Yang Xiao

Updated July 15, 2025

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

Network and Information Security
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, KY, USA

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

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

Education

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

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

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

Conference Publications

(underlined: student directly supervised; *: I am the corresponding author.)

[1] Closing the Visibility Gap: A Monitoring Framework for Verifiable Open RAN Operations
H. Yu, M. M. Al Barat, **Y. Xiao**, Y. T. Hou, W. Lou
IEEE Conference on Communications and Network Security 2025 (**CNS'25**), September 2025.

[2] Scale-MIA: A Scalable Model Inversion Attack against Secure Federated Learning via Latent Space Reconstruction
S. Shi, N. Wang, **Y. Xiao**, C. Zhang, Y. Shi, Y. T. Hou, W. Lou
Network and Distributed System Security Symposium 2025 (**NDSS'25**), February 2025.

[3] TriSAS: Toward Dependable Inter-SAS Coordination with Auditability
S. Shi, **Y. Xiao**, C. Du, Y. Shi, C. Wang, R. Gazda, Y. T. Hou, E. Burger, L. DaSilva, W. Lou
19th ACM ASIA Conference on Computer and Communications Security (**ASIACCS'24**), July 2024.

[4] AAKA: An Anti-Tracking Cellular Authentication Scheme Leveraging Anonymous Credentials
H. Yu, C. Du, **Y. Xiao**, A. Keromytis, C. Wang, R. Gazda, Y. T. Hou, W. Lou
Network and Distributed System Security Symposium 2024 (**NDSS'24**), February 2024.

[5] Rethinking Single Sign-On: A Reliable and Privacy-Preserving Alternative with Verifiable Credentials
A. D. Johnson, I. Alom, **Y. Xiao***
10th ACM Workshop on Moving Target Defense (**MTD**), November 2023. (Collocated with CCS 2023)

[6] Bijack: Breaking Bitcoin Network with TCP Vulnerabilities
S. Li, S. Shi, **Y. Xiao**, C. Zhang, Y. T. Hou, W. Lou

28th European Symposium on Research in Computer Security (**ESORICS'23**), September 2023.

[7] UCBlocker: Unwanted Call Blocking Using Anonymous Authentication
C. Du, H. Yu, **Y. Xiao**, Y. T. Hou, A. Keromytis, W. Lou
32nd USENIX Security Symposium (**USENIX Security'23**), August 2023.

[8] 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 (**USENIX Security'23**), August 2023.

[9] MS-PTP: Protecting Network Timing from Byzantine Attacks
S. Shi, **Y. Xiao**, C. Du, M. Shahriar, A. Li, N. Zhang, Y. Hou, W. Lou
16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (**WiSec'23**), May 2023.

[10] A Decentralized Truth Discovery Approach to the Blockchain Oracle Problem
Y. Xiao, N. Zhang, W. Lou, Y. T. Hou
IEEE Conference on Computer Communications 2023 (**INFOCOM'23**), May 2023.

[11] 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
38th Annual Computer Security Applications Conference (**ACSAC'22**), December 2022.

[12] Mobile Tracking in 5G and Beyond Networks: Problems, Challenges, and New Directions
C. Du, H. Yu, **Y. Xiao**, W. Lou, C. Wang, R. Gazda, Y. T. Hou
19th IEEE International Conference on Mobile Ad-Hoc and Smart Systems (**MASS'22**), October 2022.

[13] CANShield: Signal-based Intrusion Detection for Controller Area Networks
M. H. Shahriar, **Y. Xiao**, P. Moriano, W. Lou, Y. T. Hou
9th Embedded Security in Cars USA conference (**escar USA'22**), June 2022.

[14] 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
17th ACM ASIA Conference on Computer and Communications Security (**ASIACCS'22**), May 2022.

[15] Session Key Distribution Made Practical for CAN and CAN-FD Message Authentication
Y. Xiao, S. Shi, N. Zhang, W. Lou, Y. T. Hou
36th Annual Computer Security Applications Conference (**ACSAC'20**), December 2020.

