

Email: xiaoy@uky.edu
Phone: +1 (859) 257-3101

Office: 233 James F. Hardyman Building, University of Kentucky
Web: <https://yang-sec.github.io/>

RESEARCH	Distributed System Security	
INTERESTS	Blockchain and Decentralized Systems Trusted and Privacy-preserving Computing Mobile Communications and Network Security Cyber-Physical Security	
PROFESSIONAL	Assistant Professor	08/2022 – Present
APPOINTMENT	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 Dissertation: <i>Blockchain and Distributed Consensus: From Security Analysis to Novel Applications</i> Advisor: Dr. Wenjing Lou	
	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	
CONFERENCE	1. Bijack: Breaking Bitcoin Network with TCP Vulnerabilities	
PUBLICATIONS	S. Li, S. Shi, Y. Xiao , C. Zhang, Y. T. Hou, W. Lou <i>European Symposium on Research in Computer Security (ESORICS)</i> , 2023.	
	2. UCBlocker: Unwanted Call Blocking Using Anonymous Authentication	
	C. Du, H. Yu, Y. Xiao , Y. T. Hou, A. Keromytis, W. Lou <i>USENIX Security Symposium (Security)</i> , 2023.	
	3. ARI: Attestation of Real-time Mission Execution Integrity	
	J. Wang, Y. Wang, A. Li, Y. Xiao , R. Zhang, W. Lou, Y. Hou, N. Zhang <i>USENIX Security Symposium (Security)</i> , 2023.	
	4. MS-PTP: Protecting Network Timing from Byzantine Attacks	
	S. Shi, Y. Xiao , C. Du, M. Shahriar, A. Li, N. Zhang, Y. Hou, W. Lou <i>ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)</i> , 2023.	
	5. A Decentralized Truth Discovery Approach to the Blockchain Oracle Problem	
	Y. Xiao , N. Zhang, W. Lou, Y. T. Hou <i>IEEE International Conference on Computer Communications (INFOCOM)</i> , 2023.	
	6. Squeezing More Utility via Adaptive Clipping on Differentially 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.

7. 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
IEEE International Conference on Mobile Ad-Hoc and Smart Systems (MASS), 2022.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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

JOURNAL

PUBLICATIONS

1. 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
Accepted for publication in IEEE Internet of Things Journal (IOT-J), 2023.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.

8. 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.

9. 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.

TEACHING

Instructor, University of Kentucky

- CS 585/685: Intermediate/Special Topics in Computer Science: Blockchain Technologies Fall 2022
- CS 371: Introduction to Computer Networking Spring 2023
- CS 572: Network Security Fall 2023

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)

ADVISING

PhD Students

- Yue Li University of Kentucky, 08/2023 - Now
- Ifteher Alom University of Kentucky, 08/2023 - Now

Master Students

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

Undergrad Students

- Athan Johnson University of Kentucky, 05/2023 - Now

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 Co-chair
- IEEE Conference on Communications and Network Security (CNS) 2020: Web Chair

Technical Program Committee

- IEEE International Conference on Computer Communications (INFOCOM) 2024
- International Conference on Computer Communications and Networks (ICCCN) 2023
- IEEE Military Communications Conference (MILCOM) 2023

Panelist

- 2019 Secure and Trustworthy CyberSpace (SaTC) PI Meeting Undergraduate Track, NSF 10/2019

- Panel: What to Expect from Grad School

Journal Review

- IEEE/ACM Transactions on Networking (TON)
- IEEE Internet of Things Journal (IOT-J)
- International Journal of Intelligent Systems (INT2)
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- Digital Communications and Networks (DCAN)

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

TALKS	Blockchain, DApps, and Trustworthy Computing	
POSTERS	– Seminar talk, <i>University of Kentucky Computer Science Keeping Current Seminars (KCS)</i>	3/2023
WORKSHOPS	Blockchain and Trusted Execution Environment: Security Properties, Synergies, and a Privacy Application	
	– Invited talk, <i>Delta 2022 Cybersecurity Conference, UTN Facultad Regional Delta, Argentina</i>	11/2022
	Session Key Distribution Made Practical for CAN and CAN-FD Message Authentication	
	– Invited talk, <i>Learning from Authoritative Security Experiment Results (LASER) Workshop</i>	12/2020
	A Layered View towards Blockchain: From Consensus Security to Smart Contract Application	
	– Invited talk, <i>CS Graduate Seminars, Virginia Tech</i>	11/2020
	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, <i>6th Midwest Workshop on Control and Game Theory, Ann Arbor, MI</i>	04/2017
AWARDS	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	– IEEE Member, Communications Society, Computer Society	11/2017 – Present
MEMBERSHIPS	– ACM Professional Member	10/2020 – Present