Ning Zhang

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

RESEARCH INTERESTS

System Security: Trusted computing; Vulnerability research; Blockchain

Medical Security: Medical data privacy; Medical device security; Medical IoT

Cyber-physical Security: Attack and defense with acoustic, electromagnetics and optics

TEACHING INTERESTS

Computer security and privacy, Operating system, Vulnerability research, Cryptography

EDUCATION

Ph.D. in Computer Science and Applications 2011-2016
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

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

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

PUBLICATIONS

System Security

1. 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

2. 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

3. 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

4. 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

5. 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

6. 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

7. Ning Zhang, Ruide Zhang, Kun Sun, Wenjing Lou, Y. Thomas Hou, Sushil Jajodia,
"Forensic Challenges under Misused Architectural Features,"
IEEE Transactions on Information Forensics and Security (TIFS), 2018

8. 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

9. 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

10. 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

Distributed System Security

8. 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

9. 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

10. Yang Xiao, Ning Zhang, Jing Li, 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

11. 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

12. 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 & Security (IEEE TIFS), 2018

13. 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

14. 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

15. 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

16. 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

17. 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

18. 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

19. 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

20. 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

21. 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

22. 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

23. 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

24. Ning Zhang, Ming Li, Wenjing Lou,
"Distributed Data Mining with Differential Privacy,"
IEEE International Conference on Communications (ICC), 2011

TEACHING EXPERIENCE

CSE 637S: Software Security Undergraduate/Graduate-level
Instructor Spring 2019

Design and develop new class materials for software security covering various vulnerable software patterns.

CSE 571S: Network Security Undergraduate/Graduate-level
Instructor Fall 2018

Design and develop new class materials for network security covering topics on IPSec, TLS, PKI, HTTPS network attacks and blockchain
Design homework assignments and class projects to provide both theoretical foundation and practical knowledge
Teach lectures and lead discussions

Network Security Undergraduate/Graduate-level
Instructor Fall 2017

Design and develop new class materials for network security covering topics on IPSec, TLS, PKI, HTTPS etc
Design homework assignments and class projects to provide both theoretical foundation and practical knowledge
Teach lectures and lead discussions

Security and Privacy in IoT Graduate-level
Guest Lecturer Fall 2017
Instructor: Dr. Wenjing Lou, CS, Virginia Tech
Help generate class materials, teach 5 lectures and lead discussions on system security topics of IoT

Network Security Graduate-level
Guest Lecturer Fall 2012
Instructor: Dr. Wenjing Lou, CS, Virginia Tech
Demonstration of network man-in-the-middle attack, DNS poisoning attack

Advance Computer Networks Lab Undergraduate-level
Teaching Assistant Spring 2007
Instructor: Dr. Don Towsley, CS, UMASS Amherst
Led all discussion sessions, designed and set up networking lab exercises and environments, held office hours, graded homework assignments and exams

Programming with Java Undergraduate-level
Teaching Assistant Fall 2006
Instructor: Dr. Andrew McCallum, CS, UMASS Amherst
Independently led weekly hour long discussion sessions with more than 50 students, held office hours and graded homework assignments and exams

Introduction to Networking Undergraduate-level
Teaching Assistant Fall 2005
Instructor: Dr. Jim Kurose, CS, UMASS Amherst
Led discussion sessions, held office hours and graded homework assignments and exams

ACADEMIC ACTIVITIES AND SERVICES

Panelist

- NSF Panelist: 2017,2020
- Workshop on Distributed Ledger of Things 2018

Conference Organization

- ACM Conference on Security and Privacy in Wireless and Mobile Networks 2020: Student travel grant chair

Technical Program Committee

- IEEE International Conference on Communication: 2018, 2019, 2020
- IEEE International Conference on Computer Communications: 2019, 2020
- ACM Conference on Security and Privacy in Wireless and Mobile Networks: 2020
- IEEE Conference on Communications and Network Security: 2020

Conference Review

- ACM Conference on Computer and Communications Security (CCS)
- IEEE International Conference on Computer Communications (INFOCOM)
- IEEE International Conference on Dependable Systems and Networks
- European Symposium on Research in Computer Security
- IEEE Communications and Network Security
- International Conference on Security and Privacy in Communication Networks
- IEEE Computer Society Mobile Security Technology

Journal Review

- ACM Transaction on Privacy and Security
- ACM Transaction on Cyber-physical System
- ACM Transactions on Reconfigurable Technology and Systems

- IEEE/ACM Transactions on Networking
- IEEE Transaction on Computers
- IEEE Transactions on Information Forensics and Security
- IEEE Transaction on Vehicle Technology
- Artificial Intelligence Review
- KSII Transactions on Internet and Information Systems

Volunteering

- Session Chair, ICC 2017
- Virginia Tech NVC space committee: 2013-2016
- Student Volunteer, IEEE Conference on Communications and Network Security: 2013, 2014, 2016
- Student Volunteer, NSF workshop on Wireless Security 2015

AWARDS AND HONORS

- Raytheon Advance Scholar Fellowship
- Raytheon Technical Honors
- Raytheon Achievement Awards - Multiple times
- Charles J. Hoff Scholarship
- Massachusetts Telecommunication Council Technical Achievement Scholarship
- Third place, 17th Annual Mathematics Competition at UMass Amherst
- Third place, 16th Annual Mathematics Competition at UMass Amherst

COMMUNITY INVOLVEMENT

- Recruiting at Virginia Tech Engineering Expo 2017
- Organizational judge for Virginia Tech at the Regional Science Fair 2016
- President of Graduate Student Assembly, NCR, Virginia Tech 2014–2016
- Delegate of Graduate Student Assembly, NCR, Virginia Tech 2013
- Vice president of Graduate Student Assembly, NCR, Virginia Tech 2012