## Mu Zhang


CONTACT INFORMATION

School of Computing
University of Utah
MEB 2168
Salt Lake City, Utah 84112

*Voice:* (315) 460-0968
*E-mail:* muzhang@cs.utah.edu
*WWW:* https://www.cs.utah.edu/ muzhang/


RESEARCH INTERESTS

Software and Systems Security, Smart Contract Security, Cyber-Physical Systems Security, Mobile Security

EDUCATION

**Syracuse University**, Syracuse, New York, USA

Ph.D., Computer & Information Science and Engineering, June, 2015

- Thesis Topic: A Semantics and Context-Aware Approach to Android Application Security
- Advisor: Heng Yin

**Southeast University**, Nanjing, China

M.E., Computer Architecture, Oct, 2008

**Southeast University**, Nanjing, China

B.E., Computer Science & Technology, July, 2004

PROFESSIONAL EXPERIENCE

**University of Utah**, Salt Lake City, Utah, USA
*Tenure-Track Assistant Professor* **Jul, 2019 – present**

**Cornell University**, Ithaca, New York, USA
*Postdoctoral Associate, Supervised by Elaine Shi* **Aug, 2017 - Jun, 2019**

**NEC Laboratories America, Inc**, Princeton, New Jersey, USA
*Researcher* **July, 2015 - July, 2017**

**Syracuse University**, Syracuse, New York, USA
*Research Assistant* **Jan, 2011 - June, 2015**
*Teaching Assistant* **October, 2010 - May, 2015**

GRANTS

**Current: Total $2.55M, My Share $1.13M**

(Sole-PI) Semantics-Aware Discovery of Advanced Persistent Threats in Cyber-Physical Systems, DARPA, 2021–2024, $681,783.

(PI) CICI:SIVD: Context-Aware Vulnerability Detection in Configurable Scientific Computing Environments, NSF, 2021–2024, $499,834. (Co-PIs: Hari Sundar, Sneha Kasera, My share 50%)

(Sole-PI) Automated and Robust Recovery of dApp Semantics for Detecting Unfair Logic, Cisco Research, 2022–2023, $65,421.

(PI) Segregated Cybersecurity Instructional Laboratory, Basic Engineering Equipment Funds (BEEF), John and Marcia Price College of Engineering, University of Utah, 2023, $47,099. (Co-PIs: Sneha Kumar Kasera, Jun Xu, Sameer Patil, Stefan Nagy, Pratik Soni, Luis Garcia. I led this project; the entire funding is for purchasing equipment.)

(Co-PI) EAGER: SaTC-EDU: Teaching Security in Undergraduate Artificial Intelligence Courses Using Transparency and Contextualization, NSF, 2020–2023, $316,000. (PI: Eliane Wiese, Co-PI:

Suresh Venkatasubramanian, My share 33%)

(Co-PI) Towards Building a Superior Cybersecurity Workforce: Comprehensive Graduate Programs in Secure Computing, Utah System of Higher Education, 2022–2024, $670,887. (PI: Sneha Kumar Kasera, Co-PI: Sameer Patil, Jun Xu, My share 5%)

(Co-PI) Computer Science Targeted Workforce Development Grant, Utah System of Higher Education, 2023–2024, $269,182. (PI: Sneha Kumar Kasera. $70,649 is budgeted for computer security lab equipment.)

## Honors and Awards

ACM SIGSOFT Distinguished Paper Award, ISSTA, 2023. The first author is my PhD student.
CCS 2022 Best Paper Honorable Mention, CCS, 2022. The first author was my postdoc.
Top Graduate Teachers Spring 2021, College of Engineering, University of Utah, 2021
ACM SIGPLAN Distinguished Paper Award, OOPSLA, 2019
All University Doctoral Prize, Syracuse University, 2016

## Publications

### Books and Book Chapters

**Mu Zhang** and Heng Yin, "Android Application Security: A Semantics and Context-Aware Approach", SpringerBriefs in Computer Science, September 2016.

### Conference Papers

Levi Taiji Li (my PhD student), Ningyu He, Haoyu Wang and **Mu Zhang**, "VetEOS: Statically Vetting EOSIO Contracts for the "Groundhog Day" Vulnerabilities", will appear in The Network and Distributed System Security Symposium (**NDSS'24**), Top-tier Conference, Acceptance Rate = 20%, San Diego, February 2024.

