

SEULBAE KIM

Assistant Professor

Department of Computer Science and Engineering
Pohang University of Science and Technology (POSTECH)

+82-54-279-2259 / seulbae@postech.ac.kr / seulbae-security.github.io

INTERESTS

Cyber-physical systems security (drones, self-driving vehicles, robotic systems, IoT devices)
System and software security

EDUCATION

Georgia Institute of Technology *Aug 2018 - Dec 2023*
Ph.D. in Computer Science, College of Computing
Thesis: Fortifying Cyber-Physical Systems through Comprehensive Bug-finding and Mitigation
Advisor: Dr. Taesoo Kim

Korea University *Mar 2016 - Aug 2018*
M.S. in Computer Science and Engineering
Thesis: Scalable Approach for Code Clone Detection and its Application in Practice
Advisor: Dr. Heejo Lee

Korea University *Mar 2010 - Feb 2016*
B.S. in Computer Science and Engineering
(On leave for 2 years: mandatory military service)

EMPLOYMENT HISTORY

Department of Computer Science and Engineering, POSTECH *Feb 2024 - Present*
Assistant Professor
Pohang, South Korea

- Leading [Computer Security Lab](#)

Data Science and System Security Team, NEC Labs America *May 2020 - Aug 2020*
Research Intern
Princeton, NJ, USA

- Project: Finding misbehaviors of autonomous driving systems through feedback-driven fuzzing
- Product: AutoFuzzer (published as DriveFuzz [\[C2\]](#))

Center for Software Security and Assurance (CSSA) *Nov 2015 - Feb 2018*
Core Researcher & Developer
Seoul, South Korea

- Led a project on the development of vulnerability discovery technologies for IoT software security.
- Product: IoTcube [\[T13\]](#), a platform for automated vulnerability testing (<https://iotcube.net>)

Cylab, Carnegie Mellon University *Jan 2017 - Feb 2017*
Visiting Researcher
Pittsburgh, PA, USA

- Developed an automated attack-vector analysis framework for IoT firmware.

Republic of Korea Army *Sep 2011 - Jun 2013*
Radio & computer systems operator
Paju-si, Gyeonggi-do, South Korea

- Served in the RoK Army as an active duty soldier.

PUBLICATIONS - CONFERENCE

In top-tier venues:

2 in *security* (CCS [C2], S&P [C6]), 2 in *software engineering* (FSE [C3], ICSE [C4]), and 1 in *systems* (SOSP [C5]).

[C1] SOUNDBOOST: Effective RCA and Attack Detection for UAV via Acoustic Side-Channel

Haoran Wang, Zheng Yang, Sangdon Park, Yibin Yang, Seulbae Kim, William Lunardi, Martin Andreoni, Taesoo Kim, and Wenke Lee

In Proceedings of the 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2025),

Naples, Italy, June 2025. [pdf]

[C2] DriveFuzz: Discovering Autonomous Driving Bugs through Driving Quality-Guided Fuzzing

Seulbae Kim, Major Liu, Junghwan Rhee, Yuseok Jeon, Yonghwi Kwon, and Chung Hwan Kim.

In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS 2022), Los Angeles, USA, November 2022. (acceptance rate: 22.4% = 218/971) [pdf] [code]

[C3] RoboFuzz: Fuzzing Robotic Systems over Robot Operating System (ROS) for Finding Correctness Bugs

Seulbae Kim, and Taesoo Kim.

In Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2022),

Singapore, November 2022. (acceptance rate: 21.1% = 99/469) [pdf] [code]

[C4] CENTRIS: A Precise and Scalable Approach for Identifying Modified Open-Source Software Reuse

Seunghoon Woo, Sunghan Park, Seulbae Kim, Heejo Lee, and Hakjoo Oh.

In Proceedings of the 43rd International Conference on Software Engineering (ICSE 2021), Virtual, May 2021. (acceptance rate: 22.4% = 138/615) [pdf] [code]

[C5] Finding Semantic Bugs in File Systems with an Extensible Fuzzing Framework

Seulbae Kim, Meng Xu, Sanidhya Kashyap, Jungyeon Yoon, Wen Xu, and Taesoo Kim.

In Proceedings of the 27th ACM Symposium on Operating Systems Principles (SOSP 2019), Ontario, Canada, October 2019. (acceptance rate: 13.8% = 38/276) [pdf] [code]

[C6] VUDDY: A Scalable Approach for Vulnerable Code Clone Discovery

Seulbae Kim, Seunghoon Woo, Heejo Lee and Hakjoo Oh.

