

Ning Zhang

+1-678-964-6495, zhang.ning@wustl.edu
<https://cybersecurity.seas.wustl.edu/>

RESEARCH INTERESTS

Cyber-physical System Security: Real-time System Security; Control Security; Embodied AI Security
System/AI Security: Trusted Computing; Software and OS Security; Embedded System; LLM Security

EDUCATION

Ph.D. in Computer Science 2011 - 2016: Part time
Dissertation: *Attack and Defense with Hardware-Aided Security*
Advisor: Dr. Wenjing Lou
Virginia Polytechnic Institute and State University, VA

M.S. in Computer Science 2005 - 2007
B.S. in Computer Science, Mathematics and Economics 2000 - 2005
University of Massachusetts - Amherst, MA

PROFESSIONAL EXPERIENCE

Associate Professor 2024 - Now
Assistant Professor 2018 - 2024
Department of Computer Science and Engineering,
Washington University in St. Louis

Principal Cyber Engineer/Researcher, Technical Lead 2007 - 2018
SIGovs, Cyber Security Innovations, IIS, SAS, NCS, Raytheon

AWARDS AND HONORS

Army Presidential Early Career Award for Scientists and Engineers (PECASE), 2025
Distinguished Paper Award, USENIX Security, 2024
ARO Early Career Program (ECP) Award, 2024
Winner of FTC Voice Cloning Challenge, 2024
Outstanding Paper Award, IEEE Real-Time Systems Symposium (RTSS), 2023
Distinguished Artifact Award, USENIX Security, 2023
NSF CAREER Award, 2023
Best Paper Award, International Conference on Dependable Systems and Networks (DSN), 2023
Distinguished Paper Award, International Conference on Dependable Systems and Networks (DSN), 2023
Qualcomm Best Demo Award Runner Up, VehicleSec, NDSS 2023
Intel Research Award, 2023
Raytheon Advanced Scholar Fellowship
Raytheon Technical Honors
Raytheon Achievement Awards
Charles J. Hoff Scholarship
Massachusetts Telecommunication Council Technical Achievement Scholarship

PUBLICATIONS

Authors underlined are students supervised by me

Conference

1. Ao Li, Marion Sudvarg, Zihan Li, Sanjoy Baruah, Chris Gill, Ning Zhang
A Unified Hardware Performance Profiling Infrastructure to Measure and Manage Uncertainty
USENIX Symposium on Operating Systems Design and Implementation (OSDI), 2025
2. Ao Li, Jinwen Wang, Ning Zhang
Software Availability Protection in Cyber-Physical Systems
USENIX Security Symposium, 2025
3. Canran Wang, Jinwen Wang, Mi Zhou, Vinh Pham, Senyue Hao, Chao Zhou, Ning Zhang, Netanel Raviv
Secure Information Embedding in Forensic 3D Fingerprinting
USENIX Security Symposium, 2025
4. Zihan Li, Han Liu, Ao Li, Ching-Hsiang Chan, Yevgeniy Vorobeychik, William Yeoh, Wenjing Lou, Ning Zhang
Resilient Federated Learning on Embedded Devices with Constrained Network Connectivity
Design Automation Conference (DAC), 2025
5. Yuhao Wu, Evin Jaff, Ke Yang, Ning Zhang, Umar Iqbal
An In-Depth Investigation of Data Collection in LLM App Ecosystems
ACM Internet Measurement Conference (IMC), 2025
6. Mario Guenzel, Marion Sudvarg, Ao Li, Ning Zhang, Jian-Jia Chen
Optimal Priority Assignment for Synchronous Harmonic Tasks With Dynamic Self-Suspension
IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), 2025
7. Yuhao Wu, Franziska Roesner, Tadayoshi Kohno, Ning Zhang, Umar Iqbal
IsolateGPT: An Execution Isolation Architecture for LLM-Based Agentic Systems
Network and Distributed System Security Symposium (NDSS), 2025
8. Zelun Kong, Minkyung Park, Le Guan, Ning Zhang, Chung Hwan Kim
TZ-DataShield: Automated Data Protection for Embedded Systems via Data-Flow-Based Compartmentalization
Network and Distributed System Security Symposium (NDSS), 2025
9. Junlin Wu, Jiong Xiao Wang, Chaowei Xiao, Chenguang Wang, Ning Zhang, Yevgeniy Vorobeychik
Preference Poisoning Attacks on Reward Model Learning
IEEE Symposium on Security and Privacy (Oakland), 2025
10. Han Liu, Xianfeng Tang, Tianlang Chen, Jiapeng Liu, Indu Indu, Henry Peng Zou, Peng Dai, Roberto Fernandez Galan, Michael D Porter, Dongmei Jia, Ning Zhang, Lian Xiong
Sequential LLM Framework for Fashion Recommendation
Empirical Methods in Natural Language Processing (EMNLP), 2024
11. Zhiyuan Yu, Ao Li, Ruoyao Wen, Yijia Chen, Ning Zhang
PhySense: Defending Physically Realizable Attacks for Autonomous Systems via Consistency Reasoning
ACM Conference on Computer and Communications Security (CCS), 2024
12. Yujie Wang, Kailani Lemieux Mack, Thidapat (Tam) Chantem, Sanjoy Baruah, Ning Zhang, Bryan C. Ward
Partial Context-Sensitive Pointer Integrity for Real-time Embedded Systems
IEEE Real-Time Systems Symposium (RTSS), 2024

