# Jaeseung Choi

Senior Researcher
Cyber Security Research Center (CSRC)
Korea Advanced Institute of Science and Technology (KAIST)

Mail: jschoi17@kaist.ac.kr
Phone: +82-042-350-8392
Web: https://softsec.kaist.ac.kr/~jschoi
Office: KAIST N5 #2312, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea

## RESEARCH INTERESTS

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

## RESEARCH POSITION

**Senior Researcher at CSRC, KAIST** 2022.03 - Present

## EDUCATION

**Software Security Lab, KAIST** 2017.03 - 2022.02
Ph.D. in Computer Science
Advisor: Prof. Sang Kil Cha
Thesis: Extending the Capacity of Program-Aware Fuzzing with Binary-Level Static Analysis

**Programming Research Lab, Seoul National University (SNU)** 2015.03 - 2017.02
M.S. in Computer Science and Engineering
Advisor: Prof. Kwangkeun Yi

**Seoul National University (SNU)** 2011.03 - 2015.02
B.S. in Computer Science and Engineering

## PROFESSIONAL EXPERIENCE

**Visiting Research at UC Berkeley** 2015.05 - 2015.08
Worked for DARPA Cyber Grand Challenge (CGC) project
Host: Prof. Dawn Song

**Research Intern at Programming Research Laboratory, SNU** 2013.09 - 2015.02
Advisor: Prof. Kwangkeun Yi

**Research Intern at Real-time Ubiquitous System Laboratory, SNU** 2013.03 - 2013.07
Advisor: Prof. Chang-Gun Lee

**Internship at SAP Labs Korea** 2012.12 - 2013.01
HANA DBMS team

## AWARDS

**Outstanding Ph.D. Thesis Award** 2022.02
KAIST School of Computing

**NAVER Ph.D. Fellowship 2021** 2021.12
NAVER Corporation

**Best Paper Award** 2019.02
NDSS Workshop on Binary Analysis Research (NDSS BAR)

**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 (5th out of 54)** 2015.02
Department of Computer Science & Engineering, SNU

**Science & ICT Minister's Certificate (Best 10)** 2014.03
Information Security Education Program, *BoB*
Korea Information Technology Research Institute (KITRI)

**National Scholarship for Science & Engineering** 2011 - 2014
Korea Student Aid Foundation (KOSAF)

## PUBLICATIONS

1. **Jaeseung Choi**, "Extending the Capacity of Program-Aware Fuzzing with Binary-Level Static Analysis." Ph.D. Thesis, 2021
2. **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
3. **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
4. Donghyeon Oh, **Jaeseung Choi**, Sang Kil Cha. "Semantics-Preserving Mutation-Based Fuzzing on JavaScript Interpreters." In *Journal of the Korea Institute of Information Security and Cryptology*, Vol. 30, No. 4, 2020
5. **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
6. 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
7. 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

## ACADEMIC SERVICE

**Artifact Evaluation Committee**
ACSAC 2021

**Student Volunteer**
ICSE 2020

**External Reviewer**
ASIACCS 2018-2021
WWW 2020
EuroS&P 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).

## TALKS (SELECTED)

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 2021.11
**Technical Talk at Security@KAIST (link)**

Smartian: Enhancing Smart Contract Fuzzing with Static and Dynamic Data-Flow Analyses 2021.11
**Conference Talk at ASE 2021**

NtFuzz: Enabling Type-Aware Kernel Fuzzing on Windows with Static Binary Analysis 2021.05
**Seminar Talk at Prosys Lab, KAIST**

NtFuzz: Enabling Type-Aware Kernel Fuzzing on Windows with Static Binary Analysis 2021.05
**Conference Talk at S&P 2021**

Grey-box Concolic Testing on Binary Code 2019.05
**Conference Talk at ICSE 2019**

Grey-box Concolic Testing on Binary Code 2019.02
**Technical Talk at SIGPL Winter School 2019**

## 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

## TEACHING EXPERIENCE

**Teaching Assistant, Information Security Laboratory** 2017-2018 Spring Semester
KAIST IS521 (Graduate Course)

**Teaching Assistant, Program Analysis** 2016 Spring Semester
SNU 4541.664A (Graduate Course)

**Teaching Assistant, Programming Language** 2015 Fall Semester
SNU 4190.310 (Undergraduate Course)

## OTHER EXPERIENCE

**8th Place in DEFCON 21 CTF Final** 2013.08
*Alternatives* team

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

## 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