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 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 WWW, ASIACCS, Euro S&P, APSys, USENIX Enigma, and NDSS BAR.

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: Lujo 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

2020 – Present	Director of Cyber Security Research Center, KAIST	Daejeon, Korea
2020 – Present	Associate Professor, KAIST	Daejeon, Korea
2015 – 2020	Assistant Professor, KAIST	Daejeon, Korea
Summer 2013	Research Intern, Microsoft Research	Redmond, WA
Summer 2011	Research Intern, Microsoft Research	Redmond, WA

Honors and Awards

2019	Best Paper Award (*NDSS BAR* 2019)	San Diego, CA
2018, 2019	MSIT Minister Prize (*Data Challenge* 2018, 2019)	Seoul, Korea
2018	Best Paper Award (*WISA* 2018)	Jeju, Korea
2014	**ACM Distinguished Paper Award** (*ICSE* 2014)	Hyderabad, India
2013	Student Travel Grant Award (*CCS* 2013)	Berlin, Germany
2011	Ann and Martin McGuinn Graduate Fellowship (CMU)	Pittsburgh, PA
2010	Student Travel Grant Award (*CCS* 2010)	Chicago, IL
2010	Moon-Jung Chung Scholarship (*KOCSEA* 2010)	Vienna, VA
2010	Carnegie Institute of Technology Dean's Tuition Fellowship	Pittsburgh, PA

Publications

Refereed Conference and Workshop Papers

[1] Valentin J. M. Manès, Soomin Kim, and **Sang Kil Cha**. Ankou: Guiding Grey-box Fuzzing towards Combinatorial Difference. In *Proceedings of the International Conference on Software Engineering*, pages 1024–1036, 2020

[2] Suyoung Lee, HyungSeok Han, **Sang Kil Cha**, and Sooel Son. Montage: A Neural Network Language Model-Guided JavaScript Fuzzer. In *Proceedings of the USENIX Security Symposium*, 2020

[3] Valentin J. M. Manès, HyungSeok Han, Choongwoo Han, **Sang Kil Cha**, Manuel Egele, Edward J. Schwartz, and Maverick Woo. The Art, Science, and Engineering of Fuzzing: A Survey. *IEEE Transactions on Software Engineering*, pages 1–1, 2019

[4] Jaeseung Choi, Joonun Jang, Choongwoo Han, and **Sang Kil Cha**. Grey-box Concolic Testing on Binary Code. In *Proceedings of the International Conference on Software Engineering*, pages 736–747, 2019

[5] HyungSeok Han, DongHyeon Oh, and **Sang Kil Cha**. CodeAlchemist: Semantics-Aware Code Generation to Find Vulnerabilities in JavaScript Engines. In *Proceedings of the Network and Distributed System Security Symposium*, 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 NDSS Workshop on Binary Analysis Research*, 2019

[7] Jina Hong, JinKi Lee, HyunKyu Lee, YoonHa Chang, KwangHo Choi, and **Sang Kil Cha**. AlertVision: Visualizing Security Alerts. In *Proceedings of the World Conference on Information Security*, 2018

[8] Chanhee Lee, Changhoon Yoon, Seungwon Shin, and **Sang Kil Cha**. INDAGO: A New Framework For Detecting Malicious SDN Applications. In *Proceedings of the IEEE International Conference on Network Protocols*, pages 220–230, 2018

[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

[10] 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

[11] 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

[12] 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

[13] **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

[14] 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

[15] 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

[16] 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

[17] **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

[18] 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

[19] **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

[20] **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

[21] **Sang Kil Cha** and Zhenkai Liang. Asia's Surging Interest in Binary Analysis. *Communications of the ACM*, 63(4):86–88, 2020

[22] Thanassis Avgerinos, Alexandre Rebert, **Sang Kil Cha**, and David Brumley. Enhancing Symbolic Execution with Veritesting. *Communications of the ACM*, 59(6):93–100, 2016

[23] 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

[24] **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

[25] **Sang Kil Cha**, Soomin Kim, and Minsu Lee. System and Method for Visualizing Binary Structure. Korea Patent 10-1974069, 2019

[26] **Sang Kil Cha**, SeongIl Wi, Jaeseung Choi, and HyungSeok Han. Git-based System and Method for Providing Attack and Defense Hacking Contests. Patent App. Korea 10-2018-0094406, 2018

[27] 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

[28] David Brumley, **Sang Kil Cha**, Thanassis Avgerinos, and Alexandre Rebert. Detecting Exploitable Bugs in Binary Code. US Patent 9542559, 2017