Yu Pan (my PhD student), Zhichao Xu (Utah student), Levi Taiji Li (my PhD student), Yunhe Yang (my PhD student) and **Mu Zhang**, "Automated Generation of Security-Centric Descriptions for Smart Contract Bytecode", appeared in the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis (**ISSTA'23**), Top-tier Conference, Acceptance Rate = 117/372 = 31%, Seattle, July 2023. **ACM SIGSOFT Distinguished Paper (9/372 = 2%)**

Sirus Shahini (Utah student), **Mu Zhang**, Mathias Payer and Robert Ricci, "Arvin: Greybox Fuzzing Using Approximate Dynamic CFG Analysis", appeared in The 18th ACM ASIA Conference on Computer and Communications Security (**AsiaCCS'23**), Second-tier Security Conference, Melbourne, Australia, July 2023.

Qingzhao Zhang, Xiao Zhu, **Mu Zhang** and Z. Morley Mao, "Automated Runtime Mitigation for Misconfiguration Vulnerabilities in Industrial Control Systems", appeared in the 25th International Symposium on Research in Attacks, Intrusions and Defenses (**RAID'22**), Second-tier Security Conference, Acceptance Rate = 35/139 = 25%, Limassol, Cyprus, October 2022.

Yue Duan (my postdoc), Xin Zhao, Yu Pan (my PhD student), Shucheng Li, Minghao Li, Fengyuan Xu and **Mu Zhang**, "Towards Automated Safety Vetting of Smart Contracts in Decentralized Applications", appeared in ACM Conference on Computer and Communications Security 2022 (**CCS'22**), Top-tier Conference, Acceptance Rate = 219/972 = 22%, Los Angeles, November 2022. **CCS 2022 Best Paper Honorable Mention (20/972 = 2%)**

Jiaping Gui (my intern at NEC Labs), Ding Li, Zhengzhang Chen, Junghwan Rhee, Xusheng Xiao, **Mu Zhang**, Kangkook Jee, Zhichun Li and Haifeng Chen, "APTrace: A Responsive System for Agile Enterprise Level Causality Analysis", appeared in 36th IEEE International Conference on

Data Engineering (**ICDE'20**, Industry and Application Track), Top-tier Conference, Acceptance Rate = 26%, Dallas, Texas, April 2020.

Joseph P. Near, David Darais, Chike Abuah, Tim Stevens, Pranav Gaddamadugu, Lun Wang, Neel Somani, **Mu Zhang**, Nikhil Sharma, Alex Shan, Dawn Song, "Duet: An Expressive Higher-order Language and Linear Type System for Statically Enforcing Differential Privacy", appeared in 2019 ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages, and Applications (**OOPSLA'19**), Top-tier Conference, Acceptance Rate = 36%, Athens, Greece, October 2019. **ACM SIGPLAN Distinguished Paper Award**

**Mu Zhang**, Chien-Ying Chen, Bin-Chou Kao, Yassine Qamsane, Yuru Shao, Yikai Lin, Elaine Shi, Sibin Mohan, Kira Barton, James Moyne, Z. Morley Mao, "Towards Automated Safety Vetting of PLC Code in Real-World Plants", appeared in the 40th IEEE Symposium on Security and Privacy (**Oakland'19**), San Francisco, CA, May 2019.

Yutao Tang, Ding Li, Zhichun Li, **Mu Zhang**, Kangkook Jee, Xusheng Xiao, Zhenyu Wu, Junghwan Rhee, Fengyuan Xu and Qun Li, "NodeMerge: Template Based Efficient Data Reduction For Big-Data Causality Analysis", appeared in The 25th ACM Conference on Computer and Communications Security (**CCS'18**), Toronto, Canada, October 2018.

Yushan Liu*****, **Mu Zhang***, Ding Li, Kangkook Jee, Zhichun Li, Zhenyu Wu, Junghwan Rhee, Prateek Mittal, "Towards a Timely Causality Analysis for Enterprise Security", appeared in Proceedings of Network and Distributed System Security Symposium (**NDSS'18**), San Diego, CA, February 2018. ***This work was conducted when the first author was an intern at NEC Labs, mentored by me, who was a Researcher at NEC.**

Yue Duan, **Mu Zhang**, Abhishek Vasisht Bhaskar, Heng Yin, Xiaorui Pan, Tongxin Li, Xueqiang Wang, XiaoFeng Wang, "Things You May Not Know About Android (Un)Packers: A Systematic Study based on Whole-System Emulation", appeared in Proceedings of Network and Distributed System Security Symposium (**NDSS'18**), San Diego, CA, February 2018.