13. Ao Li, Ning Zhang
Data-flow Availability: Achieving Timing Assurance in Autonomous Systems
USENIX Symposium on Operating Systems Design and Implementation (OSDI), 2024
14. Han Liu, Yuhao Wu, Zhiyuan Yu, Ning Zhang
Please Tell Me More: Privacy Impact of Explainability through the Lens of Membership Inference Attack
IEEE Symposium on Security and Privacy (Oakland), 2024.
15. Yujie Wang, Ao Li, Jinwen Wang, Sanjoy Baruah, Ning Zhang
Opportunistic Data Flow Integrity for Real-time Cyber-physical Systems Using Worst Case Execution Time Reservation
USENIX Security Symposium, 2024
16. Zhiyuan Yu, Xiaogeng Liu, Shunning Liang, Zach Cameron, Chaowei Xiao, Ning Zhang
Don't Listen To Me: Understanding and Exploring Jailbreak Prompts of Large Language Models
USENIX Security Symposium, 2024
Distinguished Paper Award
17. Yuhao Wu, Jinwen Wang, Yujie Wang, Zihan Li, Shixuan Zhai, Yi He, Kun Sun, Qi Li, Ning Zhang
Here Comes a New Firmware: A Study on Vulnerabilities during Firmware Update Procedure
USENIX Security Symposium, 2024
18. Ao Li, Jinwen Wang, Sanjoy Baruah, Bruno Sinopoli, Ning Zhang
An Empirical Study of Performance Interference: Timing Violation Patterns and Impacts
IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), 2024
19. Marion Sudvarg, Ao Li, Daisy Wang, Sanjoy Baruah, Jeremy Buhler, Pontus Ekberg, Christopher Gill, Ning Zhang
Elastic Scheduling for Harmonic Task Systems
IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), 2024
20. Yujie Wang, Cailani Lemieux Mack, Xi Tan, Ning Zhang, Ziming Zhao, Sanjoy Baruah, Bryan C. Ward
InsectACIDE: Debugger-Based Holistic Asynchronous CFI for Embedded System
IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), 2024
21. Chengjie Wu, Hao Hu, Yiqin Yang, Ning Zhang, Chongjie Zhang
Planning, Fast and Slow: Online Reinforcement Learning with Action-Free Offline Data via Multiscale Planners
International Conference on Machine Learning (ICML), 2024
22. Sanjoy Baruah, Pontus Ekberg, Mehdi Hosseinzadeh, Ao Li, Bryan Ward, Ning Zhang
Who's Afraid of Butterflies? A Close Examination of the Butterfly Attack
IEEE Real-Time Systems Symposium (RTSS), 2023
Outstanding Paper Award
23. Jinwen Wang, Yujie Wang, Ning Zhang
Secure and Timely GPU Execution in Cyber-physical Systems
ACM Conference on Computer and Communications Security (CCS), 2023
24. Zhiyuan Yu, Shixuan Zhai, Ning Zhang
AntiFake: Using Adversarial Audio to Prevent Unauthorized Speech Synthesis
ACM Conference on Computer and Communications Security (CCS), 2023
25. Jiadong Lou, Xiaohan Zhang, Yihe Zhang, Xinghua Li, Xu Yuan, Ning Zhang
Devils in Your Apps: Vulnerabilities and User Privacy Exposure in Mobile Notification Systems
IEEE/IFIP International Conference on Dependable Systems and Network (DSN), 2023
Best Paper Award, Distinguished Paper Award

