

**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 APPOINTMENT	<b>Assistant Professor</b> Department of Computer Science, University of Kentucky, KY, USA	08/2022 – Present
	<b>Graduate Research Assistant</b> Department of Electrical and Computer Engineering, Virginia Tech, VA, USA	08/2017 – 05/2022
	<b>Research Intern</b> Mathematics and Modeling Department, Schlumberger-Doll Research, MA, USA	05/2016 – 08/2016
EDUCATION	<b>Virginia Polytechnic Institute and State University</b> , VA, USA – Ph.D. in Computer Engineering	08/2017 – 05/2022
	<b>University of Michigan</b> , MI, USA – M.S. in Electrical Engineering-Systems	09/2015 – 04/2017
	<b>Shanghai Jiao Tong University</b> , Shanghai, China – B.S.E. in Information Engineering – (Secondary) B.Econ. in Finance	09/2010 – 06/2014
CONFERENCE PUBLICATIONS	(underlined: student directly supervised; <b>bold*</b> : I am the corresponding author.)	
	[1] TriSAS: Toward Dependable Inter-SAS Coordination with Auditability S. Shi, <b>Y. Xiao</b> , 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 ( <b>ASIACCS'24</b> ), July 2024.	
	[2] AAKA: An Anti-Tracking Cellular Authentication Scheme Leveraging Anonymous Credentials H. Yu, C. Du, <b>Y. Xiao</b> , A. Keromytis, C. Wang, R. Gazda, Y. T. Hou, W. Lou Network and Distributed System Security Symposium 2024 ( <b>NDSS'24</b> ), February 2024.	
	[3] Rethinking Single Sign-On: A Reliable and Privacy-Preserving Alternative with Verifiable Credentials <u>A. D. Johnson, I. Alom</u> , <b>Y. Xiao*</b> 10th ACM Workshop on Moving Target Defense ( <b>MTD</b> ), November 2023. (Collocated with CCS 2023)	
	[4] Bijack: Breaking Bitcoin Network with TCP Vulnerabilities S. Li, S. Shi, <b>Y. Xiao</b> , C. Zhang, Y. T. Hou, W. Lou 28th European Symposium on Research in Computer Security ( <b>ESORICS'23</b> ), September 2023.	
	[5] UCBlocker: Unwanted Call Blocking Using Anonymous Authentication C. Du, H. Yu, <b>Y. Xiao</b> , Y. T. Hou, A. Keromytis, W. Lou 32nd USENIX Security Symposium ( <b>USENIX Security'23</b> ), August 2023.	
	[6] ARI: Attestation of Real-time Mission Execution Integrity J. Wang, Y. Wang, A. Li, <b>Y. Xiao</b> , R. Zhang, W. Lou, Y. Hou, N. Zhang USENIX Security Symposium ( <b>USENIX Security'23</b> ), August 2023.	

- [7] 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.
- [8] 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.
- [9] 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  
38th Annual Computer Security Applications Conference (**ACSAC'22**), December 2022.
- [10] 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.
- [11] 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.
- [12] 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.
- [13] 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.
- [14] 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.
- [15] 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] 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  
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  
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.