Qian Feng, Minghua Wang, **Mu Zhang**, Rundong Zhou, Andrew Henderson and Heng Yin, "Extracting Conditional Formulas for Cross-Platform Bug Search", appeared in ACM Asia Conference on Computer and Communications Security (**ASIACCS'17**), April 2017.

Curtis Carmony, **Mu Zhang**, Xunchao Hu, Abhishek Vasisht Bhaskar and Heng Yin, "Extract Me If You Can: Abusing PDF Parsers in Malware Detectors", appeared in Proceedings of Network and Distributed System Security Symposium (**NDSS'16**), San Diego, CA, February 2016.

**Mu Zhang**, Yue Duan, Qian Feng and Heng Yin, "Towards Automatic Generation of Security-Centric Descriptions for Android Apps", appeared in the 22th ACM Conference on Computer and Communications Security (**CCS'15**), Denver, Colorado, USA, October 2015.

**Mu Zhang**, Yue Duan, Heng Yin and Zhiruo Zhao, "Semantics-Aware Android Malware Classification Using Weighted Contextual API Dependency Graphs", appeared in the 21th ACM Conference on Computer and Communications Security (**CCS'14**), Scottsdale, Arizona, USA, November 2014.

**Mu Zhang** and Heng Yin, "Efficient, Context-Aware Privacy Leakage Confinement for Android Applications without Firmware Modding", appeared in the 9th ACM Symposium on Information, Computer and Communications Security (**ASIACCS'14**), Kyoto, Japan, June 2014.

**Mu Zhang** and Heng Yin, "AppSealer: Automatic Generation of Vulnerability-Specific Patches for Preventing Component Hijacking Attacks in Android Applications", appeared in the 21st Annual Network and Distributed System Security Symposium (**NDSS'14**), San Diego, CA, February 2014.

Lok-Kwong Yan, Manjukumar Jayachandra, **Mu Zhang**, and Heng Yin, "V2E: Combining Hardware Virtualization and Software Emulation for Transparent and Extensible Malware Analysis", appeared in the Eighth Annual International Conference on Virtual Execution Environments (**VEE'12**), March 2012.

Workshop, Posters and Short Papers

Mary Hall, Ganesh Gopalakrishnan, Eric Eide, Johanna Cohoon, Jeff M. Phillips, **Mu Zhang**, Shireen Y. Elhabian, Aditya Bhaskara, Harvey Dam, Artem Yadrov, Tushar Kataria, Amir Mohammad Tavakkoli, Sameeran Joshi, Mokshagna Sai Teja Karanam, "An NSF REU Site Based on Trust and Reproducibility of Intelligent Computation: Experience Report", in The 11th Workshop on Education for High-Performance Computing (EduHPC-23), held in conjunction with SC23: The International Conference for High Performance Computing, Networking, Storage and Analysis, Denver, CO, USA, November 2023.

Yunhe Yang (my PhD), **Mu Zhang**, "From Tactics to Techniques: A Systematic Attack Modeling for Advanced Persistent Threats in Industrial Control Systems", appeared in The 1st International Workshop on Re-design Industrial Control Systems with Security (RICSS), co-located with IEEE EuroS&P 2023, Delft, Netherlands, July 2023.

Levi Taiji Li (my PhD), **Mu Zhang**, "Poster: EOSDFA: Data Flow Analysis of EOSIO Smart Contracts", appeared in ACM Conference on Computer and Communications Security 2022 (**CCS'22**), Top-tier Conference, Los Angeles, November 2022.