26. Zhiyuan Yu, Yuanhaur Chang, Shixuan Zhai, Nicholas Deily, Tao Ju, XiaoFeng Wang, Uday Jammalamadaka, Ning Zhang
Integrity Verification for 3D Printed Patient-Specific Devices via Computing Tomography
USENIX Security Symposium, 2023
Distinguished Artifact Award
27. Jinwen Wang, Yujie Wang, Ao Li, Yang Xiao, Ruide Zhang, Wenjing Lou, Y. Thomas Hou, Ning Zhang
ARI: Attestation of Real-time Mission Execution Integrity
USENIX Security Symposium, 2023
28. Zhiyuan Yu, Yuanhaur Chang, Ning Zhang, Chaowei Xiao
SMACK: Semantically Meaningful Adversarial Audio Attack
USENIX Security Symposium, 2023
29. Zhiyuan Yu, Yuhao Wu, Ning Zhang, Chenguang Wang, Yevgeniy Vorobeychik, Chaowei Xiao
Is That My Code: Benchmark Suite for IP Code Violation of Large Language Models
International Conference for Machine Learning (ICML) , 2023
30. Han Liu, Yuhao Wu, Shixuan Zhai, Bo Yuan, Ning Zhang
RIATIG: Reliable and Imperceptible Adversarial Text-to-Image Generation with Natural Prompts
IEEE/CVF Computer Vision and Pattern Recognition Conference (CVPR), 2023
31. Han Liu, Yuhao Wu, Zhiyuan Yu, Yevgeniy Vorobeychik, Ning Zhang
SlowLiDAR: Increasing the Latency of LiDAR-Based Detection Using Adversarial Examples
IEEE/CVF Computer Vision and Pattern Recognition Conference (CVPR), 2023
32. Jinwen Wang, Yuhao Wu, Han Liu, Bo Yuan, Roger Chamberlain, Ning Zhang
IP Protection in TinyML
ACM/IEEE Design Automation Conference (DAC), 2023
33. Zheyuan Ma, Xi Tan, Lukasz Ziarek, Ning Zhang, Hongxin Hu and Ziming Zhao
Return-to-Non-Secure Vulnerabilities on ARM Cortex-M TrustZone: Attack and Defense
ACM/IEEE Design Automation Conference (DAC), 2023
34. Tanmaya Mishra, Jinwen Wang, Thidapat Chantem, Ryan Gerdes, Ning Zhang
A Procrastinating Control-Flow Integrity Framework for Periodic Real-Time Systems
International Conference on Real-time Networks and Systems (RTNS), 2023
35. Shanghao Shi, Yang Xiao, Changlai Du, Md Hasan Shahriar, Ao Li, Ning Zhang, Y. Thomas Hou, and Wenjing Lou
MS-PTP: Protecting Network Timing from Byzantine Attacks
ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2023
36. A Decentralized Truth Discovery Approach to the Blockchain Oracle Problem
Yang Xiao, Ning Zhang, Wenjing Lou, Y. Tom Hou
42nd IEEE International Conference on Computer Communications (INFOCOM), 2023
37. Han Liu, Zhiyuan Yu, Mingming Zha, XiaoFeng Wang, William Yeoh, Yevgeniy Vorobeychik, Ning Zhang
When Evil Calls: Targeted Adversarial Voice over IP Network
ACM Conference on Computer and Communications Security (CCS), 2022
38. Zhiyuan Yu, Zhuohang Li, Yuanhaur Chang, Skylar Fong, Jian Liu, Ning Zhang
HeatDeCam: Detecting Hidden Spy Cameras via Thermal Emissions
ACM Conference on Computer and Communications Security (CCS), 2022
39. Jinwen Wang, Ao Li, Haoran Li, Chenyang Lu, and Ning Zhang
RT-TEE: Real-time System Availability for Cyber-physical Systems
IEEE Symposium on Security and Privacy (Oakland), 2022

40. Ao Li, Marion Sudvarg, Han Liu, Zhiyuan Yu, Chris Gill, Ning Zhang
PolyRhythm: Adaptive Tuning of a Multi-Channel Attack Template for Timing Interference
IEEE Real-Time Systems Symposium (RTSS), 2022
41. Ao Li, Han Liu, Jinwen Wang, Ning Zhang
From Timing Variations to Performance Degradation: Understanding and Mitigating the Impact of Software Execution Timing in SLAM
IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2022
42. Reward Delay Attacks on Deep Reinforcement Learning
Anindya Sarkar, Jiarui Feng, Yevgeniy Vorobeychik, Christopher Gill, Ning Zhang
Conference on Decision and Game Theory for Security (GameSec), 2022
43. Huifeng Zhu, Zhiyuan Yu, Weidong Cao, Ning Zhang, Xuan Zhang
PowerTouch: A Security Objective-Guided Automation Framework for Generating Wired Ghost Touch Attacks on Touchscreens
IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2022
44. Ning Wang, Yang Xiao, Yimin Chen, Ning Zhang, Wenjing Lou, Y. Thomas Hou
Squeezing More Utility via Adaptive Clipping on Differentially Private Gradients in Federated Meta-Learning
Annual Computer Security Applications Conference (ACSAC), 2022
45. Jiameng Shi, Le Guan, Wenqiang Li, Dayou Zhang, Ping Chen, Ning Zhang
HARM: Hardware-assisted Continuous Re-randomization for Microcontrollers
IEEE European Symposium on Security and Privacy (EuroSecP), 2022
46. Manav Kulshrestha, Mingyang Xie, Ayan Chakrabarti, Ning Zhang, Yevgeniy Vorobeychik
PROVES: Establishing Image Provenance using Semantic Signatures
IEEE Winter Conference on Applications of Computer Vision (WACV), 2022
47. Jiadong Lou, Xu Yuan, Ning Zhang
Messy State of Wiring: Vulnerabilities in Emerging Personal Payment Systems
30th USENIX Security Symposium, 2021
48. Shengye Wan, Kun Sun, Ning Zhang, Yue Li
Remotely Controlling TrustZone Applications? A Study on Securely and Resiliently Receiving Remote Commands
ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2021
49. Qiben Yan, Kehai Liu, Qin Zhou, Hanqing Guo, Ning Zhang
SurfingAttack: Interactive Hidden Attack on Voice Assistants Using Ultrasonic Guided Waves
Network and Distributed System Security Symposium (NDSS), 2020
Reported by: Scientific American, Science Daily, Futurity, BBC Radio, Forbes, Popular Mechanics, Inverse, Gizmodo, FastCompany, Hackster, Techworm, CISOMAG, Android Authority, ACM TechNews.
50. Liang Tong, Aron Laszka, Chao Yan, Ning Zhang, Yevgeniy Vorobeychik
Finding Needles in a Moving Haystack: Prioritizing Alerts with Adversarial Reinforcement Learning
34th AAAI Conference on Artificial Intelligence (AAAI), 2020
51. Yang Xiao, Ning Zhang, Jin Li, Wenjing Lou, Y. Thomas Hou
Enforcing Private Data Usage Control with Blockchain and Attested Off-chain Contract Execution
25th European Symposium on Research in Computer Security (ESORICS), 2020
52. Yang Xiao, Ning Zhang, Wenjing Lou and Y. Thomas Hou
Modeling the Impact of Network Connectivity on Consensus Security of Proof-of-Work Blockchain
39th IEEE International Conference on Computer Communications (INFOCOM), 2020

