

HONG HU

Assistant Professor
College of Information Sciences and Technology, Penn State University
305F, Steam Services Building, University Park, PA 16802

✉ honghu@psu.edu
🌐 <https://huhong789.github.io/>
☎ (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

WORK EXPERIENCE

Assistant Professor, Penn State University, State College, PA, USA August 2020–Present

System security and software security

Research Scientist, Georgia Institute of Technology, Atlanta, GA, USA February 2019–July 2020

Host: Prof. Wenke Lee and Prof. Taesoo Kim

Postdoctoral Fellow, Georgia Institute of Technology, Atlanta, GA, USA February 2017–January 2019

Advisors: Prof. Wenke Lee and Prof. Taesoo Kim

Research Fellow, National University of Singapore, Singapore July 2016–January 2017

Advisor: Prof. Zhenkai Liang

RESEARCH INTERESTS

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

PUBLICATIONS

14 papers in top-tier security conferences (*Oakland*, *Security*, *CCS*, *NDSS*)

One paper in the top-tier database conference (*VLDB*)

One paper in the top-tier industry security conference (*BlackHat USA*)

Peer-Reviewed Conferences

[1] Identifying Behavior Dispatchers for Malware Analysis.

Kyuhong Park, Burak Sahin, Yongheng Chen, Jisheng Zhao, Evan Downing, Hong Hu, and Wenke Lee.

In *Proceedings of the 16th ACM ASIA Conference on Computer and Communications Security (AsiaCCS 2021)*, Hong Kong, China, June 2021.

- [2] **Sharing More and Checking Less: Leaveraging Common Input Keywords to Detect Bugs in Embedded Systems (to appear).**
Libo Chen, Yanhao Wang, Quanpu Cai, Yunfan Zhan, Hong Hu, Jiaqi Linghu, Qinsheng Hou, Chao Zhang, Haixin Duan, and Zhi Xue.
In *Proceedings of the 30th USENIX Security Symposium (Security)*, Vancouver, B.C., Canada, August 2021.
- [3] **Abusing Hidden Properties to Attack the Node.js Ecosystem (to appear).**
Feng Xiao, Jianwei Huang, Yichang Xiong, Guangliang Yang, Hong Hu, Guofei Gu, and Wenke Lee.
In *Proceedings of the 30th USENIX Security Symposium (Security)*, Vancouver, B.C., Canada, August 2021.
- [4] **Preventing Use-After-Free Attacks with Fast Forward Allocation (to appear).**
Brian Wickman, Hong Hu, Insu Yun, Daehee Jang, JungWon Lim, Sanidhya Kashyap, and Taesoo Kim.
In *Proceedings of the 30th USENIX Security Symposium (Security)*, Vancouver, B.C., Canada, August 2021.
- [5] **One Engine to Fuzz 'em All: Generic Language Processor Testing with Semantic Validation (to appear).**
Yongheng Chen, Rui Zhong, Hong Hu, Hangfan Zhang, Yupeng Yang, Dinghao Wu, and Wenke Lee.
In *Proceedings of the 42nd IEEE Symposium on Security and Privacy (Oakland)*, San Francisco, CA, May 2021.
- [6] **WINNIE: Fuzzing Windows Applications with Harness Synthesis and Fast Cloning.**
Jinho Jung, Stephen Tong, Hong Hu, Jungwon Lim, Yonghui Jin, and Taesoo Kim.
In *Proceedings of the 2021 Annual Network and Distributed System Security Symposium (NDSS)*, Virtual, February 2021.
- [7] **SQUIRREL: Testing Database Management Systems with Language Validity and Coverage Feedback.**
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.
- [8] **Apollo: Automatic Detection and Diagnosis of Performance Bugs in Database Management Systems.**
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.
- [9] **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. Top 10 Finalist, CSAW 2020.**
- [10] **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.
- [11] **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.**
- [12] **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.
- [13] **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.
- [14] **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.
- [15] **Data-Oriented Programming: On the Expressiveness of Non-Control Data Attacks.**
Hong Hu, Shweta Shinde, Sendroui Adrian, Zheng Leong Chua, Prateek Saxena, and Zhenkai Liang.
In *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, May 2016.
- [16] **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.
- [17] **Automatic Generation of Data-Oriented Exploits.**

Hong Hu, Zheng Leong Chua, Sendriu Adrian, Prateek Saxena, and Zhenkai Liang.
In *Proceedings of the USENIX Security Symposium (Security)*, August 2015.

[18] **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.

[19] **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.

[20] **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

[21] **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.

[22] **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 Delaying (SALAD 2018)*, July 2018.

[23] **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.

[24] **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

Top 10 Finalist , CSAW 2020	2020
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 [15, 17] become the foundation for this grant.

PROFESSIONAL ACTIVITIES

Program Committee Member

ACM ASIA Conference on Computer and Communications Security (ASIACCS) 2021, 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 Dependable and Secure Computing (TDSC) 2020, 2019

IEEE Transactions on Software Engineering (TSE) 2019

IEEE Transactions on Computers (TC) 2020, 2018, 2016

IEEE Transactions on Information Forensics and Security (TIFS) 2018

TEACHING EXPERIENCE

IST 454 Computer Forensics, IST, Penn State University Fall 2020

Instructor. Undergraduate level course with 56 students

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 [11]. Co-lead author.

<https://github.com/cxreet/razor>

Fuzzification. Anti-Fuzzing Techniques [12]. Contributor.

<https://github.com/sslab-gatech/fuzzification>

uCFI. Enforcing Unique Code Target Property for Control-Flow Integrity [13]. Lead author.

<https://github.com/uCFI-GATech>

Chrome-attack. PoCs of Attacking Chrome to Bypass SOP [14]. Contributor.

<https://github.com/jiayaoqijia/Web-Local-Attacks>

DOP-Assist. Tools for Constructing Data-oriented Programming Attacks [15]. Lead author.

<https://github.com/melynx/DOP-StaticAssist>

Data-attacks. Examples of Data-oriented Attacks and Data-oriented Programming [15, 17]. 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, Hillsboro, 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