Nithin Chalapathi (Utah student), Vinu Joseph (Utah student), Aditya Bhaskara, **Mu Zhang**, Pavel Panchekha, Ganesh Gopalakrishnan, "Correctness-preserving Compression of Datasets and Neural Network Models", appeared in Fourth International Workshop on Software Correctness for HPC Applications (**Correctness'20**, Collocated with SC20: The International Conference for High Performance Computing, Networking, Storage and Analysis), Virtual Event, Atlanta, Georgia, November 2020

Yue Duan, **Mu Zhang**, Heng Yin and Yuzhe Tang, "Privacy-Preserving Offloading of Mobile App to the Public Cloud", appeared in the 7th USENIX Workshop on Hot Topics in Cloud Computing (**HotCloud'15**), Santa Clara, CA, July 2015.

Yue Duan, **Mu Zhang**, Heng Yin and Yuzhe Tang, "Poster: Privacy-Preserving Offloading of Mobile App to the Public Cloud", appeared in the 36th IEEE Symposium on Security and Privacy (**Oakland'15**), May 2015.

**Mu Zhang** and Heng Yin, "Transforming and Taming Privacy-Breaching Android Application", appeared in the 20th Annual Network and Distributed System Security Symposium (**NDSS'13**), **Invited Paper**, February 2013.

Lok-Kwong Yan, Manjukumar Jayachandra, **Mu Zhang**, and Heng Yin, "Transparent and extensible malware analysis by combining hardware virtualization and software emulation", appeared in the 19th Annual Network and Distributed System Security Symposium (**NDSS'12**), **Invited Paper**, February 2012.

Teaching

- CS 6491 Software and System Security, Spring 2024.
- CS 4400 Computer Systems, Fall 2023.
- CS 6956 Software and System Security, Spring 2023.
- CS 4400 Computer Systems, Fall 2022.
- CS 6956 Software and System Security, Spring 2022.
- CS 4400 Computer Systems, Fall 2021.

- CS 6956 Software Security, Spring 2021.
- CS 4400 Computer Systems, Fall 2020.
- CS 6956-001 Special Topics: Software Security, Fall 2019.

## Current & Past Students

### PhD Student

- Yu Pan (2021 - Expected 2026)
  - CCS'22 – Best Paper Honorable Mention
  - ISSTA'23 – ACM SIGSOFT Distinguished Paper
- Md Raihan Ahmed (2021 - Expected 2026)
- Levi Taiji Li (2021 - Expected 2026)
  - ISSTA'23 – ACM SIGSOFT Distinguished Paper
  - NDSS'24
- Yunhe Yang (2022- Expected 2027)
  - ISSTA'23 – ACM SIGSOFT Distinguished Paper

### Masters Student

- Shubham Mazumder (2022 - 2022)
- Mahima Pawar (2023 - 2024)
- Shital Jumbad (2023 - 2023)
- Harshitha Josyula (2023 - 2024)

### Undergraduate Student

- Shiyang Li (UROP Award recipient, Graduated 2021)
- Raj Reddy (Expected 2024)

### Postdoc

- Yue Duan (Jan 2020 - Aug 2020), now Assistant Professor at Singapore Management University.

### PhD Dissertation Committee

- Ruotong Yu (CS, Expected 2024)
- Sirus Shahini (CS, Expected 2024)
- Zhao Chang (CS, Graduated 2021)
- Yanqing Peng (CS, Expected 2022)
- Alex Palomino (ECE, Graduated 2022)
- Mohammed Masum Siraj Khan (ECE, Graduated 2022)
- Jonathan Phillip Smith (CS, Expected 2022)
- Cheng Chen (ECE, Expected 2024)
- Mehdi Ganjkhani (ECE, Expected 2025)

### MS Thesis Committee

- Jonathon Devin Brugman (CS, Graduated 2020)

## Professional Activities

### Organizer

- Workshop Co-chair, The 1st International Workshop on Re-design Industrial Control Systems with Security (RICSS, co-located with IEEE EuroS&P) 2023
- Treasurer, ACM Conference on Computer and Communications Security (CCS) 2024

### Program Committee

- ACM Conference on Computer and Communications Security (CCS) 2024
- ACM Conference on Computer and Communications Security (CCS) 2023
- ACM Conference on Computer and Communications Security (CCS) 2022
- The Network and Distributed System Security (NDSS) 2024
- The Network and Distributed System Security (NDSS) 2023