In Proceedings of the 38th IEEE Symposium on Security and Privacy (S&P 2017), San Jose, CA, May 2017. (acceptance rate: 13.3% = 60/450) [pdf] [code]

[C7] SIGMATA: Storage Integrity Guaranteeing Mechanism against Tampering Attempts for Video Event Data Recorders

Hyuckmin Kwon, Seulbae Kim and Heejo Lee.

In Proceedings of the 7th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC 2016), Orlando, FL, March 2016. (won the session's best paper award) [pdf]

PUBLICATIONS - JOURNAL

[J1] Riding the IoT Wave with VFuzz: Discovering Security Flaws in Smart Home

Carlos Nkuba, Seulbae Kim, Sven Dietrich, and Heejo Lee.

IEEE Access, Volume 10, pp. 1775-1789, December 2021. [pdf] [code] [CVE summary]

[J2] Finding Bugs in File Systems with an Extensible Fuzzing Framework

Seulbae Kim, Meng Xu, Sanidhya Kashyap, Jungyeon Yoon, Wen Xu, and Taesoo Kim.

ACM Transactions on Storage, Volume 16, Issue 2, May 2020. [pdf]

[J3] Software systems at risk: An empirical study of cloned vulnerabilities in practice.

Seulbae Kim and Heejo Lee.

Computers & Security, Volume 77, pp. 720-736, August 2018. [pdf]

PATENTS

- [P1] **Apparatus and Method for Detecting Code Cloning of Software**
Heejo Lee and [Seulbae Kim](#), US 10146532 B2, December 2018.
- [P2] **Apparatus and Method for Detecting Code Cloning of Software**
Heejo Lee and [Seulbae Kim](#), KR 10-1780233, September 2017.

INVITED TALKS AND PRESENTATIONS

- [T1] **Semantics-Aware Kernel Testing for Deep Bug Discovery**
At Computer Systems Society Winter Conference,
Pyeongchang, South Korea, January 2026.
- [T2] **FortAIfy: An AI-Driven Threat Intelligence and Response System for UAV Swarms**
At TH GENZERO Workshop,
Abu Dhabi, UAE, November 2024.
- [T3] **Automated Red Teaming: Towards Finding Bugs in Military AI Robots**
At Responsible AI in the Military Domain (REAIM) Summit 2024,
Seoul, South Korea, September 2024.
- [T4] **Holistic Bug Hunting: Enhancing Security and Robustness of Cyber-Physical Systems**
At Ulsan National Institute of Science & Technology (UNIST),
Ulsan, South Korea, May 2024.
- [T5] **Holistic Bug Hunting: Enhancing Security and Robustness of Cyber-Physical Systems**
At Kyungpook National University,
Daegu, South Korea, April 2024.
- [T6] **ROBOFUZZ: Fuzzing Robotic Systems over Robot Operating System (ROS) for Finding Correctness Bugs**
At 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2022),
Singapore, November 2022.
- [T7] **DRIVEFUZZ: Discovering Autonomous Driving Bugs through Driving Quality-Guided Fuzzing**
At 29th ACM Conference on Computer and Communications Security (CCS 2022),
Los Angeles, CA, USA, November 2022.
- [T8] **Revamping Bug Detection Methodology for Cyber-Physical Systems**
At 2022 Summer AI/CSE Seminar Series, Pohang University of Science and Technology (POSTECH),
Virtual, August 2022.
- [T9] **Finding Semantic Bugs in File Systems with an Extensible Fuzzing Framework**
At 27th ACM Symposium on Operating Systems Principles (SOSP 2019),
Ontario, Canada, October 2019.
- [T10] **Automated Vulnerable Code Clone Detection in Open Source, and its Best Practice**
At Viterbi School of Engineering, University of Southern California,
Los Angeles, CA, USA, November 2017.
- [T11] **Case Study and Exercise on Software Vulnerability Analysis**
At 3rd Korea Institute of Information Security and Cryptography (KIISC) Short-term Seminar,
Seoul, South Korea, September 2017.
- [T12] **UDDY: A Scalable Approach for Vulnerable Code Clone Discovery**
At 38th IEEE Symposium on Security and Privacy,
San Jose, CA, USA, May 2017.
- [T13] **IoTcube: An Automated Analysis Platform for Finding Security Vulnerabilities**
At 38th IEEE Symposium on Security and Privacy,
San Jose, CA, USA, May 2017.

- [T14] **SIGMATA: Storage Integrity Guaranteeing Mechanism against Tampering Attempts for Video Event Data Recorders**
At 7th Multi-Conference on Complexity, Informatics and Cybernetics,
 Orlando, FL, USA, March 2016.

