

Jaeseung Choi

Assistant Professor

Department of Computer Science and Engineering, Sogang University

Mail: jschoi22@sogang.ac.kr

Phone: +82-2-705-8490

Web: <https://islab-sogang.github.io>

Office: Adam Schall Hall (AS) 711, Baekbeom-ro, Mapo-gu, Seoul, 04107 Republic of Korea

RESEARCH INTERESTS

Software security, software testing, fuzzing, static analysis, binary analysis.

EDUCATION

Software Security Lab, KAIST Ph.D. in Computer Science Advisor: Prof. Sang Kil Cha Thesis: Extending the Capacity of Program-Aware Fuzzing with Binary-Level Static Analysis	2017.03 - 2022.02
Programming Research Lab, Seoul National University (SNU) M.S. in Computer Science and Engineering Advisor: Prof. Kwangkeun Yi	2015.03 - 2017.02
Seoul National University (SNU) B.S. in Computer Science and Engineering	2011.03 - 2015.02

PROFESSIONAL EXPERIENCE

Assistant Professor at Sogang University Department of Computer Science and Engineering	2022.09 - Present
Senior Researcher at CSRC, KAIST Research Division 1	2022.03 - 2022.07
Visiting Research at UC Berkeley Worked for DARPA Cyber Grand Challenge (CGC) project Host: Prof. Dawn Song	2015.05 - 2015.08
Research Intern at Programming Research Laboratory, SNU Advisor: Prof. Kwangkeun Yi	2013.09 - 2015.02
Research Intern at Real-time Ubiquitous System Laboratory, SNU Advisor: Prof. Chang-Gun Lee	2013.03 - 2013.07
Internship at SAP Labs Korea HANA DBMS team	2012.12 - 2013.01

SELECTED PUBLICATIONS

1. Minkyung Park, **Jaeseung Choi**, Hyeonmin Lee and Taekyoung Kwon. “Pave: Information Flow Control for Privacy-preserving Online Data Processing Services” In *Proceedings of the ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, 2025
2. Tae Eun Kim, **Jaeseung Choi***, Seongjae Im, Kihong Heo, and Sang Kil Cha. “Evaluating Directed Fuzzers: AreWe Heading in the Right Direction?” In *Proceedings of the ACM International Conference on the Foundations of Software Engineering (FSE)*, 2024
* Corresponding author
3. Tae Eun Kim, **Jaeseung Choi**, Kihong Heo, and Sang Kil Cha. “DAFL: Directed Grey-box Fuzzing Guided by Data Dependency.” In *Proceedings of the USENIX Security Symposium (USENIX Security)*, 2023
4. **Jaeseung Choi**, “Extending the Capacity of Program-Aware Fuzzing with Binary-Level Static Analysis.” Ph.D. Thesis, 2021
5. **Jaeseung Choi***, Doyeon Kim*, Soomin Kim, Gustavo Grieco, Alex Groce, and Sang Kil Cha. “SMARTIAN: Enhancing Smart Contract Fuzzing with Static and Dynamic Data-Flow Analyses.” In *Proceedings of the 36th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, 2021
* Co-first authors
6. **Jaeseung Choi**, Kangsu Kim, Daejin Lee, and Sang Kil Cha. “NTFUZZ: Enabling Type-Aware Kernel Fuzzing on Windows with Static Binary Analysis.” In *Proceedings of the 42nd IEEE Symposium on Security and Privacy (S&P)*, 2021
7. **Jaeseung Choi**, Joonun Jang, Choongwoo Han, and Sang Kil Cha. “Grey-box Concolic Testing on Binary Code.” In *Proceedings of the 41st IEEE/ACM International Conference on Software Engineering (ICSE)*, 2019
8. Minkyu Jung, Soomin Kim, HyungSeok Han, **Jaeseung Choi**, and Sang Kil Cha. “B2R2: Building an Efficient Front-End for Binary Analysis.” In *Proceedings of the Network and Distributed System Security Workshop on Binary Analysis Research (NDSS BAR)*, 2019
9. SeongIl Wi, **Jaeseung Choi**, and Sang Kil Cha. “Git-based CTF: A Simple and Effective Approach to Organizing In-Course Attack-and-Defense Security Competition.” In *Proceedings of the USENIX Workshop on Advances in Security Education*, 2018

