Yang Xiao

Updated April 23, 2023

Email: xiaoy@uky.edu
Office: 233 James F. Hardymon Building, University of Kentucky
Phone: +1 (859) 257-3101
Web: https://yang-sec.github.io/

Research Interests

Distributed System Security, Blockchain and Decentralized Systems, Trusted and Privacy-preserving Computing, Mobile Communications and Network Security, Cyber-Physical Security

Professional Appointment

Assistant Professor 08/2022 – Present
Department of Computer Science, University of Kentucky

Graduate Research Assistant 08/2017 – 05/2022
Department of Electrical and Computer Engineering, Virginia Tech

Research Intern 05/2016 – 08/2016
Mathematics and Modeling Department, Schlumberger-Doll Research

Education

Virginia Polytechnic Institute and State University 08/2017 – 05/2022
– Ph.D. in Computer Engineering

University of Michigan 09/2015 – 04/2017
– M.S. in Electrical Engineering-Systems

Shanghai Jiao Tong University 09/2010 – 06/2014
– B.S.E. in Information Engineering
– (Secondary) B.Econ. in Finance

Selected Conference Publications

1. ARI: Attestation of Real-time Mission Execution Integrity
   J. Wang, Y. Wang, A. Li, **Y. Xiao**, R. Zhang, W. Lou, Y. Hou, N. Zhang
   USENIX Security Symposium, 2023.
2. MS-PTP: Protecting Network Timing from Byzantine Attacks
   S. Shi, **Y. Xiao**, C. Du, M. Shahriar, A. Li, N. Zhang, Y. Hou, W. Lou
   *ACM Conference on Security and Privacy in Wireless and Mobile Networks (**WiSec**), 2023.*
3. A Decentralized Truth Discovery Approach to the Blockchain Oracle Problem
   Y. Xiao, N. Zhang, W. Lou, Y. T. Hou
   *IEEE International Conference on Computer Communications (**INFOCOM**), 2023.*
4. Squeezing More Utility via Adaptive Clipping on Deferentially Private Gradients in Federated Meta-Learning
   N. Wang, **Y. Xiao**, Y. Chen, N. Zhang, W. Lou, Y. T. Hou
   *Annual Computer Security Applications Conference (**ACSAC**), 2022.*
5. CANShield: Signal-based Intrusion Detection for Controller Area Networks
   M. H. Shahriar, **Y. Xiao**, P. Moriano, W. Lou, Y. T. Hou
   *Embedded Security in Cars (**escar**) USA conference, 2022.*
6. FLARE: Defending Federated Learning against Model Poisoning Attacks via Latent Space Representations
   N. Wang, **Y. Xiao**, Y. Chen, Y. Hu, W. Lou, Y. T. Hou
   *ACM ASIA Conference on Computer and Communications Security (**AsiaCCS**), 2022.*
7. Session Key Distribution Made Practical for CAN and CAN-FD Message Authentication
   Y. Xiao, S. Shi, N. Zhang, W. Lou, Y. T. Hou
   *Annual Computer Security Applications Conference (**ACSAC**), 2020.*
8. PrivacyGuard: Enforcing Private Data Usage Control with Blockchain and Off-chain Contract Execution
   Y. Xiao, N. Zhang, J. Li, W. Lou, Y. T. Hou
   *European Symposium on Research in Computer Security (**ESORICS**), 2020.*

9. Modeling the Impact of Network Connectivity on Consensus Security of Proof-of-Work Blockchain
   Y. Xiao, N. Zhang, W. Lou, Y. T. Hou
   *IEEE International Conference on Computer Communications (**INFOCOM**), 2020.*

Book Chapters

1. Distributed Consensus Protocols and Algorithms
   Y. Xiao, N. Zhang, J. Li, W. Lou, Y. T. Hou
   Blockchain for Distributed Systems Security, Wiley & Sons, 2019

Selected Journal Publications

1. BD-SAS: Enabling Dynamic Spectrum Sharing in Low-trust Environment
   Y. Xiao, S. Shi, W. Lou, C. Wang, X. Li, N. Zhang, Y. T. Hou, J. H. Reed
   *Accepted for publication in IEEE Transactions on Cognitive Communications and Networking (**TCCN**), 2023.*
2. MANDA: On Adversarial Example Detection for Network Intrusion Detection System
   N. Wang, Y. Chen, **Y. Xiao**, Y. Hu, W. Lou, Y. T. Hou
   *In IEEE Transactions on Dependable and Secure Computing (**TDSC**), 2022.*
3. Decentralized Spectrum Access System: Vision, Challenges, and a Blockchain Solution
   Y. Xiao, S. Shi, W. Lou, C. Wang, X. Li, N. Zhang, Y. T. Hou, J. H. Reed
   In IEEE Wireless Communications, 2022.
4. Challenges and New Directions in Securing Spectrum Access Systems
   S. Shi, **Y. Xiao**, W. Lou, C. Wang, X. Li, Y. T. Hou, J. H. Reed
   *In IEEE Internet of Things Journal (**IOT-J**), 2021.*
5. A Survey of Distributed Consensus Protocols for Blockchain Networks
   Y. Xiao, N. Zhang, W. Lou, Y. T. Hou
   *In IEEE Communications Surveys & Tutorials (**COMST**), 2020.*
6. Offloading Decision in Edge Computing for Continuous Applications Under Uncertainty
   W. Chang, **Y. Xiao**, W. Lou, G. Shou
   *In IEEE Transactions on Wireless Communications (**TWC**), 2020.*

Teaching

Instructor, University of Kentucky
- CS 371: Introduction to Computer Networking — Spring 2023
- CS 585/685: Intermediate/Special Topics in Computer Science: Blockchain Technologies — Fall 2022

Guest Lecturer, Virginia Tech
- CS 5560: Fundamentals of Information Security - Cryptocurrency & Blockchain — Spring 2019

Graduate Teaching Assistant, Virginia Tech
- ECE 2534: Microcontroller Programming and Interfacing — Fall 2017

Research Grants

US National Science Foundation
- "Collaborative Research: SaTC: CORE: Medium: An Anti-tracking and Robocall-free Architecture for Next-G Mobile Networks," NSF Award #2247561, 05/01/2023–04/30/2027, $300,000 (PI)

Academic Services

Conference Organization & Program Committee
- ICCCN 2023: TPC Member
- IEEE INFOCOM 2023: Web Co-chair, Session Chair
- IEEE CNS 2020: Web Chair

Panelist
- 2019 Secure and Trustworthy CyberSpace (SaTC) PI Meeting Undergraduate Track, NSF

Journal & Conference Review
- IEEE/ACM TDSC, IEEE TON, IEEE IOT-J, INT2
- IEEE S&P, IEEE SECON, IEEE INFOCOM, ICCCN, SecureComm