to ISSTA '25!
- [12/19/2024] FIBLE is accepted to OOPSLA '25!
- [09/10/2024] RGFuzz is accepted to IEEE S&P '25!
- [08/11/2024] Team Atlanta proceeds to the AIxCC final!
- [03/22/2024] \$145K from Pwn2Own 2024 (Google Chrome, Microsoft Edge)!
- [01/25/2024] \$10K Bug Bounty from Google v8CTF!

Recommended courses

- EE209 Programming Structures for Electrical Engineering
- EE309: Advanced Programming Techniques for Electrical Engineering
- EE415: Introduction to Operating System
- EE517: Software Hacking Theory and Practice
- EE515: Security of Emerging Systems

Career after graduation

- Postdoc @ Georgia Tech (PhD)
- Security researcher @ Theori, ENKI Whitehat, 78ResearchLab, and S2W

Introduction to the Lab.

Our lab is one of the best labs that study *hacking*. If you are interested in understanding and analyzing systems, finding vulnerabilities, and exploiting them, don't hesitate to contact us!