53. Wei Yan, Huifeng Zhu, Zhiyuan Yu, Fatemeh Tehranipoor, John Chandy, Ning Zhang, Xuan Zhang
Bit2RNG: Leveraging Bad-page Initialized Table with Bit-error Insertion for True Random Number Generation in Commodity Flash Memory
IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2020
54. RusTEE: Developing Memory-Safe ARM TrustZone Application
Shengye Wan, Mingshen Sun, Kun Sun, Ning Zhang, Xu He
Annual Computer Security Applications Conference (ACSAC), 2020
55. Session Key Distribution Made Practical for CAN and CAN-FD Message Authentication
Yang Xiao, Shanghao Shi, Ning Zhang, Wenjing Lou, Y. Thomas Hou
Annual Computer Security Applications Conference (ACSAC), 2020
56. Ruide Zhang, Ning Zhang, Assad Moini, Wenjing Lou and Y. Thomas Hou
PrivacyScope: Automatic Analysis of Private Data Leakage in TEE-Protected Applications
40th IEEE International Conference on Distributed Computing Systems (ICDCS), 2020
57. Liang Tong, Bo Li, Chen Hajaj, Chaowei Xiao, Ning Zhang, Yevgeniy Vorobeychik,
Improving Robustness of ML Classifiers against Realizable Evasion Attacks Using Conserved Features,
28th USENIX Security Symposium, 2019
58. Shengye Wan, Jianhua Sun, Kun Sun, Ning Zhang, Qi Li,
SATIN: A Secure and Trustworthy Asynchronous Introspection on Multi-Core ARM Processors,
49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2019
59. Ruide Zhang, Ning Wang, Ning Zhang, Zheng Yan, Wenjing Lou and Y. Thomas Hou
PriRoster: Privacy-preserving Radio Context Attestation in Cognitive Radio Network
IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), 2019
60. Ning Zhang, Jin Li, Wenjing Lou, and Y. Thomas Hou,
PrivacyGuard: Enforcing Private Data Usage with Blockchain and Attested Execution,
13th International Workshop on Data Privacy Management (DPM), co-located with ESORICS, 2018
61. Ning Zhang, Wenhai Sun, Wenjing Lou, Y. Thomas Hou, Wade Trappe,
ROSTER: Radio Context Attestation in Cognitive Radio Network,
6th IEEE Conference on Communications and Network Security (CNS), 2018
62. Wenhai Sun, Ning Zhang, Wenjing Lou, Y. Thomas Hou,
Tapping the Potential: Enabling Leakage-controlled Chunk-based Deduplication on Encrypted Storage in the Cloud,
6th IEEE Conference on Communications and Network Security (CNS), 2018
63. Mohannad Alhanahnah, Qiben Yan, Ning Zhang, Zhenxiang Chen,
Towards Efficient Signature Generation and Classification of Cross-Architecture IoT Malware,
6th IEEE Conference on Communications and Network Security (CNS), 2018
64. Chen Cao, Le Guan, Ning Zhang, Neng Gao, Jingqiang Lin, Peng Liu, Ji Xiang, Wenjing Lou,
CryptMe: Practical Memory Encryption for ARM Devices,
21st International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2018
65. Ning Zhang, Kun Sun, Deborah Shands, Wenjing Lou, Y. Thomas Hou,
TruSense: Information Leakage from TrustZone,
37th IEEE International Conference on Computer Communications (INFOCOM), 2018
66. Ning Zhang, Ruide Zhang, Qiben Yan, Wenjing Lou, Y. Thomas Hou, Danfeng Yao,
Black Penguin: On the Feasibility of Detecting Intrusion with Homogeneous Memory
Network Forensic Workshop, IEEE Conference on Communications and Network Security (CNS), 2017

