

CHA, SANG KIL

KAIST N5 #2319, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Korea

☎ +82-(0)42-350-3569 | ✉ sangkilc@kaist.ac.kr | 🌐 [sangkilc](#)

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

Executive Summary

Sang Kil Cha is an experimental computer scientist whose research is at the intersection of computer security and software engineering. His research mainly involves building and evaluating systems that can analyze programs. He published numerous papers at a variety of top-tier conferences in computer science such as Oakland, CCS, NDSS, USENIX Security, ICSE, and ASE. He received an ACM distinguished paper award in 2014. He has been serving as a program committee for various international conferences including AsiaCCS, APSys, USENIX Enigma, and WISA.

Education

- 2010 – 2015 **Ph.D. in Electrical and Computer Engineering**
Carnegie Mellon University, Pittsburgh, PA
Advisor: David Brumley
Thesis Title: Towards Resource-Aware Security Testing of Software
Thesis Committee: Lujio Bauer, David Molnar, and Vyas Sekar
- 2008 – 2009 **M.S. in Electrical and Computer Engineering**
Carnegie Mellon University, Pittsburgh, PA
- 2001 – 2008 **B.S. in Electrical and Computer Engineering**
Korea University, Seoul, Korea

Research Interests

Software security, systems security, software engineering, and program analysis.

Professional Experience

| | | |
|-------------|-------------------------------------|----------------|
| Nov. 2015 – | Assistant Professor, KAIST | Daejeon, Korea |
| Summer 2013 | Research Intern, Microsoft Research | Redmond, WA |
| Summer 2011 | Research Intern, Microsoft Research | Redmond, WA |

Honors and Awards

| | | |
|------|--|------------------|
| 2014 | ACM Distinguished Paper Award (<i>ICSE</i> 2014) | Hyderabad, India |
| 2013 | Student Travel Grant Award (<i>CCS</i> 2013) | Berlin, Germany |
| 2011 | Ann and Martin McGuinn Graduate Fellowship (CMU) | Pittsburgh, PA |
| 2010 | Student Travel Grant Award (<i>CCS</i> 2010) | Chicago, IL |
| 2010 | Moon-Jung Chung Scholarship (<i>KOCSEA</i> 2010) | Vienna, VA |
| 2010 | Carnegie Institute of Technology Dean's Tuition Fellowship | Pittsburgh, PA |

Publications

Refereed Conference and Workshop Papers

- [1] 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
- [2] HyungSeok Han and **Sang Kil Cha**. IMF: Inferred Model-based Fuzzer. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 2345–2358, 2017
- [3] Soomin Kim, Markus Faerevaag, Minkyu Jung, SeungIl Jung, DongYeop Oh, JongHyup Lee, and **Sang Kil Cha**. Testing Intermediate Representations for Binary Analysis. In *Proceedings of the IEEE/ACM International Conference on Automated Software Engineering*, pages 353–364, 2017
- [4] Weidong Cui, Marcus Peinado, **Sang Kil Cha**, Yanick Fratantonio, and Vasileios P. Kemerlis. RETracer: Triaging Crashes by Reverse Execution from Partial Memory Dumps. In *Proceedings of the International Conference on Software Engineering*, pages 820–831, 2016
- [5] **Sang Kil Cha**, Maverick Woo, and David Brumley. Program-Adaptive Mutational Fuzzing. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 725–741, 2015
- [6] Alexandre Rebert, **Sang Kil Cha**, Thanassis Avgerinos, Jonathan Foote, David Warren, Gustavo Grieco, and David Brumley. Optimizing Seed Selection for Fuzzing. In *Proceedings of the USENIX Security Symposium*, pages 861–875, 2014
- [7] Thanassis Avgerinos, Alexandre Rebert, **Sang Kil Cha**, and David Brumley. Enhancing Symbolic Execution with Veritesting. In *Proceedings of the International Conference on Software Engineering*, pages 1083–1094, 2014

- [8] Maverick Woo, **Sang Kil Cha**, Samantha Gottlieb, and David Brumley. Scheduling Black-box Mutational Fuzzing. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 511–522, 2013
- [9] **Sang Kil Cha**, Thanassis Avgerinos, Alexandre Rebert, and David Brumley. Unleashing Mayhem on Binary Code. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 380–394, 2012
- [10] Thanassis Avgerinos, **Sang Kil Cha**, Brent Lim Tze Hao, and David Brumley. AEG: Automatic Exploit Generation. In *Proceedings of the Network and Distributed System Security Symposium*, pages 283–300, 2011
- [11] **Sang Kil Cha**, Brian Pak, David Brumley, and Richard J. Lipton. Platform-Independent Programs. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 547–558, 2010
- [12] **Sang Kil Cha**, Iulian Moraru, Jiyong Jang, John Truelove, David Brumley, and David G. Andersen. SplitScreen: Enabling Efficient, Distributed Malware Detection. In *Proceedings of the USENIX Symposium on Networked Systems Design and Implementation*, pages 377–390, 2010

Refereed Journal Papers

- [13] Thanassis Avgerinos, Alexandre Rebert, **Sang Kil Cha**, and David Brumley. Enhancing Symbolic Execution with Veritesting. *Communications of the ACM*, 59(6):93–100, 2016
- [14] Thanassis Avgerinos, **Sang Kil Cha**, Alexandre Rebert, Edward J. Schwartz, Maverick Woo, and David Brumley. Automatic Exploit Generation. *Communications of the ACM*, 57(2):74–84, 2014
- [15] **Sang Kil Cha**, Iulian Moraru, Jiyong Jang, John Truelove, David Brumley, and David G. Andersen. SplitScreen: Enabling Efficient, Distributed Malware Detection. *Journal of Communications and Networks*, 13(2):187–200, 2011