[16] PrivacyGuard: Enforcing Private Data Usage Control with Blockchain and Off-chain Contract Execution
Y. Xiao, N. Zhang, J. Li, W. Lou, Y. T. Hou
25th European Symposium on Research in Computer Security (**ESORICS'20**), September 2020.

[17] 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 2020 (**INFOCOM'20**), July 2020.

Book Chapters

[1] Basic Proof-of-Stake Consensus Mechanisms
Y. Xiao*, W. Sun
Proof-of-Stake for Blockchain Networks: Fundamentals, challenges and approaches, IET, 2024

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

Journal Publications

(underlined: student directly supervised; *: I am the corresponding author.)

[1] DEXO: A Verifiable and Scalable Oracle Mechanism for Inter-DApp Data Exchange.
Y. Li, I. Alom, W. Sun, **Y. Xiao***
In *IEEE Internet of Things Journal (**IOT-J**), June 2025.*

[2] CANShield: Deep Learning-Based Intrusion Detection Framework for Controller Area Networks at the Signal-Level
M. H. Shahriar, **Y. Xiao**, P. Moriano, W. Lou, Y. T. Hou
In *IEEE Internet of Things Journal (**IOT-J**), December 2023.*

[3] 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
In *IEEE Transactions on Cognitive Communications and Networking (**TCCN**), 2023.*

[4] SofitMix: A Secure Offchain-Supported Bitcoin-Compatible Mixing Protocol
H. Xie, S. Fei, Z. Yan, **Y. Xiao**
In *IEEE Transactions on Dependable and Secure Computing (**TDSC**), 2022.*

[5] 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.*

[6] 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.*

[7] 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.*

[8] 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.*

[9] 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.*

[10] Performance Analysis of Random Access Network with Post-backoff
C. Bu, **Y. Xiao**, T. Ye, P. Wu, X. Zhang, J. Wu
In *Telecommunications Science, 2016.*

Talks, Interviews

Distributed Consensus Protocols for Blockchain
– Invited virtual talk, *IEMS 5725 Blockchain and Applications*, CUHK 4/2024

On Mobile Network Security
– Invited talk on mobile tracking and authentication, UK CyberCon'24 10/2024
– TV interviews on the anti-tracking mobile network project, UK Now and LEX 18 12/2023
– TV interview on mobile apps security for online sports betting, Fox 56 10/2023

Blockchain and Trusted Execution Environment: Security Properties, Synergies, Applications
– Invited talk, *Delta 2022 Cybersecurity Conference, UTN Facultad Regional Delta, Argentina* 11/2022

A Layered View towards Blockchain: From Consensus Security to Smart Contract Application
– Invited talk, *CS Graduate Seminars*, Virginia Tech 11/2020

Workshops, Posters

Session Key Distribution Made Practical for CAN and CAN-FD Message Authentication
– Workshop talk, *Learning from Authoritative Security Experiment Results (LASER) Workshop* 12/2020

Enforcing Private Data Usage Control with Blockchain and Attested Off-chain Contract Execution

– Poster, 2019 SaTC PI Meeting, NSF, Alexandria, VA 04/2019

A Graph Random-Walk Based Sampling Algorithm for Load Balancing in Cloud Systems

– Poster, *6th Midwest Workshop on Control and Game Theory*, Ann Arbor, MI 04/2017

Grants

US National Science Foundation

– "CAREER: Foundations of Operational Resilience and Secure Communication for Networked Real-Time Systems," NSF Award #2442382, 07/15/2025–06/30/2030, $534,264 (PI)

– "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)

Office of Naval Research

– "Byzantine Resilient Federated Learning in Sporadically Connected Wireless Networks, ONR Award #N00014-24-1-2730, subawarded through Virginia Tech, 10/01/2024–09/30/2027, $300,000 (Co-PI)

Teaching

Instructor, University of Kentucky

– CS 270: Systems Programming Fall 2025
– CS 371: Introduction to Computer Networking Spring 2023, 2024
– CS 378: Introduction to Cryptology Spring 2025
– CS 572: Network Security Fall 2023, 2024
– CS 585/685: Intermediate/Special Topics in CS: 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