67. Wenhai Sun, Ning Zhang, Wenjing Lou, Y. Thomas Hou,
When Gene Meets Cloud: Enabling Scalable and Efficient Range Query on Encrypted Genomic Data,
36th IEEE International Conference on Computer Communications (INFOCOM), 2017
68. Ruide Zhang, Ning Zhang, Changlai Du, Wenjing Lou, Y. Thomas Hou, Yuichi Kawamoto,
From Electromyogram to Password: Exploring the Privacy Impact of Wearables in Augmented Reality,
ACM Transactions on Intelligent Systems and Technology (TIST), 2017
69. Ruide Zhang, Ning Zhang, Changlai Du, Wenjing Lou, Y. Thomas Hou, Yuichi Kawamoto,
AugAuth: Shoulder-Surfing Resistant Authentication for Augmented Reality,
IEEE International Conference on Communications (ICC), 2017
70. Ning Zhang, Kun Sun, Wenjing Lou, Y. Thomas Hou,
CaSE: Cache-Assisted Secure Execution on ARM Processors,
37th IEEE Symposium on Security and Privacy (Oakland), San Jose, CA, May 2016
71. Ning Zhang, He Sun, Kun Sun, Wenjing Lou, Y. Thomas Hou,
CacheKit: Evading Memory Introspection Using Cache Incoherence,
1st IEEE European Symposium on Security and Privacy (EuroS&P), 2016
72. Ning Zhang, Kun Sun, Wenjing Lou, Y. Thomas Hou, Sushil Jajodia,
Now You See Me: Hide and Seek in Physical Address Space,
10th ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2015
73. Ning Zhang, Wenjing Lou, Xuxian Jiang, Y. Thomas Hou,
Enabling Trusted Data-Intensive Execution in Cloud Computing,
2nd IEEE Conference on Communications and Network Security (CNS), 2014
74. Ning Zhang, Ming Li, Wenjing Lou, Y. Thomas Hou,
MUSHI: Toward Multiple Level Security Cloud with Strong Hardware Level Isolation,
IEEE Military Communications Conference (MILCOM), 2012
75. Ning Zhang, Ming Li, Wenjing Lou,
Distributed Data Mining with Differential Privacy,
IEEE International Conference on Communications (ICC), 2011

Conference Short Papers

1. Yuhao Wu, Yujie Wang, Shixuan Zhai, Zihan Li, Ao Li, Jinwen Wang, Ning Zhang
Measuring Security Protection in Real-time Embedded Firmware
IEEE Real-Time Systems Symposium (RTSS), 2022
2. Ao Li, Jinwen Wang, Ning Zhang
Chronos: Timing Interference as a New Attack Vector on Autonomous Cyber-physical Systems
ACM Conference on Computer and Communications Security (CCS), 2021
3. Brian Tung, Zhiyuan Yu, Ning Zhang
Towards Automated Computational Auditing of mHealth Security and Privacy Regulations
ACM Conference on Computer and Communications Security (CCS), 2021

Book Chapters

1. Yang Xiao, Ning Zhang, Jin Li, Wenjing Lou, Y. Thomas Hou,
Distributed Consensus Protocols and Algorithms,
Blockchain for Distributed Systems Security, First Edition. Wiley Sons, 2019
2. Ning Zhang,
Ransomware
Encyclopedia of Cryptography, Security and Privacy, 2022

Journal

1. Marion Sudvarg, Jordan Sun, Ao Li, Chris Gill and Ning Zhang
Priority-Based Concurrency and Shared Resource Access Mechanisms for Nested Intercomponent Requests in CAMkES
Real-Time Systems, 2024
2. Xiaohan Zhang, Jinwen Wang, Yueqiang Cheng, Qi Li, Kun Sun, Yao Zheng, Ning Zhang
Interface-Based Side Channel in TEE-Assisted Networked Services
IEEE/ACM Transactions on Networking (ToN), 2024
3. Yang Xiao, Shanghao Shi, Wenjing Lou, Chonggang Wang, Xu Li, Ning Zhang, Y. Thomas Hou, Jeffrey H. Reed
Decentralized Spectrum Access System: Vision, Challenges, and a Blockchain Solution,
IEEE Wireless Communications, 2022
4. Zhiyuan Yu, Zack Kaplan, Qiben Yan, Ning Zhang,
Security and Privacy in the Emerging Cyber-Physical World: A Survey,
IEEE Communications Surveys and Tutorials, 2021
5. Xinghua Li, Yanbing Ren, Laurence T Yang, Ning Zhang, Bin Luo, Jian Weng, and Ximeng Liu,
Perturbation-hidden: Enhancement of vehicular privacy for location-based services in internet of vehicles
IEEE Transactions on Network Science and Engineering, 2020
6. Yang Xiao, Ning Zhang, Wenjing Lou, and Y. Thomas Hou,
A Survey of Distributed Consensus Protocols for Blockchain Networks,
IEEE Communications Surveys and Tutorials, 2020
7. Wei Yan, Ning Zhang, Laurent L Njilla, Xuan Zhang,
PCBChain: Lightweight Reconfigurable Blockchain Primitives for Secure IoT Applications,
IEEE Transactions on Very Large Scale Integration (VLSI) System, 2020
8. Yaxing Chen, Wenhai Sun, Ning Zhang, Qinghua Zheng, Wenjing Lou, and Y. Thomas Hou,
Towards Efficient Fine-grained Access Control and Trustworthy Data Processing for Remote Monitoring Services in IoT,
IEEE Transactions on Information Forensics and Security (TIFS), 2019
9. Ning Zhang, Ruide Zhang, Kun Sun, Wenjing Lou, Y. Thomas Hou, Sushil Jajodia,
Memory Forensic Challenges under Misused Architectural Features,
IEEE Transactions on Information Forensics and Security (TIFS), 2018

