Yang Xiao

Updated May 6, 2023

Email: xiaoy@uky.edu
Phone: +1 (859) 257-3101
Office: 233 James F. Hardymon Building, University of Kentucky
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
  Dissertation: *Blockchain and Distributed Consensus: From Security Analysis to Novel Applications*
  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 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. 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.*

6. 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.*

7. 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.*

8. 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.*

9. 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.*

10. 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. 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. 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.*

3. 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.*

4. 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.

5. 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.*

6. 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.*

7. 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.*

8. 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 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

Undergraduate Tutor, SJTU

- CS 358: Data Structure — Fall 2014

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

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: Web Co-chair; Session 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 Communictions and Networks (ICCCN) — 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

Talks Posters Workshops

Blockchain, DApps, and Trustworthy Computing
- Seminar talk, *University of Kentucky Computer Science Keeping Current Seminars (KCS)* 3/2023

Blockchain and Trusted Execution Environment: Security Properties, Synergies, and a Privacy Application
- Invited talk, *Delta 2022 Cybersecurity Conference, UTN Facultad Regional Delta, Argentina* 11/2022

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

A Layered View towards Blockchain: From Consensus Security to Smart Contract Application
- Invited talk, *CS Graduate Seminars*, Virginia Tech 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, *6th Midwest Workshop on Control and Game Theory*, Ann Arbor, MI 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 Memberships

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