- USENIX Security Symposium 2024
- Annual Computer Security Applications Conference (ACSAC) 2023
- Annual Computer Security Applications Conference (ACSAC) 2022
- Annual Computer Security Applications Conference (ACSAC) 2021
- ACM ASIA Conference on Computer and Communications Security (ASIACCS) 2024
- ACM ASIA Conference on Computer and Communications Security (ASIACCS) 2023
- ACM ASIA Conference on Computer and Communications Security (ASIACCS) 2022
- ACM ASIA Conference on Computer and Communications Security (ASIACCS) 2021
- International Symposium on Research in Attacks, Intrusions and Defenses (RAID) 2023
- 7th Deep Learning Security and Privacy Workshop (DLSP, co-located with the 45th IEEE Symposium on Security and Privacy) 2024
- 6th Deep Learning Security and Privacy Workshop (DLSP, co-located with IEEE Symposium on Security and Privacy) 2023
- 5th Deep Learning Security Workshop (DLS, co-located with IEEE Symposium on Security and Privacy) 2022
- IEEE 5th IEEE Conference on Dependable and Secure Computing (DSC) 2022
- Workshop on Foundations of Computer Security (FCS, Affiliated with CSF) 2020
- Machine Learning for Program Analysis workshop (co-located with IJCAI-PRICAI) 2020
- 1st International Workshop on Smart Manufacturing Modeling and Analysis [SM$^2$N] (co-located with CPS-IoT week) 2019
- International Workshop on Security and Privacy for the Internet-of-Things (IoTSec, co-located with IoTDI) 2018
- ACM Conference on Computer and Communications Security (CCS) 2017 (Poster Session)

Proposal Review Panelist

- NSF SaTC 2024
- NSF SaTC 2022
- NIH Bridge2AI 2021
- NSF CPS 2019

## Internal Services

- Chair, Student-Fueled Outreach Planning Committee, Kahlert School of Computing 2023
- Associate Director, Computer Engineering Program, Price College of Engineering 2021
- Director, Computer Engineering Track, Kahlert School of Computing 2021
- Member, Hiring Committee, Kahlert School of Computing 2023
- Member, Curriculum Committee, Kahlert School of Computing 2021
- Member, Grad Visit Committee, Kahlert School of Computing 2021
- Member, Cybersecurity Search Committee, Kahlert School of Computing 2020
- Member, Graduate Admission Committee, Kahlert School of Computing 2019 – 2023
- Member, System Engineering Certificate Committee, Price College of Engineering 2019
- Member, Scholarship Committee, Price College of Engineering 2019 – 2020

## Invited & Conference Talks

- Backtracking Intrusions in Modern Industrial Internet of Things. Idaho National Laboratory, January 2024.
- Backtracking Intrusions in Modern Industrial Internet of Things. The Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University, December 2023.
- Automated Detection of Configuration-based Vulnerabilities in HPC Workload Managers. NIST 3rd High-Performance Computing Security Workshop, March 2023.
- Towards Automated Safety Vetting of Smart Contracts in Decentralized Applications. Cisco Research, September 2022.
- Neural Network-based Recovery of VM-protected Android Apps for Semantics-Aware Malware Detection. Illinois Institute of Technology, April 2022.
- Neural Network-based Recovery of VM-protected Android Apps for Semantics-Aware Malware Detection. Fudan University, Mar 2022.

- Automated Safety Vetting of Industrial Controller Code in Real-World Environments: State of the Arts and Future Work. Nanjing University, Sep 2020.
- Towards Automated Safety Vetting of PLC Code in Real-World Plants. IEEE Symposium on Security and Privacy, May 2019.
- Fighting Emerging Security Threats using a Semantics and Context-Aware Approach. Baidu X-Lab, Nov 2018.
- Towards a Timely Causality Analysis for Enterprise Security. Binghamton University, March 2018.
- Towards Automatic Generation of Security-Centric Descriptions for Android Apps. Cornell University, March 2017.
- Towards Automatic Generation of Security-Centric Descriptions for Android Apps. ACM CCS, Oct 2015.
- A Semantics and Context-Aware Approach to Android Application Security. Columbia University, February 2015.
- Semantics-Aware Android Malware Classification Using Weighted Contextual API Dependency Graphs, ACM CCS, Nov 2014.
- AppSealer: Automatic Generation of Vulnerability-Specific Patches for Preventing Component Hijacking Attacks in Android Applications, NDSS, Feb 2014.