Advising

PhD Students

– Yue Li University of Kentucky, 08/2023 - Now
– Ifteher Alom University of Kentucky, 08/2023 - Now
– Sudip Bhujel University of Kentucky, 08/2024 - Now

Master Students

– Yue Li University of Kentucky, 12/2022 - 05/2023

Undergrad Students

(EURF: Engineering Undergraduate Research Fellow; REU: NSF Research Experiences for Undergraduates)

– Cameron Lira (EURF) University of Kentucky, 05/2025 - 08/2023
– John Hostettler (REU) University of Kentucky, 05/2025 - 07/2023
– Gavin Prewitt (REU) University of Kentucky, 05/2025 - 07/2023
– Athan Johnson (EURF) University of Kentucky, 05/2023 - 09/2023
– William Rillo (Lab Assistant) University of Kentucky, 01/2025 - 05/2025

PhD Advisory Committee

– Xu Tao University of Kentucky, 04/2023 – Now
– Yuhang Jiang University of Kentucky, 03/2023 – Now

Master Advisory Committee

– Jacob Sobota University of Kentucky, 03/2023 – 04/2023
– Franklin Stokan University of Kentucky, 02/2023 – 04/2023
– Samuel Armstrong University of Kentucky, 10/2022 – 03/2023

Academic Services

Conference Organization

– IEEE International Conference on Computer Communications (INFOCOM) 2023, 2024: Web Chair

– IEEE Conference on Communications and Network Security (CNS) 2020: Web Chair

Technical Program Committee

– Network and Distributed System Security (NDSS) Symposium 2026
– Annual Computer Security Applications Conference (ACSAC) 2024,2025
– IEEE International Conference on Computer Communications (INFOCOM) 2024,2025
– IEEE Military Communications Conference (MILCOM) 2023-2025
– International Conference on Computer Communications and Networks (ICCCN) 2023

Panelist

– NSF Panelist 2023
– NSF SaTC PI Meeting Undergraduate Track - Student Panelist 2019

Journal Review

– IEEE/ACM Transactions on Networking (TON)
– IEEE Internet of Things Journal (IOT-J)
– IEEE Transactions on Dependable and Secure Computing (TDSC)
– IEEE Transactions on Information Forensics and Security (TIFS)
– IEEE Transactions on Communications (TCOM)
– IEEE Transactions on Computers (TC)
– ACM Transactions on Privacy and Security (TOPS)
– International Journal of Intelligent Systems (INT2)
– ACM Transactions on Cyber-Physical Systems (TCPS)

Conference Review

– EAI International Conference on Security and Privacy in Comm. Netw. (SecureComm) 2019
– IEEE International Conference on Computer Communications (INFOCOM) 2021
– IEEE International Conference on Sensing, Communication, and Networking (SECON) 2022
– IEEE Symposium on Security and Privacy (Oakland) 2023
– European Symposium on Research in Computer Security (ESORICS) 2023

University Services

Department of Computer Science, University of Kentucky

– Committee on Higher Degrees 09/2022 - 08/2024
– Hiring Committee 09/2024 - Now
– Faculty Member, Cybersecurity Certificate Program 04/2023 - Now

Awards

Distinguished Member of the INFOCOM 2024 Technical Program Committee 2024
– Awarded by the INFOCOM 2024 organizing committee

INFOCOM 2020 Student Travel Grant 2020
– Awarded by the INFOCOM 2020 organizing committee

BitShares Graduate Fellowship 2019
– Awarded by Virginia Tech CS Department, funded by BitShares Inc.

Completion of the Elite Engineer Cultivation Program in Information Engineering 2014
– Certified by Shanghai Jiao Tong University

First Prize in the 28th National Physics Contest of College Students (Shanghai Division) 2011
– Awarded by Shanghai Physics Society

Professional Memberships

– IEEE Member, Communications Society, Computer Society 11/2017 – Present
– ACM Professional Member 10/2020 – Present