HONG HU

Research Scientist
School of Computer Science, Georgia Institute of Technology
Coda E0970A, 756 W Peachtree St NW, Atlanta, GA 30308

hhu86@gatech.edu
https://cc.gatech.edu/~hhu86
(678) 468-0856

EDUCATION

National University of Singapore, Singapore ..... May 2016
Ph.D. in Computer Science
Dissertation: Systematic Methods for Memory Error Detection and Exploitation
Advisor: Prof. Zhenkai Liang

Huazhong University of Science of Technology, Wuhan, China ..... June 2011
B.E. in Information Security
Thesis: Cloud-Based Isolated Execution Environment

RESEARCH EXPERIENCE

Research Scientist, Georgia Institute of Technology, Atlanta, GA, USA ..... February 2019–Present
Develop platforms to reduce the attack surface of operating systems and user space programs
Detect program vulnerabilities with static analysis and program testing

Postdoctoral Fellow, Georgia Institute of Technology, Atlanta, GA, USA ..... February 2017–January 2019
Advisors: Prof. Wenke Lee and Prof. Taesoo Kim
Protect buggy programs from control-flow hijacking attacks
Study and develop tools to debloat operating system and user space programs

Research Fellow, National University of Singapore, Singapore ..... July 2016–January 2017
Advisor: Prof. Zhenkai Liang
Develop toolchains to lift binary into LLVM intermediate language (IR)

Research Assistant, National University of Singapore, Singapore ..... February 2016–June 2016
Advisor: Prof. Zhenkai Liang
Develop exploit techniques to demonstrate the Turing-Completeness of data-oriented attacks
Detect tools to automatically construct data-oriented attacks

RESEARCH INTERESTS

System security and software security, focusing on identifying new exploitation methods and building comprehensive defenses.

PUBLICATIONS

9 papers in top-tier security conferences (*Oakland, Security, CCS, NDSS*) — 5 as the first author
One paper in VLDB, the top-tier database conference
In total, I have published 14 conference papers, 6 first-authored and 8 co-authored.

Peer-Reviewed Conferences

[1] **SQUIRREL: Testing Database Management Systems with Language Validity and Coverage Feedback. (to appear)**.
Rui Zhong, Yongheng Chen, Hong Hu, Hangfan Zhang, Wenke Lee, and Dinghao Wu.
In *Proceedings of the ACM Conference on Computer and Communications Security (**CCS**)*, November 2020.

[2] **Apollo: Automatic Detection and Diagnosis of Performance Bugs in Database Management Systems (to appear)**.
Jinho Jung, Hong Hu, Joy Arulraj, Taesoo Kim, and Woonhak Kang.
In *Proceedings of the International Conference on Very Large Data Bases (**VLDB**)*, September 2020.

[3] **Desensitization: Privacy-Aware and Attack-Preserving Crash Report**.
Ren Ding*, Hong Hu*, Wen Xu, and Taesoo Kim.
In *Proceedings of the Annual Network and Distributed System Security Symposium (**NDSS**)*, February 2020.
*** Co-first authors.**

[4] **Where Does It Go? Refining Indirect-Call Targets with Multi-Layer Type Analysis**.
Kangjie Lu and Hong Hu.
In *Proceedings of the ACM Conference on Computer and Communications Security (**CCS**)*, November 2019.
Best paper award.

[5] **Razor: A Framework for Post-deployment Software Debloating**.
Chenxiong Qian*, Hong Hu*, Mansour Alharthi, Simon Pak Ho Chung, Taesoo Kim, and Wenke Lee.
In *Proceedings of the USENIX Security Symposium (**Security**)*, August 2019.
*** Co-first authors.**

[6] **Fuzzification: Anti-Fuzzing Techniques**.
Jinho Jung, Hong Hu, David Solodukhin, Daniel Pagan, Kyu Hyung Lee, and Taesoo Kim.
In *Proceedings of the USENIX Security Symposium (**Security**)*, August 2019.

[7] **Enforcing Unique Code Target Property for Control-Flow Integrity**.
Hong Hu, Chenxiong Qian, Carter Yagemann, Simon Pak Ho Chung, William R. Harris, Taesoo Kim, and Wenke Lee.
In *Proceedings of the ACM Conference on Computer and Communications Security (**CCS**)*, October 2018.

[8] **The "Web/Local" Boundary Is Fuzzy - A Security Study of Chrome's Process-based Sandboxing**.
Yaoqi Jia, Zheng Leong Chua, Hong Hu, Shuo Chen, Prateek Saxena, and Zhenkai Liang.
In *Proceedings of the ACM Conference on Computer and Communications Security (**CCS**)*, October 2016.

