✉ yz113@iu.edu | 1phan 1phan.com | Yifan Zhang

Assistant Professor	San Diego State University	2025.08 – present
Ph.D., Computer Science	Indiana University Bloomington *Advisor: Dr. XiaoFeng Wang, Dr. Luyi Xing*	2019.08 – 2025.07
B.Eng., Information Security	Xidian University	2015.08 – 2019.08

Research Interests

My current research interests lie in the areas of software supply chain, mobile, and IoT security and privacy. I am dedicated to uncovering new attack vectors and identifying emerging privacy issues in these domains and other emerging ecosystems. My approach utilizes program analysis, machine learning, Large Language Models (LLMs) and formal verification techniques to detect, measure, and safeguard against these newly identified security and privacy vulnerabilities.

Publications

1. **Y. Zhang**, Z. Hu, X. Wang, Y. Hong, Y. Nan, X. Wang, J. Cheng, L. Xing. "Navigating the Privacy Compliance Maze: Understanding Risks with Privacy-Configurable Mobile SDKs" **USENIX Security**, 2024.

   Real-world impacts: We reported the poor privacy practices to more than 40 Android SDK vendors. Six Android advertisement vendors acknowledged our report, and Vungle has fixed the issues in its latest version.

2. **Y. Zhang***, X. Wang*, X. Wang, Y. Jia, L. Xing. "Union under Duress: Understanding Hazards of Duplicate Resource Mismediation in Android Software Supply Chain." (* co-first author) **USENIX Security**, 2023.

   Real-world impacts: The Android Studio team acknowledged our vulnerability report. We also informed hundreds of related SDK vendors that are vulnerable to this new attack vector.

3. **Y. Zhang***, H. Chen*, X. Han*, H. Rong, Y. Zhang, T. Mao, H. Zhang, X Wang, L. Xing, X. Chen "WitheredLeaf: Finding Entity-Inconsistency Bugs with LLMs" (* co-first author) **arxiv**, 2024.

   Real-world impacts: We identified 123 new flaws in 154 Python and C GitHub repositories, each with over 1,000 stars. Of the 69 submitted fixes, 27 have been successfully merged.

4. Z. Hu*, J. Ye*, **Y. Zhang**, X. Wang "Seeing is Not Always Believing: An Empirical Analysis of Fake Evidence Generators" **EuroS&P**, 2024

5. Y. Nan, X. Wang, L. Xing, X. Liao, R. Wu, J. Wu, **Y. Zhang**, X. Wang. "Are You Spying on Me? Large-Scale Analysis on IoT Data Exposure through Companion Apps." **USENIX Security**, 2023.

   Real-world impacts: We sent more than 1,000 emails to app developers whose apps fail to disclose certain IoT data items. Twenty-one developers acknowledged our findings and updated their privacy policies. We also reported the list of apps to Google Play. Google Play responded to our request promptly and is investigating the privacy issues of these apps.

6. Y. Jia, B. Yan, L. Xing, D. Zhao, X. Wang, **Y. Zhang**, Y. Liu, K. Zheng, Y. Zhang, D. Zou, H. Jin. "Who's In Control? On Security Risks of Disjointed IoT Device Management Channels." **ACM Conference on Computer and Communications Security (CCS)**, 2021.

   Real-world impacts: We revealed security vulnerabilities in IoT devices and systems widely used by many people every day. These vulnerabilities allow attackers and cybercriminals to control smart devices belonging to others and steal personal data. The manufacturers include iRobot, HONYAR, MiHome, August, Yale, LIFX, Philips Hue, Tuya, Amazon Alexa, Wink, iHome, Abode Home Alarm, Aqara Camera, ismartgate, Koogeek, Meross, Refoss, Yeelight, Level, Ultraloq, Kwikset Aura, Honeywell, Schlage, Geonfino, Tile, Chipolo, Govee, Beurer, Belkin, WeMo, SwitchMate, Sunpro, Broil-King, Biobeat, Molekule, NetVue, Singlecue, Hippokura, SwitchBot, and Dyson.

   We reported these vulnerabilities to the respective vendors and provided security patches. The vendors acknowledged the issues and adopted our security designs and patches to fix their products.

7. H. Lu, L. Xing, Y. Xiao, **Y. Zhang**, X. Liao, X. Wang, X. Wang. "Demystifying resource management risks in emerging mobile app-in-app ecosystems." **ACM Conference on Computer and Communications Security (CCS)**, 2020.

   Real-world impacts: Our security design were implemented by Chrome, Firefox, Safari, Wechat, Alipay.

Teaching at SDSU

Instructor	CS574	Computer Security	Fall 2025

Teaching at IU

Instructor	B649	CYBER DEFENSE COMPETITIONS	Fall 2021
Co-Instructor	B546	MALWARE: THREAT AND DEFENSE	Fall 2022
Guest Instructor	B649	CYBER DEFENSE COMPETITIONS	Fall 2023
Guest Instructor	B649	CYBER DEFENSE COMPETITIONS	Fall 2024
Associate Instructor	B649	CYBER DEFENSE COMPETITIONS	Fall 2019
Associate Instructor	B433	SECURE PROTOCOLS	Spring 2021
Associate Instructor	B433	SECURE PROTOCOLS	Spring 2022

Professional Services

Program Committee: SDIoTSec 2024 , SafeThings 2024, USENIX Security (AEC) 2024
Sub-reviewer: PoPETs 2024, IEEE S&P 2022, TDSC 2022, Inscrypt 2022, WiSec 2021, NDSS 2021, CCS 2020, NDSS 2020, IEEE S&P 2020

Internship

Research Intern	Samsung Research America	Feb 26th - May 31st, 2024

Awards

- Usenix Security Travel Award, 2023
- Best Applied Security Paper Award TOP-10 Finalists, CSAW 2022.
- Defcon final 2022, team r3kapig
- HackIN 2022, 2nd place
- Acknowledged by Opera on their Security Hall of Fame, 2019
- HackIN 2019, 1st place
- Acknowledged by Tencent on their Security Hall of Fame, 2018
- Defcon final 2018, team r3kapig
- First Prize, 10th National Student Information Security Competition, 2017
- First Prize, 2nd National Student Cryptography Competition, 2016

- Grand Prize, 2016 Shaanxi Province Cyberspace Security Technology Competition (CTF)
- Second Prize, 2015 Shaanxi Province Cyberspace Security Technology Competition (CTF)