Workshop Papers

1. Jinwen Wang, Ao Li, Haoran Li, Chenyang Lu, and Ning Zhang
RT-TEE: Real-time System Availability for Cyber-physical Systems
Symposium on Vehicle Security and Privacy (VehicleSec) with Network and Distributed System Security (NDSS) Symposium, 2023
Qualcomm Best Demo Award Runner Up
2. Meles Gebreyesus Weldegebriel. Neal Patwari. Ning Zhang and Jie Wang,
Pseudonymity: Precise, Private Closed Loop Control for Spectrum Reuse with Passive Receivers,
Workshop on Digital Spectrum Twinning, IEEE International Conference on RFID, 2022
3. Ethan Gaebel, Ning Zhang, Wenjing Lou, Y. Thomas Hou,
Looks Good to Me: Authentication for Augmented Reality,
6th International Workshop on Trustworthy Embedded Devices, 23rd ACM Conference on Computer and Communications Security (TRUSTED CCS), 2016

INVITED LECTURE

- Security Seminar, Northeastern University, 2024
- CSE Seminar, University of Michigan, Ann Arbor, 2024
- Invited Talk, Intel Labs, 2023
- CSE Colloquium Talk, Penn State University, 2023
- Graduate Student Seminar, Wayne State University, 2023
- Jasper Lecture Series, Washington University, 2023
- CERIAS Security Seminar, Purdue University, 2022
- Department Seminar, George Mason University, 2022
- Cornell Systems Lunch, Cornell University, 2018

TEACHING

Washington University in St. Louis

- CSE 433S: Introduction to Computer Security Fall 2020 - Now

Fall 2024, Role: Instructor, Student Body: Undergraduate/Graduate = 24/9

Evaluation: Overall: 6 (Department Average: 5.5), Inclusive: 6.75 (Department Average: 6.09)

Fall 2023, Role: Instructor, Student Body: Undergraduate/Graduate = 31/9

Evaluation: Overall: 5.54 (Department Average: 5.16), Inclusive: 6.67 (Department Average: 5.92)

Fall 2022, Role: Instructor, Student Body: Undergraduate/Graduate = 27/10

Evaluation: Overall: 5.87 (Department Average: 5.25), Inclusive: 6.52 (Department Average: 5.93)

Fall 2021, Role: Instructor, Student Body: Undergraduate/Graduate = 21/14

Evaluation: Overall: 5.94 (Department Average: 5.45), Inclusive: 6.60 (Department Average: 6.06)

Fall 2020, Role: Co-Instructor with Prof. Steve Cole, Student Body: Undergraduate/Graduate = 55/17

Evaluation: Overall: 5.33 (Department Average: 5.82), Inclusive: 6.53 (Department Average: 6.20)

- CSE 569S: Recent Advances in Computer Security and Privacy Spring 2021-Now

Spring 2024, Role: Instructor, Student Body: Undergraduate/Graduate = 2/9

Evaluation: Overall : 6.75 (Department Average: 5.54), Inclusive : 6.88 (Department Average: 6.10)

Spring 2022, Role: Instructor, Student Body: Undergraduate/Graduate = 3/29

Evaluation: Overall : 6.54 (Department Average: 5.44), Inclusive : 6.74 (Department Average: 6.02)

Spring 2021, Role: Instructor, Student Body: Undergraduate/Graduate = 2/9

Evaluation: Overall : 6.60 (Department Average: 5.83), Inclusive : 7.00 (Department Average: 6.26)

Fall 2019, Role: Instructor, Student Body: Undergraduate/Graduate = 2/26

Evaluation: Overall: 5.83 (Department Average: 5.48), Inclusive: 6.71 (Department Average: 6.03)

- CSE 7300: Research Seminar on Software Systems Spring, Fall 2022

Fall 2022, Student Body: Undergraduate/Graduate = 0/8

Evaluation: Overall : 7 (Department Average: 5.25) Inclusive : 7 (Department Average: 5.93)

Spring 2022, Student Body: Undergraduate/Graduate = 0/8

Evaluation: Overall : 6.75 (Department Average: 5.44) Inclusive : 6.75 (Department Average: 6.02)

- CSE 569S: Advanced IoT, Real-Time, and Embedded Systems Security (Newly Developed) Fall 2019
 Role: Instructor, Student Body: Undergraduate/Graduate = 2/26
 Evaluation: Overall: 5.83 (Department Average: 5.48), Inclusive: 6.71 (Department Average: 6.03)
- CSE 637S: Software Security (Newly Developed) Spring 2019
 Role: Instructor, Student Body: Undergraduate/Graduate = 6/25
 Evaluation: Overall: 6.73 (Department Average: 5.77) Inclusive: 6.62 (Department Average: 6.16)
- CSE 571S: Network Security (Newly Developed) Fall 2018
 Student Body: Undergraduate/Graduate = 2/14
 Evaluation: Overall: 6.63 (Department Average: 5.46), Inclusive: 6.86 (Department Average: 5.99)

