

Cha, Sang Kil

Curriculum Vitae

CyLab, Carnegie Mellon University

4720 Forbes Avenue

Pittsburgh, PA 15213

☎ +1 (412) 638 1253

✉ sangkil@cmu.edu

🌐 <http://users.ece.cmu.edu/~sangkil/>

Education

- 2010– **Ph.D. in Electrical and Computer Engineering**
Carnegie Mellon University, Pittsburgh, PA (expected 2015)
Advisor: David Brumley
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; program analysis.

Honors and Awards

- 2014 **ACM Distinguished Paper Award**, ICSE, Hyderabad, India.
- 2013 **Student Travel Grant Awards**, CCS, Berlin, Germany.
- 2011 **Ann and Martin McGuinn Graduate Fellowship**, Carnegie Mellon University, Pittsburgh, PA.
- 2010 **Student Travel Grant Awards**, CCS, Chicago, IL.
- 2010 **Moon-Jung Chung Scholarship**, Korean Computer Scientists and Engineers Association in America, Vienna, VA.
- 2010 **Carnegie Institute of Technology Dean's Tuition Fellowship**, Carnegie Mellon University, Pittsburgh, PA.
- 2007 **Korea Research Foundation Science Scholarship**, Korea University, Seoul, Korea.

Conference Publications

- [1] Sang Kil Cha, Maverick Woo, and David Brumley. Program-Adaptive Mutational Fuzzing. In *Proceedings of the IEEE Symposium on Security and Privacy (IEEE S&P)*, To appear, 2015.
- [2] Alexandre Rebert, Sang Kil Cha, Thanassis Avgerinos, and David Brumley. Optimizing Seed Selection for Fuzzing. In *Proceedings of the USENIX Security Symposium (USENIX Security)*, pages 861–875, 2014.
- [3] Thanassis Avgerinos, Alexandre Rebert, Sang Kil Cha, and David Brumley. Enhancing Symbolic Execution with Veritesting. In *Proceedings of the International Conference on Software Engineering (ICSE)*, pages 1083–1094, 2014.
ACM Distinguished Paper Award
- [4] 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 (CCS)*, pages 511–522, 2013.
- [5] 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 (IEEE S&P)*, pages 380–394, 2012.
- [6] Thanassis Avgerinos, Sang Kil Cha, Brent L.T. Hao, and David Brumley. AEG: Automatic Exploit Generation. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, pages 283–300, 2011.
- [7] 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 (CCS)*, pages 547–558, 2010.
- [8] 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 (NSDI)*, pages 377–390, 2010.

Journal Publications

- [9] Thanassis Avgerinos, Sang Kil Cha, Alexandre Rebert, Edward J. Schwartz, Maverick Woo, and David Brumley. Automatic Exploit Generation. *Communications of the ACM (CACM)*, 57(2):74–84, 2014.
- [10] 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

- [11] David Brumley, Sang Kil Cha, Thanassis Avgerinos, and Alexandre Rebert. Detecting Exploitable Bugs in Binary Code. Patent App. US 20130312103, 2013.
- [12] Weidong Cui, David Molnar, and Sang Kil Cha. Computer Memory Access Monitoring and Error Checking. Patent App. US 20130152053, 2013.
- [13] David Brumley, Thanassis Avgerinos, and Sang Kil Cha. Automated Exploit Generation. Patent App. US 20120317647, 2012.

Teaching Experience

- Spring 2011 **Teaching Assistant**
Vulnerability, Defense Systems, and Malware Analysis
Carnegie Mellon University, Pittsburgh, PA
Worked with professor David Brumley
- 2010 **Lecturer**
Introduction to Reversing and Offensive Computing
Korea University, Seoul, Korea
BK21 Short-Course Lecture on Software (12/27–12/31, 2010)
- Fall 2010 **Teaching Assistant**
Introduction to Computer and Network Security and Applied Cryptography
Carnegie Mellon University, Pittsburgh, PA
Worked with professor David Brumley
- Spring 2009 **Teaching Assistant**
Mechatronic Design
Carnegie Mellon University, Pittsburgh, PA
Worked with Professor Charles Neuman and John Dolan
- Fall 2007 **Peer Tutor**
Data Structure & Algorithm
Korea University, Seoul, Korea
Gave lectures to undergraduate peers for a semester
- Spring 2007 **Peer Tutor**
Internet Programming
Korea University, Seoul, Korea
Gave lectures to undergraduate peers for a semester

Professional Experience

- Summer 2013 **Research Intern**, *Microsoft Research, Redmond, WA*
Worked with Weidong Cui and Marcus Peinado
- Summer 2011 **Research Intern**, *Microsoft Research, Redmond, WA*
Worked with David Molnar and Weidong Cui
- 2009– **Research Assistant**, *Carnegie Mellon University, Pittsburgh, PA*
Worked with professor David Brumley
- 2003–2005 **Public Officer**, *Office of Education, SeongNam, Korea*
Worked at the office of education as part of Korean military duty

Professional Activities

- 2013– **Program Committee**
International Workshop on Information Security Applications (WISA) 2013, 2014
- 2011– **Journal Reviewer**
2 papers in IEEE Transactions on Information Forensics & Security
1 paper in Journal of Computer Virology and Hacking Techniques
1 paper in KSII Transaction on Internet and Information Systems

2010– **External Reviewer**
ACM CCS 2013
ACSAC 2013
ASIACCS 2010, 2011
IEEE S&P 2011, 2012, 2013
NDSS 2014
USENIX ATC 2014

Other Activities

2009–2011 **Hacking Competitions**, *Plaid Parliament of Pwning (PPP)*
- 2011, 7th place at Defcon 19 Final
- 2010, 1st place at 9th HUST Hacking Festival
- 2010, 1st place at RootedCon CTF
- 2010, 1st place at 8th HUST Hacking Festival
- 2009, 4th place at iCTF
- 2009, 3rd place at HackJam

2009 **Founding Member**, *Plaid Parliament of Pwning (PPP)*, Carnegie Mellon University, Pittsburgh, PA.

2009 **CSAW Research Award Finalist**, *Polytechnic Institute of New York University*, New York, NY.

Talks

2014 Optimizing Seed Selection for Fuzzing, *USENIX Security*, San Diego, CA
2013 Unleashing Mayhem on Binary Code, *KAIST Seminar*, Daejeon, Korea
2012 Bypassing Malware Analyses, *Security Workshop*, Sejong University, Seoul, Korea
2012 Symbolic Execution and Secure Software, *Korea University Seminar*, Seoul, Korea
2012 Unleashing Mayhem on Binary Code, *IEEE S&P*, San Francisco, CA
2011 Platform-Independent Programs, *Microsoft Research Seminar*, Redmond, WA
2010 Platform-Independent Programs, *ACM CCS*, Chicago, IL
2010 SplitScreen: Enabling Efficient, Distributed Malware Detection, *NSDI*, San Jose, CA