[29] **Sang Kil Cha**, Chanho Ryu, SeungIl Jung, and DongYeop Oh. Apparatus and Method for Intermediate Language Transformation of Binary Data. Patent App. Korea 10-2016-0155803, 2016

[30] David Brumley, Thanassis Avgerinos, and **Sang Kil Cha**. Automated Exploit Generation. US Patent 9135405, 2015

[31] 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

2020–2021	The Web Conference (WWW)
2020	IEEE Euro S&P
2020	ISSTA Doctoral Symposium
2020	International Conference on Information Systems Security (ICISS)
2020	ACM LCTES
2020	SoftEng
2018 – 2021	ACM ASIACCS
2018	ACM APSys
2018 – 2019	NDSS Workshop on Binary Analysis Research (BAR)
2016, 2018	USENIX Enigma
2018	Netsec-KR
2013 – 2020	International Workshop on Information Security Applications (WISA)

Selected Talks

2019	Binary Analysis and Finding Security Vulnerabilities *Invited Speaker at Korea University Seminar*	Seoul, Korea
2019	Finding Vulnerabilities in Large and Complex COTS Software *Invited Speaker at Qualcomm Seminar*	San Diego, CA
2018	Git-based CTF and Automated Hacking Competition *Invited Speaker at Cyber Conflict Exercise 2018*	Jeju, Korea
2018	Binary-level Vulnerability Discovery: Past, Present, and Future *Invited Speaker at POSTECH CS Seminar*	Pohang, Korea
2017	Binary Analysis and Hacking *Invited Speaker at Cyber Conflict Exercise 2017*	Seoul, Korea
2017	Cyberwarfare and Artificial Intelligence *Advisory Panel at KTV Science Talk Show*	Sejong, Korea
2017	Automated Bug Finding *Invited Speaker at Korea University Seminar*	Seoul, Korea
2016	Towards Resource-Aware Fuzzing *Invited Speaker at International Symposium on Mobile Security*	Seoul, Korea
2016	AI & Security *Keynote Speaker at International Cyber Security Conference*	Seoul, Korea
2016	Automatic Exploit Generation	Seoul, Korea

	Keynote Speaker at SECUINSIDE	
2016	Towards Resource-Aware Fuzzing *Invited Speaker at Samsung Seminar*	Suwon, Korea
2016	Towards Resource-Aware Fuzzing *Invited Speaker at KAIST CS Colloquium*	Daejeon, Korea

Teaching

Spring 2019	IS521 - Information Security Laboratory	KAIST
	IS511 - Introduction to Information Security (co-taught with 5 others)	KAIST
	CS220 - Programming Principles	KAIST
Fall 2018	IS561 - Binary Code Analysis and Secure Software Systems	KAIST
Spring 2018	IS521 - Information Security Laboratory	KAIST
	IS511 - Introduction to Information Security (co-taught with 5 others)	KAIST
	CS408E - Computer Science Project (mentored 1 team)	KAIST
Fall 2017	IS561 - Binary Code Analysis and Secure Software Systems	KAIST
Spring 2017	IS521 - Information Security Laboratory	KAIST
	IS511 - Introduction to Information Security (co-taught with 4 others)	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 –	Soomin Kim	Ph.D.
2019.9 –	Hyungseok Kim	Ph.D.
2019.3 –	Kangsu Kim	M.S.
2019.3 –	Dohyeok Kim	M.S.
2019.3 –	Doyeon Kim	M.S.
2019.8 –	Daejin Lee	M.S.
2020.3 –	Myeonggeun Shin	M.S.

Students Supervised

2016.1 – 2017.2	Choongwoo Han, M.S., Now at Naver, 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, Korea
2016.8 – 2018.7	Mun Beom Kim, M.S., Now at the Army, Korea
2017.3 – 2019.2	Seongil Wi, M.S., Now at GSIS KAIST as a Ph.D. student
2017.3 – 2019.2	Markus Faerevaag, M.S., Now at Deloitte, Denmark
2017.8 – 2019.7	Jiwon Choi, M.S., Now at National Security Research Institute, Korea
2018.8 – 2019.7	Minkyu Jung, M.S., Now at KAIST as a Ph.D. student
2018.3 – 2019.7	HyungSeok Han, M.S., Now at Theori
2018.3 – 2020.2	Hongsik Kim, M.S., Now at National Security Research Institute, Korea
2018.3 – 2020.2	Donghyeon Oh, M.S., Now at National Security Research Institute, Korea

Selected Grants

2018	Developing JavaScript Mutation Algorithm for Fuzzing 50,000,000 KRW from LIG	PI
2018–2019	Model-based Fuzzing for Finding Kernel Vulnerabilities 180,000 USD (90,000 USD from ONRG and 90,000 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