Virginia Polytechnic Institute and State University

- ECE/CS 5984: Information Security Fall 2017
 Role: Instructor, Level: Graduate, Material: Newly Developed
 Overall Evaluation: 6.53/7

ADVISING

PhD Student

- Ruide Zhang (co-advising with Dr. Wenjing Lou) Sep 2014 - May 2020
 Thesis title: *Hardware-Aided Privacy Protection and Cyber Defense for IoT*
 First Job: Research and Development Security Engineer at Byte Dance (TikTok)
- Jinwen Wang Sep 2019 - Now
- Zhiyuan Yu Sep 2019 - Now
- Ao Li Sep 2021 - Now
- Yuhao Wu (Co-advised with Umar Iqbal starting 2024) Sep 2021 - Now
- Oliver Yuanhaur Chang Sep 2021 - Now
- Han Liu Sep 2021 - Now
- Tomson Li Sep 2023 - Now
- Ching-Hsiang Chan Jan 2025 - Now
- Steven Thompson Jan 2025 - Now (Spring 2025 as research staff)

Master Student

- Evin Jaff Sep 2023 - Dec 2024
- Rico Coleman Sep 2023 - May 2024
- Xinhang Yuan Sep 2023 - May 2024
- Zishuai Liu Sep 2023 - May 2024
- Matthew Kim Jan 2023 - Dec 2023
- Guorui Li May 2023 - Sep 2023
- Shunning Liang May 2023 - Aug 2023
- Lien Zhu Sep 2022 - May 2023
- Tomson Li Sep 2022 - May 2023
- Jack Zhai Sep 2022 - May 2023
- Ben Gilman Sep 2022 - May 2023

- Yara Alsiyat Jan 2022 - Dec 2022
- Jacob Gilhaus Jan 2022 - May 2022
- Zack Kaplan Jan 2021 - Dec 2021
- Clare Yuqian Huo Jan 2021 - Dec 2021
- Brian Tung Sep 2020 - May 2021
- Zhenyi Zhang Sep 2020 - May 2021
- Matthew Venezia Sep 2020 - May 2021
- Joe Albert Sep 2020 - May 2021
- Yizhe Yang Jan 2021 - May 2021
- Nicholas Deily Jan 2020 - May 2020
- Wenjie Qiu Sep 2019 - May 2020
- Elaine Cole Sep 2019 - May 2020
- Ighor Tavares Sep 2019 - May 2020
- Griffin Shaw Sep 2019 - May 2020
- Zixuan Li Sep 2019 - May 2020
- Kaiye Yu Sep 2019 - May 2020
- Arvind Radhakrishnan May 2019 - Aug 2019

Undergraduate

- Will Rosenberg Sep 2023 - Now
- Yijia Chen Sep 2023 - Dec 2023
- Kaiyue Jiang Sep 2023 - Dec 2023
- Elysia Quah May 2023 - Dec 2023
- Mitchell Oldham May 2023 - Aug 2023
- Aroon Sankoh Jan 2023 - May 2023
- Louie Kolter (Valedictorian) Sep 2022 - May 2023
- Annika Petrikin Sep 2022 - May 2023
- Sherry Zhang Sep 2022 - May 2023
- Trystan Ng Sep 2022 - Dec 2022
- Tobias Pristupin Sep 2022 - Dec 2022
- Young Lin Jan 2022 - Aug 2022
- Noah Maguigad Sep 2021 - Now
- Jack Zhai Sep 2021 - May 2022
- Ben Gilman Jan 2022 - May 2022
- Skylar Fong May 2021 - Dec 2021
- Nicole Emi May 2021 - Aug 2021
- Diva Harsoor Jan 2021 - Dec 2021
- Molly Issac Jan 2021 - May 2021
- William Gozlan Jan 2021 - May 2021
- Zack Kaplan Jan 2020 - May 2020
- Charlie Ziegenbein Jan 2020 - May 2020
- Thomas Ellis Sep 2019 - May 2020
- Hakkyung Lee May 2019 - March 2020
- Ryan Xu Jan 2019 - Dec 2019
- Renhao Liu Jan 2019 - May 2019
- Will Zhao Summer 2019

PhD Dissertation Committee

- Meles Weldegebriel Washington University, TBD
- Adith Bloor Washington University, TBD
- Van Nhat Huy Phan Rutgers University, 2025
- Hongchao Zhang Washington University, 2025
- Junli Wu Washington University, 2025
- Ali Ghubaish Washington University, TBD
- Dor Rahav Washington University, 2023
- Jinghan Yang Washington University, 2023
- Huifeng Zhu Washington University, 2023
- Mustafizur Rahman Washington University, 2023
- Yang Xiao Virginia Tech, 2022
- Tanmaya Mishra Virginia Tech, 2022
- Maede Zolanvari Washington University, 2021
- Tara Salman Washington University, 2021
- Liang Tong Washington University, 2021
- Haoran Li Washington University, 2021
- Dolvara Gunatilaka Washington University, 2020
- Lav Gupta Washington University, 2019
- Wenhai Sun Virginia Tech, 2018