	<p>[5] Decentralized Spectrum Access System: Vision, Challenges, and a Blockchain Solution  <b>Y. Xiao</b>, S. Shi, W. Lou, C. Wang, X. Li, N. Zhang, Y. T. Hou, J. H. Reed  In <i>IEEE Wireless Communications</i>, 2022.</p> <p>[6] Challenges and New Directions in Securing Spectrum Access Systems  S. Shi, <b>Y. Xiao</b>, W. Lou, C. Wang, X. Li, Y. T. Hou, J. H. Reed  In <i>IEEE Internet of Things Journal (IOT-J)</i>, 2021.</p> <p>[7] A Survey of Distributed Consensus Protocols for Blockchain Networks  <b>Y. Xiao</b>, N. Zhang, W. Lou, Y. T. Hou  In <i>IEEE Communications Surveys &amp; Tutorials (COMST)</i>, 2020.</p> <p>[8] Offloading Decision in Edge Computing for Continuous Applications Under Uncertainty  W. Chang, <b>Y. Xiao</b>, W. Lou, G. Shou  In <i>IEEE Transactions on Wireless Communications (TWC)</i>, 2020.</p> <p>[9] Performance Analysis of Random Access Network with Post-backoff  C. Bu, <b>Y. Xiao</b>, T. Ye, P. Wu, X. Zhang, J. Wu  In <i>Telecommunications Science</i>, 2016.</p>		
UNDER REVIEW	<p>[1] DEXO: A Verifiable and Scalable Oracle Mechanism for Inter-DApp Data Exchange.  <u>Y. Li</u>, <u>I. Alom</u>, W. Sun, <b>Y. Xiao</b>*  Submitted for possible conference publication.</p> <p>[2] Basic Proof-of-Stake Consensus Mechanism.  <b>Y. Xiao</b>*, W. Sun  Submitted as book chapter.</p>		
TALKS, INTERVIEWS, POSTERS	<p>On Mobile Network Security</p> <ul style="list-style-type: none"> <li>– UK Now and LEX 18 interviews on the anti-tracking mobile network project 12/2023</li> <li>– Fox 56 interview on mobile apps security for online sports betting 10/2023</li> </ul> <p>Blockchain, DApps, and Trustworthy Computing</p> <ul style="list-style-type: none"> <li>– Seminar talk, <i>University of Kentucky Computer Science Keeping Current Seminars (KCS)</i> 3/2023</li> </ul> <p>Blockchain and Trusted Execution Environment: Security Properties, Synergies, and a Privacy Application</p> <ul style="list-style-type: none"> <li>– Invited talk, <i>Delta 2022 Cybersecurity Conference, UTN Facultad Regional Delta, Argentina</i> 11/2022</li> </ul> <p>Session Key Distribution Made Practical for CAN and CAN-FD Message Authentication</p> <ul style="list-style-type: none"> <li>– Invited talk, <i>Learning from Authoritative Security Experiment Results (LASER) Workshop</i> 12/2020</li> </ul> <p>A Layered View towards Blockchain: From Consensus Security to Smart Contract Application</p> <ul style="list-style-type: none"> <li>– Invited talk, <i>CS Graduate Seminars, Virginia Tech</i> 11/2020</li> </ul> <p>Enforcing Private Data Usage Control with Blockchain and Attested Off-chain Contract Execution</p> <ul style="list-style-type: none"> <li>– Poster, 2019 SaTC PI Meeting, NSF, Alexandria, VA 04/2019</li> </ul> <p>A Graph Random-Walk Based Sampling Algorithm for Load Balancing in Cloud Systems</p> <ul style="list-style-type: none"> <li>– Poster, <i>6th Midwest Workshop on Control and Game Theory</i>, Ann Arbor, MI 04/2017</li> </ul>		
RESEARCH GRANTS	<p><b>US National Science Foundation</b></p> <ul style="list-style-type: none"> <li>– “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)</li> </ul>		
TEACHING	<p><b>Instructor</b>, University of Kentucky</p> <ul style="list-style-type: none"> <li>– CS 585/685: Intermediate/Special Topics in Computer Science: Blockchain Technologies Fall 2022</li> <li>– CS 371: Introduction to Computer Networking Spring 2023, 2024</li> <li>– CS 572: Network Security Fall 2023</li> </ul>		

**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

**Master Students**

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

**Undergrad Students**

- Athan Johnson University of Kentucky, 05/2023 - 09/2023

**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**

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

**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	<b>Department of Computer Science, University of Kentucky</b>	
SERVICES	– Committee on Higher Degrees	09/2022 - Now
	– Faculty Member, Cybersecurity Certificate Program	04/2023 - Now
AWARDS	<b>Distinguished Member of the INFOCOM 2024 Technical Program Committee</b>	2024
	– Awarded by the INFOCOM 2024 organizing committee	
	<b>INFOCOM 2020 Student Travel Grant</b>	2020
	– Awarded by the INFOCOM 2020 organizing committee	
	<b>BitShares Graduate Fellowship</b>	2019
	– Awarded by Virginia Tech CS Department, funded by BitShares Inc.	
	<b>Completion of the Elite Engineer Cultivation Program in Information Engineering</b>	2014
	– Certified by Shanghai Jiao Tong University	
	<b>First Prize in the 28th National Physics Contest of College Students (Shanghai Division)</b>	2011
	– Awarded by Shanghai Physics Society	
PROFESSIONAL	– IEEE Member, Communications Society, Computer Society	11/2017 – Present
MEMBERSHIPS	– ACM Professional Member	10/2020 – Present