[9] **Data-Oriented Programming: On the Expressiveness of Non-Control Data Attacks**.
Hong Hu, Shweta Shinde, Sendroiu Adrian, Zheng Leong Chua, Prateek Saxena, and Zhenkai Liang.
In *Proceedings of the IEEE Symposium on Security and Privacy (**Oakland**)*, May 2016.

[10] **Identifying Arbitrary Memory Access Vulnerabilities in Privilege-Separated Software**.
Hong Hu, Zheng Leong Chua, Zhenkai Liang, and Prateek Saxena.
In *Proceedings of the European Symposium on Research in Computer Security (**ESORICS**)*, September 2015.

[11] **Automatic Generation of Data-Oriented Exploits**.
Hong Hu, Zheng Leong Chua, Sendroiu Adrian, Prateek Saxena, and Zhenkai Liang.
In *Proceedings of the USENIX Security Symposium (**Security**)*, August 2015.

[12] **DroidVault: A Trusted Data Vault for Android Devices**.
Xiaolei Li, Hong Hu, Guangdong Bai, Yaoqi Jia, Zhenkai Liang, and Prateek Saxena.
In *Proceedings of the International Conference on Engineering of Complex Computer Systems (**ICECCS**)*, August 2014.
Best paper award.

[13] **Practical Analysis Framework for Software-based Attestation Scheme**.
Li Li, Hong Hu, Jun Sun, Yang Liu, and Jin Song Dong.
In *Proceedings of the International Conference on Formal Engineering Methods (**ICFEM**)*, November 2014.

[14] **A Quantitative Evaluation of Privilege Separation in Web Browser Designs**.
Xinshu Dong, Hong Hu, Zhenkai Liang, and Prateek Saxena.
In *Proceedings of the European Symposium on Research in Computer Security (**ESORICS**)*, September 2013.

Industrial Conference/Short Paper/Poster

[15] **Discovering Hidden Properties to Attack the Node.js Ecosystem**.
Feng Xiao, Jianwei Huang, Yichang Xiong, Guangliang Yang, Hong Hu, Guofei Gu, and Wenke Lee.
In *Black Hat USA Briefings*, August 2020.

[16] **On the Effectiveness of Kernel Debloating via Compile-time Configuration (position paper)**.
Mansour Alharthi, Hong Hu, Hyungon Moon, and Taesoo Kim.
In *First International Workshop on SoftwAre debLoating And Delayering (SALAD 2018)*, July 2018.

[17] **Automatically Assessing Crashes from Heap Overflows (short paper)**.
Liang He, Yan Cai, Hong Hu, Purui Su, Zhenkai Liang, Yi Yang, Huafeng Huang, Jia Yan, Xiangkun Jia, and Dengguo Feng.
In *the 32nd IEEE/ACM International Conference on Automated Software Engineering (ASE 2017)*, October 2017.

[18] **Dereference Under the Influence (DUI), You Can't Afford It (poster)**.
Hong Hu, Zheng Leong Chua, Zhenkai Liang, and Prateek Saxena.
In *22nd Network and Distributed System Security Symposium (NDSS 2015)*, 2015.

Honors and Awards

Best Paper Award, the 26th CCS	2019
Best Paper Award, the 19th ICECCS	2014
Student Travel Grant, the 24th USENIX Security	2015
NUS Research Scholarship, National University of Singapore	2011-2015
Meritorious Winner, the Mathematical Contest in Modeling	2010
Google Excellence Scholarship, Google	2010
National Endeavor Fellowship, China Ministry of Education	2010
National Scholarship, China Ministry of Education	2008,2009

Research Grants

I have participated in the preparation of nine proposals, where three haven been awarded with $10.4 million dollars in total. I am the Co-PI of two proposals and one of them has been awarded, with details shown as follows.

Toward Autonomous Reasoning of Weird Machines in the Presence of Memory-safety Issues

Agency/Company: Defense Advanced Research Projects Agency (DARPA)
Total Dollar Amount: $805,070 Role: co-PI
Period of Contract: 01/2020 - 06/2021 Collaborators: Taesoo Kim (PI)
* I led the proposal preparation; two of my research papers [9, 11] become the foundation for this grant.