Student Mentoring

- Jay Yujie Wang (Graduated under Dr. Michael Brent) Sep 2021 - Oct 2024
First Job: Software Engineer at Amazon
- Yang Xiao (Advisor: Dr. Wenjing Lou) Sep 2018 - May 2022
First Job: Assistant Professor at University of Kentucky
- Jiadong Lou (Advisor: Dr. Xu Yuan) Sep 2019 - Sep 2021
- Xiaohan Zhang (Advisor: Dr. Xinghua Li) Sep 2019 - Sep 2021
First Job: Faculty at Shanghai Jiaotong University

ACADEMIC ACTIVITIES AND SERVICES

Editorial Board

- IEEE/ACM Transactions on Networking: 2020 - Now
- IEEE Transactions on Information Forensics and Security: 2023 - Now
- Special Issue on Security and Privacy of Safety-critical Cyber-physical Systems on ACM Transaction of Cyber-physical Systems, 2025

Panelist

- NSF Panelist: 2017, 2020, 2021, 2022, 2023, 2024, 2025
- Workshop on Distributed Ledger of Things 2018

Program/Track Chairs

- IEEE Military Communications Conference (Milcom) 2025: Track 3: Cybersecurity and Trusted Computing TPC Co-Chair
- ACM Conference on Computer and Communications Security (CCS) 2025: Artifact Evaluation Co-chair
- 10th ACM Workshop on Moving Target Defense (MTD), In conjunction with the ACM Conference on Computer and Communications Security (CCS) 2023: TPC Chair
- IEEE International Conference on Computer Communications and Networks (ICCCN) 2023: Cybersecurity Track TPC chair

Conference Organization

- Symposium on Vehicle Security and Privacy (VehicleSec), USENIX Security 2025: General Chair
- IEEE Conference on Communications and Network Security (CNS) 2025: Publication Chair
- Symposium on Vehicle Security and Privacy (VehicleSec), Network and Distributed System Security Symposium (NDSS) 2024: Publicity Chair
- IEEE Conference on Communications and Network Security 2021: Panel co-chair
- ACM Conference on Security and Privacy in Wireless and Mobile Networks 2020: Student travel grant chair

Technical Program Committee

- IEEE Symposium on Security and Privacy (Oakland): 2024, 2025
- ACM Conference on Computer and Communications Security (CCS): 2022, 2023, 2024
- USENIX Security Symposium (Security): 2024, 2025
- IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS): 2024
- IEEE Real-Time Systems Symposium (RTSS): 2024
- ACM ASIA Conference on Computer and Communications Security (ASIACCS): 2022, 2023, 2024, 2025
- ISOC The Network and Distributed System Security Symposium (NDSS): 2022
- IEEE European Symposium of Security and Privacy (EuroS&P): 2023
- Annual Computer Security Applications Conference (ACSAC): 2023
- International Conference on Security and Privacy in Communication Systems (SecureComm): 2022
- IEEE International Conference on Computer Communications (INFOCOM): 2019 - 2025
- Design Automation Conference (DAC): 2022, 2023, 2024
- IEEE International Conference on Communication (ICC): 2018, 2019, 2020
- ACM Conference on Security and Privacy in Wireless and Mobile Networks: 2020
- IEEE Conference on Communications and Network Security: 2020, 2021, 2022, 2023

Research Ethics Committee

- USENIX Security Symposium (Security): 2025

Journal Review

- ACM Transaction on Privacy and Security
- ACM Transaction on Cyber-physical System
- ACM Transactions on Reconfigurable Technology and Systems
- IEEE Journal on Emerging and Selected Topics in Circuits and Systems
- IEEE Transactions on Dependable and Secure Computing
- IEEE Transactions on Emerging Topics in Computing
- IEEE Transactions on Computers
- IEEE Transactions on Mobile Computing
- IEEE Transactions on Information Forensics and Security
- IEEE/ACM Transactions on Networking
- IEEE Transaction on Vehicle Technology
- Artificial Intelligence Review
- KSII Transactions on Internet and Information Systems

UNIVERSITY SERVICES AND COMMUNITY OUTREACH

Standardization Services

- IEEE Three-Dimensional (3D) Bioprinting of Tissue-Engineered Medical Products (TEMPs) Working Group

University Services

- Faculty Search Committee: 2019, 2022

- Primary Coordinator of Master of Cybersecurity Engineering (CySE): 2018 - Now
- Doctoral Study Committee: 2021 - Now
- Doctoral Student Admission - Cybersecurity Area Lead: 2018 - Now

Community Outreach

- Whitehouse Technical Meeting: 2024
- USENIX Security Mentoring Event: 2024
- IEEE Symposium of Security and Privacy Speed Mentoring: 2022
- Faculty Advisor of BearShell CTF Club: Jan 2019 - Now
- Domain Expert for Science Project at Sorrento Elementary: 2022
- Judge for Practicum Showcase, Center for Finance & Accounting Research, 2023
- Hosting SI-CTF at ShmooCon: 2017
- Organizational judge for Virginia Tech at the Northern Virginia Regional Science Fair: 2016