HONG HU

Assistant Professor
College of Information Sciences and Technology
Pennsylvania State University

honghu@psu.edu
https://huhong789.github.io/
E312 Westgate Building
University Park, PA 16802

RESEARCH INTERESTS

System security and software security:
– focusing on identifying new exploitation methods and building comprehensive defenses

EMPLOYMENT

Penn State University, State College, PA, USA — Aug 2020 – Present
Assistant Professor at College of Information Sciences and Technology

Georgia Institute of Technology, Atlanta, GA, USA — Feb 2019 – Jul 2020
Research Scientist

Georgia Institute of Technology, Atlanta, GA, USA — Feb 2017 – Jan 2019
Postdoctoral Fellow

EDUCATION

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

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

HONORS AND AWARDS

NSF CAREER Award	2024
Best Reviewer Award, CCS	2022
Top 10 Finalist, CSAW	2020
Best Paper Award, CCS	2019
Best Paper Award, ICECCS	2014
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

PUBLICATIONS

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

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

One paper in the top-tier conference of software engineering (*ICSE*)

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

Conference Proceedings (* co-first authors)

[1] DEEPTYPE: Refining Indirect Call Targets with Strong Multi-layer Type Analysis.
Tianrou Xia, **Hong Hu**, and Dinghao Wu.
In *Proceedings of the USENIX Security Symposium (Security)*, Philadelphia, PA, August 2024.

[2] MalwareTotal: Multi-Faceted and Sequence-Aware Bypass Tactics against Static Malware Detection.
Shuai He, Cai Fu, **Hong Hu**, Jiahe Chen, Jianqiang Lv, and Shuai Jiang.
In *Proceedings of the International Conference on Software Engineering (ICSE)*, Lisbon, Portugal, April 2024.

[3] VIPER: Spotting Syscall-Guard Variables for Data-Only Attacks.
Hengkai Ye, Song Liu, Zhechang Zhang, and **Hong Hu**.
In *Proceedings of the USENIX Security Symposium (Security)*, Anaheim, CA, August 2023.

[4] μFuzz: Redesign of Parallel Fuzzing Using Microservice Architecture.
Yongheng Chen, Rui Zhong, Yupeng Yang, **Hong Hu**, Dinghao Wu, and Wenke Lee.
In *Proceedings of the USENIX Security Symposium (Security)*, Anaheim, CA, August 2023.

[5] SFuzz: Slice-based Fuzzing for Real-Time Operating Systems.
Libo Chen, Quanpu Cai, Zhenbang Ma, Yanhao Wang, **Hong Hu**, Minghang Shen, Yue Liu, Shanqing Guo, Haixin Duan, Kaida Jiang, and Zhi Xue.
In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, Los Angeles, CA, November 2022.

[6] Detecting Logical Bugs of DBMS with Coverage-based Guidance.
Yu Liang, Song Liu, and **Hong Hu**.
In *Proceedings of the USENIX Security Symposium (Security)*, Boston, MA, August 2022.

[7] FreeWill: Automatically Diagnosing Use-after-free Bugs via Reference Miscounting Detection on Binaries.
Liang He*, **Hong Hu***, Purui Su, Yan Cai, and Zhenkai Liang.
In *Proceedings of the USENIX Security Symposium (Security)*, Boston, MA, August 2022.

[8] Cooper: Testing the Binding Code of Scripting Languages with Cooperative Mutation.
Peng Xu, Yanhao Wang, **Hong Hu**, and Purui Su.
In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, April 2022.

[9] Who Goes First? Detecting Go Concurrency Bugs via Message Reordering.
Ziheng Liu, Shihao Xia, Yu Liang, Linhai Song, and **Hong Hu**.
In *Proceedings of the ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, Lausanne, Switzerland, February–March 2022.

[10] 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 ACM ASIA Conference on Computer and Communications Security (AsiaCCS)*, Hong Kong, China, June 2021.

[11] Sharing More and Checking Less: Leaveraging Common Input Keywords to Detect Bugs in Embedded Systems.
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 USENIX Security Symposium (Security)*, Vancouver, B.C., Canada, August 2021.

[12] Abusing Hidden Properties to Attack the Node.js Ecosystem.
Feng Xiao, Jianwei Huang, Yichang Xiong, Guangliang Yang, **Hong Hu**, Guofei Gu, and Wenke Lee.
In *Proceedings of the USENIX Security Symposium (Security)*, Vancouver, B.C., Canada, August 2021.