Professional Activities

Program Committee Member

ACM ASIA Conference on Computer and Communications Security (ASIACCS)	2019

External Reviewer

Network and Distributed System Security Symposium (NDSS)	2020,2019,2018,2017,2016,2015,2014
IEEE Symposium on Security and Privacy (IEEE S&P)	2019,2018,2016,2015,2014
ACM Conference on Computer and Communications Security (CCS)	2019,2018,2017,2015,2014
USENIX Security Symposium	2018,2016,2014
USENIX Symposium on Operating Systems Design and Implementation (OSDI)	2018

USENIX Annual Technical Conference (ATC) 2019,2018
European Conference on Computer Systems (EuroSys) 2018

Journal Reviewer

IEEE Transactions on Computers (TC) 2018, 2016
IEEE Transactions on Information Forensics and Security (TIFS) 2018

TEACHING EXPERIENCE

CS4239 Software Security, Computer Science, NUS ..... Fall 2016
Teaching assistant and lab instructor. Undergraduate level course with 44 students
Help design the homework, grade homeworks and teach the lab experiments
Lecturer: Prof. Roland Yap

CS5231 Systems Security, Computer Science, NUS ..... Fall 2014
Teaching assistant. Graduate level course with 73 students
Help re-design the homework, grade homeworks and evaluate the class projects
Lecturer: Prof. Zhenkai Liang (*Annual Teaching Excellence Award* year 2014-2015)

CS4238 Computer Security Practice, Computer Science, NUS ..... Fall 2013
Teaching assistant and lab instructor. Undergraduate level course with 43 students
Help re-design the homework, grade homeworks and teach the lab experiments
Lecturer: Prof. Zhenkai Liang (*Annual Teaching Excellence Award* year 2013-2014)

OPEN SOURCE CONTRIBUTION

Razor. A Framework for Post-deployment Software Debloating [5]. Co-lead author.
https://github.com/cxreet/razor

Fuzzification. Anti-Fuzzing Techniques [6]. Contributor.
https://github.com/sslab-gatech/fuzzification

uCFI. Enforcing Unique Code Target Property for Control-Flow Integrity [7]. Lead author.
https://github.com/uCFI-GATech

Chrome-attack. PoCs of Attacking Chrome to Bypass SOP [8]. Contributor.
https://github.com/jiayaoqijia/Web-Local-Attacks

DOP-Assist. Tools for Constructing Data-oriented Programming Attacks [9]. Lead author.
https://github.com/melynx/DOP-StaticAssist

Data-attacks. Examples of Data-oriented Attacks and Data-oriented Programming [9, 11]. Lead author.
Dataset

INVITED TALKS

Exploiting Program Invariants for Software Security

University of Arizona, Tucson, Arizona February 2020
University of Delaware, Newark, Delaware February 2020
University of Waterloo, Waterloo, Ontario, Canada February 2020
George Mason University, Fairfax, Virginia February 2020
Dartmouth College, Hanover, New Hampshire March 2020
Purdue University, West Lafayette, Indiana March 2020

Virginia Polytechnic Institute and State University, Arlington, Virginia — March 2020
Penn State University, Centre County, Pennsylvania — March 2020
University of North Carolina at Chapel Hill, Chapel Hill, North Carolina — March 2020

Data-Oriented Attacks: Expressiveness, Construction and Application

Intel, Hilsboro, OR, USA — July 2019
Tsinghua University, Beijing, China — February 2017
Chinese Academy of Sciences, Beijing, China, — February 2017
Georgia Tech, Atlanta, GA, USA — May 2016
ADSC, Singapore — January 2016

RAZOR: A Framework for Post-deployment Software Debloating

PLSE Seminar, Georgia Tech, Atlanta, GA, USA — October 2019

Regaining Initiative in the Eternal War in Memory

University of Arizona, Tucson, Arizona — November 2018

System Debloating via Compile-time Configuration and Hybrid Binary Rewriting (Keynote)

The FEAST workshop 2018, Toronto, ON, Canada — October 2018

Hacking Data-Flow for Turing-Complete Attacks

Cybersecurity Lecture Series, Atlanta, GA, USA — February 2018

REFERENCES

Dr. Wenke Lee (Postdoc Advisor)

The John P. Imlay Jr. Professor of Computer Science
Georgia Institute of Technology, Atlanta, GA
http://wenke.gtisc.gatech.edu/
✉ wenke@cc.gatech.edu ☎ +1 (404) 385-2879

Dr. Taesoo Kim (Postdoc co-Advisor)

Associate Professor of Computer Science
Georgia Institute of Technology, Atlanta, GA
https://taesoo.gtisc.gatech.edu/
✉ taesoo@gatech.edu ☎ +1 (404) 385-2934

Dr. Zhenkai Liang (PhD Advisor)

Associate Professor of Computer Science
National University of Singapore, Singapore
https://www.comp.nus.edu.sg/∼liangzk/
✉ liangzk@comp.nus.edu.sg ☎ +65-6516-2257

Dr. Prateek Saxena

Associate Professor of Computer Science
National University of Singapore, Singapore
https://www.comp.nus.edu.sg/∼prateeks/
✉ prateeks@comp.nus.edu.sg ☎ +65-6601-1898