GRANTS AND CONTRACTS

- [1] **Development of an Intelligent Video Highlight Generation System Using MLOps and AI Multi-Agent Technologies**
 Agency/Company: Gyeongsangbuk-do (Gyeongbuk Techno Park)
 Total Amount: KRW 173,500,000
 Role: Co-PI
 Period of Contract: Sep 2025 - Apr 2026
 Share: 29%
- [2] **Complete Bug Finding Method for Robotic System Software**
 Agency/Company: National Research Foundation of Korea (NRF)
 Total Amount: KRW 92,754,000
 Role: PI
 Period of Contract: Sep 2025 - Aug 2026
 Share: 100%
- [3] **Security Threat and Mitigation Analysis for Linux Open-Source Security Tools**
 Agency/Company: Korea Institute of Information Security & Cryptology (KIISC)
 Total Amount: KRW 70,000,000
 Role: PI
 Period of Contract: Feb 2025 - Nov 2025
 Share: 100%
- [4] **Drone Attack Detection System Robust to Distribution Shift**
 Agency/Company: Wooseok Scholarship Foundation
 Total Amount: KRW 20,000,000
 Role: Co-PI
 Period of Contract: June 2024 - June 2025
 Share: 50%
- [5] **Architectural Design of a Zero-Trust-Based National Network Security Framework (N²SF)**
 Agency/Company: Korea Association of Cybersecurity Studies (KACS)
 Total Amount: KRW 34,000,000
 Role: Co-I
 Period of Contract: Apr 2024 - Nov 2024
 Share: 16%
- [6] **New Faculty Start-up Research Fund**
 Agency/Company: POSTECH
 Total Amount: KRW 250,000,000
 Role: PI
 Period of Contract: March 2024 - Feb 2027
 Share: 100%

TEACHING (POSTECH)

Semester	Course Number	Course Title	Enrollment	Evaluation
Fall 2025	CSED702C	Binary Analysis and Exploitation	17	5.0 / 5.0
Spring 2025	CSED415	Computer Security	31	4.96 / 5.0
Fall 2024	CSED702C	Binary Analysis and Exploitation	23	4.99 / 5.0
Spring 2024	CSED415	Computer Security	12	4.75 / 5.0

PROFESSIONAL SERVICE

Conference Committee Activities

- [1] Program Committee, *USENIX Symposium on Vehicle Security and Privacy (VehicleSec)*, 2026
- [2] Reviewer, *ACM/IEEE International Conference on Human-Robot Interaction (HRI)*, 2026
- [3] Program Committee, *Information Security Conference (ISC)*, 2025

Journal Reviewing Activities

- [1] Automated Software Engineering, 2025
- [2] IEEE Transactions on Information Forensics and Security (T-IFS), 2025
- [3] ACM Transactions on Software Engineering and Methodology (TOSEM), 2024

Other Reviewing Activities

- [1] External Reviewer, *USENIX Security Symposium (Security)*, 2024
- [2] External Reviewer, *USENIX Security Symposium (Security)*, 2023
- [3] External Reviewer, *ACM Conference on Computer and Communications Security (CCS)*, 2023
- [4] External Reviewer, *USENIX Security Symposium (Security)*, 2022
- [5] External Reviewer, *IEEE Symposium on Security and Privacy (Oakland)*, 2022
- [6] External Reviewer, *ACM Symposium on Operating Systems Principles (SOSP)*, 2021
- [7] External Reviewer, *Network and Distributed System Security Symposium (NDSS)*, 2020
- [8] External Reviewer, *IEEE Symposium on Security and Privacy (Oakland)*, 2019
- [9] External Reviewer, *ACM Conference on Computer and Communications Security (CCS)*, 2019

Memberships and Activities in Professional Societies

- [1] Advisory Committee Member, *Gyeongbuk Information Security Council*, 2024-2026

AWARDS & SCHOLARSHIPS

Teaching Excellence Prize (CSED702C)	POSTECH	<i>Jan, 2025</i>
Thank a Teacher Program Award (CS6265 TA)	Georgia Tech	<i>Dec, 2022</i>
NSA Codebreaker Challenge High Performer	The National Security Agency	<i>Dec, 2021</i>
Thank a Teacher Program Award (CS6265 TA)	Georgia Tech	<i>May, 2020</i>
Thank a Teacher Program Award (CS6265 TA)	Georgia Tech	<i>Dec, 2019</i>
DEFCON 27 CTF finals, #8 as r00timentary	Las Vegas, NV	<i>Aug, 2019</i>
Honors Scholarship	Korea University	<i>2015</i>