[13] Preventing Use-After-Free Attacks with Fast Forward Allocation.
Brian Wickman, **Hong Hu**, Insu Yun, Daehee Jang, JungWon Lim, Sanidhya Kashyap, and Taesoo Kim.
In *Proceedings of the USENIX Security Symposium (Security)*, Vancouver, B.C., Canada, August 2021.

[14] One Engine to Fuzz 'em All: Generic Language Processor Testing with Semantic Validation.
Yongheng Chen, Rui Zhong, **Hong Hu**, Hangfan Zhang, Yupeng Yang, Dinghao Wu, and Wenke Lee.
In *Proceedings of the IEEE Symposium on Security and Privacy (IEEE S&P)*, San Francisco, CA, May 2021.

[15] WINNIE: Fuzzing Windows Applications with Harness Synthesis and Fast Cloning.
Jinho Jung, Stephen Tong, **Hong Hu**, Jungwon Lim, Yonghwi Jin, and Taesoo Kim.
In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, Virtual, February 2021.

[16] 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.

[17] 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.

[18] Desensitization: Privacy-Aware and Attack-Preserving Crash Report.
Ren Ding*, **Hong Hu***, Wen Xu, and Taesoo Kim.
In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, February 2020.
Top 10 Finalist, CSAW 2020.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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 (IEEE S&P)*, May 2016.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

Journal Articles

[30] **BinCola: Diversity-sensitive Contrastive Learning for Binary Code Similarity Detection**.
Shuai Jiang, Cai Fu, Shuai He, Jianqiang Lv, Lansheng Han, and **Hong Hu**.
IEEE Transactions on Software Engineering (TSE), 2024.

Industrial Conference/Short Paper/Poster

[31] One Flip is All It Takes: Identifying Syscall-Guard Variables for Data-Only Attacks.
Hengkai Ye, Song Liu, Zhechang Zhang, and **Hong Hu**.
In *Black Hat Asia Briefings*, April 2024.

[32] Cooper Knows the Shortest Stave: Finding 134 Bugs in the Binding Code of Scripting Languages with Cooperative Mutation.
Peng Xu, Yanhao Wang, **Hong Hu**, and Purui Su.
In *Black Hat Asia Briefings*, May 2022.

[33] Abusing Hidden Properties to Attack the Node.js Ecosystem (poster).
Feng Xiao, Jianwei Huang, Yichang Xiong, Guangliang Yang, **Hong Hu**, Guofei Gu, and Wenke Lee.
In *the 31st USENIX Security Symposium (Security)*, Boston, MA, August 2022.

[34] 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.

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

[36] 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)*, October 2017.

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

GRANTS

CAREER: Enhancing Practical Defense Mechanisms against Memory Errors and Attacks

Role: PI

Total: $654,612 (my share 100%)

National Science Foundation (NSF)

07/01/2024 to 06/30/2029

SaTC: CORE: Small: Automatic Identification of Privilege-guard Variables for Data-only Attacks

Role: PI

Total: $590,071 (my share 100%)

National Science Foundation (NSF)

08/01/2023 to 07/31/2026

Testing the Binding Layer of Scripting Languages through Cooperative Mutation

Role: PI

Total: $31,793 (my share 100%)

IST@PSU Seed Grant

01/01/2023 to 08/17/2023

Identifying Non-Control Security-Critical Data through Program Dependence Learning

Role: PI with Peng Liu from Penn State as Co-PI

Total: $49,655 (my share 50%)

ICDS@PSU Seed Grant

05/01/2022 to 04/30/2023

Understanding the Soundness of Control-flow Integrity

Role: PI with Dinghao Wu from Penn State as Co-PI

Total: $55,000 (my share 50%)

IST@PSU Seed Grant

08/15/2021 to 08/14/2022

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

Role: Co-PI with Taesoo Kim from Georgia Tech as PI

Defense Advanced Research Projects Agency (DARPA)

Total: $805,070 (my share via sub-contract: $83,897)

01/03/2021 to 10/31/2021

PROFESSIONAL ACTIVITIES

Program Committee Member

ACM Conference on Computer and Communications Security (CCS)	2024, 2023, 2022
Network and Distributed System Security Symposium (NDSS)	2025, 2024, 2023, 2022
ACM ASIA Conference on Computer and Communications Security (ASIACCS)	2022, 2021, 2019