AWARDS

Ricci Engineering Best Lecture Award Sogang University	2023.12
Outstanding Ph.D. Thesis Award KAIST School of Computing	2022.02
NAVER Ph.D. Fellowship 2021 NAVER Corporation	2021.12
Best Paper Award NDSS Workshop on Binary Analysis Research (NDSS BAR)	2019.02

Science & ICT Minister's Prize (1st prize) 2018.12
Information Security R&D Data Challenge
Korea Internet and Security Agency (KISA)

B.S. Summa Cum Laude 2015.02
Department of Computer Science & Engineering, SNU

ACADEMIC SERVICE

Committee

ACNS 2023 (Program Committee)
ACSAC 2021 (Artifact Evaluation Committee)

Invited Reviewer

IEEE Transactions on Software Engineering (TSE)
IEEE Transactions on Dependable and Secure Computing (TDSC)
ACM Transactions on Software Engineering and Methodology (TOSEM)
Journal of Systems and Software (JSS)

External Reviewer

ASIACCS 2018-2021
WWW 2020
EuroS&P 2020

Student Volunteer

ICSE 2020

VULNERABILITY REPORTS

Windows Kernel Vulnerabilities

Microsoft Bug Bounty
<https://www.microsoft.com/en-us/msrc/bounty>
CVE-2020-0792, CVE-2020-1246, CVE-2020-1053, CVE-2020-17004

Linux Package Vulnerabilities

CVE-2016-5735, CVE-2017-1000229, CVE-2017-16899, CVE-2017-16938, CVE-2018-7254, CVE-2018-6767, CVE-2018-7253, CVE-2018-1056, CVE-2018-6612, CVE-2017-18120, CVE-2018-19655

Windows Application Vulnerabilities

Korea Internet and Security Agency (KISA) Bug Bounty
<https://www.krcert.or.kr/consult/software/vulnerability.do>
Hancom Hwp (2014.03), Daum PotPlayer (2015.08).

SELECTED TALKS

Enabling Effective Software Testing with Static Program Analysis 2023.06
Technical Talk at KCC 2023

Detecting OS Vulnerabilities with Static Analysis and Fuzz Testing 2022.05
Technical Talk at KIISC Workshop on CPS Security

Extending Program-Aware Fuzzing with Binary-Level Static Analysis 2022.02
Seminar Talk at Department of Computer Science & Engineering, SNU

Using Static Binary Analysis for Effective Windows Kernel Fuzzing 2022.02
Technical Talk at SIGPL Winter School 2022

Smart Contract Vulnerability Detection at EVM Bytecode level Technical Talk at Security@KAIST	2021.11
Smartian: Enhancing Smart Contract Fuzzing with Static and Dynamic Data-Flow Analyses Conference Talk at ASE 2021	2021.11
NtFuzz: Enabling Type-Aware Kernel Fuzzing on Windows with Static Binary Analysis Seminar Talk at Prosys Lab, KAIST	2021.05
NtFuzz: Enabling Type-Aware Kernel Fuzzing on Windows with Static Binary Analysis Conference Talk at S&P 2021	2021.05
Grey-box Concolic Testing on Binary Code Conference Talk at ICSE 2019	2019.05
Grey-box Concolic Testing on Binary Code Technical Talk at SIGPL Winter School 2019	2019.02

SOFTWARE

Main developer of *Smartian*

Smart contract fuzzer written in F# and C#

<https://github.com/SoftSec-KAIST/Smartian>

Main developer of *NtFuzz*

Windows kernel fuzzer written in F#, C++ and Python#

<https://github.com/SoftSec-KAIST/NTFuzz>

Main developer of *Eclipser*

Linux binary fuzzer written in F# and C

<https://github.com/SoftSec-KAIST/Eclipser>

Main developer of *B2R2*

Binary analysis framework written in F#

<https://github.com/B2R2-org/B2R2>

Developer of *GitCTF*

Educational CTF platform written in Python

<https://github.com/SoftSec-KAIST/GitCTF>

OTHER EXPERIENCE

8th Place in DEFCON 21 CTF Final <i>Alternatives</i> team	2013.08
---	---------

SNU Information Security Research Club, <i>Guardian</i> Served as a club president in 2012 http://guardian.snucse.org/	2011 - 2014
---	-------------

REFERENCE

Sang Kil Cha

Associate Professor

Graduate School of Information Security, School of Computing

Korea Advanced Institute of Science and Technology (KAIST)

Mail: sangkilc@kaist.ac.kr

Web: <https://softsec.kaist.ac.kr/~sangkilc>