Yiwei Zhang

yiweizhang@purdue.edu | yiweiz.evie@gmail.com | Homepage

EDUCATION

Purdue University West Lafayette, IN, U.S.
Ph.D., Computer Science; Advised by Prof. Elisa Bertino *Aug. 2022 – Now*

Shanghai Jiao Tong University Shanghai, China
MS, Computer Science; GPA: 3.8/4 *Aug. 2019 – Mar. 2022*

Xidian University Xi'an, China
BS, Information Security; GPA: 3.9/4 *Aug. 2015 – July 2019*

SELECTED SKILLS

Languages: Python, C, C++, JavaScript, Java, Shell

Developer Tools: Git, Docker, Source Code Analysis (LLVM/Clang), Pytorch

Security Analysis Tools: IDA, JEB, FRIDA, Wireshark, TCPDump

Others: Linux System, IoT device development, Development board debugging, Firmware extraction

PROFESSIONAL EXPERIENCE

Purdue University West Lafayette, U.S.
Research Assistant *Aug. 2022 – Now*

- **Code Vulnerability Detection Using LLMs:** Developed and engineered custom prompts for Large Language Models (LLMs) to identify critical code components (e.g., key functions, parameters, function pointers). Integrated LLM outputs with static analysis tools (LLVM) to enhance the detection of authentication vulnerabilities in software code..

- **Quantum-Secure Federated Learning:** DDesigned and implemented post-quantum cryptographic algorithms (Kyber, Dilithium) for securing communication in federated learning environments, ensuring quantum-resistant data aggregation. Enhanced model security by incorporating Differential Privacy (DP) to defend against membership inference attacks while maintaining training efficiency.

Shanghai Jiao Tong University Shanghai, China
åResearch Assistant *Aug. 2020 – Dec. 2021*

- **NLP-Assisted Memory Vulnerability Detection:** Applied Natural Language Processing (NLP) models (TensorFlow) to automatically classify and annotate memory management functions. Combined NLP techniques with static code analysis (Clang Static Analyzer) to identify memory-related vulnerabilities such as use-after-free and double-free errors.

- **IoT Companion App Analysis:** Analyzed IoT companion (Android) apps to explore the implementation of (private) communication protocols between the devices and apps. Developed automated scripts to automatically detect security flaws caused by identifying improper use of credential based on specific patterns.
- **Smart TV Control Analysis:** Analyzed channels to remote control smart TVs, i.e., IR, BLE and Wi-Fi. Engineered scripts to construct attacks on real-world smart TVs by leveraging the multiple vulnerable channels to access protected resources of TV or even hijack the TV.

Purdue University West Lafayette, U.S.
Teaching Assistant *Aug. 2024 – Dec. 2024*

- **Programming in C languages**

PUBLICATIONS

Peer-reviewed Conferences:

- Detecting Vulnerable Custom Authentication Schemes in Router OS Add-ons. Under Review.
- Xing Han, Yuheng Zhang, Xue Zhang, Zeyuan Chen, Mingzhe Wang, **Yiwei Zhang**, Siqi Ma, Yu Yu, Elisa Bertino, Juanru Li. Medusa Attack: Exploring Security Hazards of In-App QR Code Scanning. USENIX Security 2023.

- Yunlong Lyu, Yi Fang, **Yiwei Zhang**, Qibin Sun, Siqi Ma, Elisa Bertino, Kangjie Lu, Juanru Li. Goshawk: Hunting Memory Corruptions via Structure-Aware and Object-Centric Memory Operation Synopsis. IEEE S&P 2022
- **Yiwei Zhang**, Siqi Ma, Juanru Li, Elisa Bertino, Dawu Gu. KingFisher: Unveiling Insecurely Used Credentials in IoT-to-Mobile Communications. DSN 2022.
- **Yiwei Zhang**, Juanru Li. Rethinking the Security of IoT from the Perspective of Developer Customized Device-Cloud Interaction. SAC 2022.
- Hehao Li, Yizhuo Wang, **Yiwei Zhang**, Juanru Li, Dawu Gu. PEDroid: Automatically Extracting Patches from Android App Updates. ECOOP 2022.

Peer-reviewed Journal:

- Efficient Privacy-Preserving and Resilient Federated Deep Learning in Post-Quantum Era. Under Review.
- **Yiwei Zhang**, Siqi Ma, Tiancheng Chen, Juanru Li, Robert H. Deng, Elisa Bertino. EvilScreen Attack: Smart TV Hijacking via Multi-channel Remote Control Mimicry. IEEE TDSC 2023.

REFERENCES

Prof. Elisa Bertino: Computer Science Department, Purdue University bertino@purdue.edu

Dr. Rouzbeh Behnia: University of South Florida behnia@usf.edu

Dr. Siqi Ma: The University of New South Wales, Australia siqi.ma@unsw.edu.au