Journal Reviewer

IEEE Transactions on Dependable and Secure Computing (TDSC)	2023, 2022, 2021, 2020, 2019
IEEE Transactions on Software Engineering (TSE)	2020, 2019

IEEE Transactions on Computers (TC) 2020, 2018, 2016
IEEE Transactions on Information Forensics and Security (TIFS) 2018

INTERNAL SERVICES

Tenure-track Faculty Search Committe of Cybersecurity 2022-23, 2021-22
Tenure-track Faculty Search Committe of Social Justice Informatics 2020-21
Teaching Faculty Search Committe of Cybersecurity 2023-24
Faculty Annual Review Committe 2022, 2023
Graduate Advisory Committee (GAC) 2021-22
Graduate Recruiting Committee (GRC) 2022-23
Qualifying Exam Committee 2021-22, 2020-21

TEACHING

Term	Course	Enrollment	Course Quality	Instructor Quality
Spring 2024	IST 543 Foundations of Software Security - 001	35	5/5	5/5
Fall 2023	IST 454 Computer and Cyber Forensics - 002	69	5/5	5/5
Spring 2023	IST 454 Computer and Cyber Forensics - 002	64	7/7	7/7
Fall 2022	IST 454 Computer and Cyber Forensics - 002	67	7/7	7/7
Fall 2021	IST 454 Computer and Cyber Forensics - 002	63	7/7	7/7
Fall 2021	IST 454 Computer and Cyber Forensics - 001	61	7/7	7/7
Spring 2021	IST 454 Computer and Cyber Forensics - 001R	33	6/7	6/7
Spring 2021	IST 454 Computer and Cyber Forensics - 001	14	7/7	7/7
Fall 2020	IST 454 Computer and Cyber Forensics - 002	56	6/7	7/7

ADVISING

Ph.D. students

Zhechang Zhang (Fall 2023 - Present): [3, 31]
Song Liu (Fall 2022 - Present): [6, 3, 31]
Shuangpeng Bai (Fall 2022 - Present)
Hengkai Ye (Summer 2022 - Present): [3, 31]
Yu Liang (Spring 2021 - Present): [9], [6]
Shihao Xia (co-advised with Linhai Song) (Spring 2021 - Present): [9]

Thesis Committee

(Current) Tianrou Xia – PhD@PennState IST
(Current) Yu Liang – PhD@PennState IST
(Current) Shihao Xia – PhD@PennState IST
(Current) Mengting He – PhD@PennState IST
(Current) Shuofei Zhu – PhD@PennState IST
(Current) Chia-Hao Chang – PhD@PennState CSE

(Current) Yongzhe Huang – PhD@PennState CSE

(Current) Jialun Zhang – PhD@PennState CSE

(2023) Rui Zhong – PhD@PennState IST

(2023) Binchen Fang – MS@PennState IST

Qualification Committee

(2021-22) Fuzheng Duan, Wooyong Jung, Changjiang Li, Jason Lucas

(2020-21) Yalda Fazlalizadeh, Junyo Luo, Tianchun Wang, Muchao Ye

OPEN SOURCE CONTRIBUTION

Viper: A Tool for Identifying Syscall-guard Variables [3]
https://github.com/PSU-Security-Universe/viper

SQLRight: A General Platform to Test DBMS Logical Bugs [6]
https://github.com/PSU-Security-Universe/sqlright

Razor: A Framework for Post-deployment Software Debloating [20]
https://github.com/cxreet/razor

Fuzzification: Anti-Fuzzing Techniques [21]
https://github.com/sslab-gatech/fuzzification

uCFI: Enforcing Unique Code Target Property for Control-Flow Integrity [22]
https://github.com/uCFI-GATech

Chrome-attack: PoCs of Attacking Chrome to Bypass SOP [23]
https://github.com/jiayaoqijia/Web-Local-Attacks

DOP-Assist: Tools for Constructing Data-oriented Programming Attacks [24]
https://github.com/melynx/DOP-StaticAssist

Data-attacks: Examples of Data-oriented Attacks and Data-oriented Programming [24, 26]
Dataset Link

INVITED TALKS

Spotting Syscall-Guard Variables for Data-Only Attacks

National University of Singapore, Singapore — November 2023

Ensuring the Reliability and Robustness of Database Management Systems

Dagstuhl Seminar, Schloss Dagstuhl, Wadern, Germany — October-November 2023

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

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

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

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