Patents

- [16] **Sang Kil Cha**, Soomin Kim, and Minsu Lee. System and Method for Visualizing Binary Structure. Patent App. Korea 10-2018-0049693, 2018
- [17] Seungwon Shin, Chanhee Lee, Changhoon Yoon, and **Sang Kil Cha**. Apparatus, Method, and Computer Program for Malware Detection of Software Defined Network. Patent App. US 15811248, 2017
- [18] David Brumley, **Sang Kil Cha**, Thanassis Avgerinos, and Alexandre Rebert. Detecting Exploitable Bugs in Binary Code. US Patent 9542559, 2017
- [19] **Sang Kil Cha**, Chanho Ryu, Seungll Jung, and DongYeop Oh. Apparatus and Method for Intermediate Language Transformation of Binary Data. Patent App. Korea 10-2016-0155803, 2016
- [20] David Brumley, Thanassis Avgerinos, and **Sang Kil Cha**. Automated Exploit Generation. US Patent 9135405, 2015

[21] Weidong Cui, David Molnar, and **Sang Kil Cha**. Computer Memory Access Monitoring and Error Checking. Patent App. US 20130152053, 2013

Professional Services

Conference Program Committee

| | |
|-------------|--|
| 2018 – 2019 | ACM ASIACCS |
| 2018 | ACM APSys |
| 2018 | NDSS Workshop on Binary Analysis Research (BAR) |
| 2016, 2018 | USENIX Enigma |
| 2018 | Netsec-KR |
| 2013 – 2018 | International Workshop on Information Security Applications (WISA) |

Selected Invited Talks and Seminars

| | | |
|------|---|----------------|
| 2018 | Binary-level Vulnerability Discovery: Past, Present, and Future <i>Invited Speaker at POSTECH CS Seminar</i> | Pohang, Korea |
| 2017 | Binary Analysis and Hacking <i>Invited Speaker at Cyber Conflict Exercise Seminar</i> | Seoul, Korea |
| 2017 | Cyberwarfare and Artificial Intelligence <i>Advisory Panel at KTV Science Talk Show</i> | Sejong, Korea |
| 2017 | Automated Bug Finding <i>Invited Speaker at Korea University Seminar</i> | Seoul, Korea |
| 2016 | Towards Resource-Aware Fuzzing <i>Invited Speaker at International Symposium on Mobile Security</i> | Seoul, Korea |
| 2016 | AI & Security <i>Keynote Speaker at International Cyber Security Conference</i> | Seoul, Korea |
| 2016 | Automatic Exploit Generation <i>Keynote Speaker at SECUINSIDE</i> | Seoul, Korea |
| 2016 | Towards Resource-Aware Fuzzing <i>Invited Speaker at Samsung Seminar</i> | Daejeon, Korea |
| 2016 | Towards Resource-Aware Fuzzing <i>Invited Speaker at KAIST CS Colloquium</i> | Daejeon, Korea |

Teaching

| | | |
|-------------|--|-------------------------|
| Spring 2018 | IS521 - Information Security Laboratory IS511 - Introduction to Information Security (co-taught with 5 others) CS408E - Computer Science Project (mentored 1 team) | KAIST KAIST KAIST |
| Fall 2017 | IS561 - Binary Code Analysis and Secure Software Systems | KAIST |
| Spring 2017 | IS521 - Information Security Laboratory IS511 - Introduction to Information Security (co-taught with 4 others) | KAIST KAIST |
| Fall 2016 | IS893 - Advanced Software Security | KAIST |
| Spring 2016 | IS561 - Binary Code Analysis and Secure Software Systems | KAIST |

Advising

Current Students

| | | |
|----------|---------------|-------|
| 2017.3 – | Jaeseung Choi | Ph.D. |
| 2018.3 – | HyungSeok Han | Ph.D. |
| 2018.3 – | Soomin Kim | Ph.D. |
| 2016.8 – | Mun Beom Kim | M.S. |
| 2017.3 – | Seongil Wi | M.S. |
| 2017.8 – | Jiwon Choi | M.S. |
| 2018.3 – | Hongsik Kim | M.S. |
| 2018.3 – | Donghyeon Oh | M.S. |

Students Supervised

| | |
|-----------------|---|
| 2016.1 – 2017.2 | Choongwoo Han, M.S., Now at Naver Labs, Korea |
| 2016.1 – 2017.2 | Hobin Kim, M.S., Now at National Security Research Institute, Korea |
| 2016.3 – 2018.2 | Jihyeon Yoon, M.S., Now at Nexon, Korea |
| 2016.4 – 2018.2 | Jihoon Kim, M.S., Now at Naver Labs, Korea |

Selected Grants

| | | |
|-------------|---|----|
| 2018 | Developing JavaScript Mutation Algorithm for Fuzzing 50,000,000 KRW from LIG | PI |
| 2018 | Model-based Fuzzing for Finding Kernel Vulnerabilities 90,000 USD (45,000 USD from ONRG and 45,000 USD from ONR) | PI |
| 2017 | Binary Smart Fuzzing 98,000,000 KRW from Samsung | PI |
| 2017 | Next-Generation SIEM Development 60,000,000 KRW from AhnLab | PI |
| 2017 – 2018 | Cyber Immune System 225,000,000 KRW from IITP | PI |
| 2017 | Smart Fuzzing for Emerging Vehicle Platform 50,000 USD from Ford Motor Company | PI |
| 2016 | Search-based Fuzzing 37,000,000 KRW from KAIST | PI |
| 2016 – 2018 | Building a Platform for Automated Reverse Engineering and Vulnerability Detection with Binary Code Analysis 1,510,000,000 KRW from IITP | PI |
| 2015 – 2018 | Discovering Vulnerabilities with Binary Code Analysis 100,000,000 KRW from KAIST | PI |