Zhilong Wang

Phone: (814)699-2248
Email: izhilongwang@gmail.com
Website: https://www.linkedin.com/in/zhilong-wang-996498162/

Education

Pennsylvania State University *Aug. 2019 - Dec. 2023*

Ph.D. student in College of Information Sciences and Technology
Major: Cyber Security
Advisor: Peng Liu
Research: Deep Learning for Security-oriented Program Analysis

Nanjing University *Sept. 2016 - Jun. 2019*

M.S. in Department of Computer Science and Technology
Major: Computer Science and Technology
Advisor: Bing Mao
Research: Develop BROP prevention mechanism (Polymorphic Canary), code obfuscation scheme (ROPOB), and kernel module tracing method (HART)

Zhengzhou University *Sept. 2012 - Jul. 2016*

Earned Bachelor's Degree of Computer Science and Technology

- GPA: 3.6/4.0 Ranking: 1/240

Research Interests

Zhilong have 7 year experience in program analysis and software security and 4 year experience in deep learning. His Phd thesis is "Deep Learning for Security Oriented Program Analysis".

He enjoy adopt deep learning method to analyze vulnerable code pattern, customizing compiler (LLVM, GCC), kernel to enhance software protection. Now his is extremely interested in the vulnerabilities in large language model (LLM) and application of LLM in code analysis.

Research Projects

Recent Research Projects

- **Security of large language model:** jailbreak large language models [i].
- **Large language model for software security:** identify user privilege related variables [ii], code analysis [iii].
- **Deep learning for software vulnerability analysis:** We proposed a toolchain to automatically discover software vulnerabilities (i.e., silent buffer overflow) based on GNN-assisted dynamic data flow analysis [v].
- **Deep learning for security-critical variable identification:** We develop an automatic toolchain to find security-critical variables in software, which will facilitate the protection of important data in software [iv].
- **Deep learning for ransomware reverse engineering:** We develop an automatic method to locate the encryption loop in ransomware, which is an essential step in ransomware analysis.

Previous Research Projects

- **System security**. Hardware-assisted modular kernel protections [2].
- **Software security**. An effective detection model to prevent advanced buffer overflow attacks [4 [1],5]; Program obfuscation technique based on Return-Oriented Programming [6]; The trade-offs analysis in Control-Flow Integrity [1].

Work Experience

R&D Intern for JD.COM American through Intellipro Group Inc. *May 2021 - Aug. 2021*

- **Privacy-Preserving Machine Learning** serving cluster on Graphene-SGX.
- Develop transparent data encryption with Intel SGX enclave.

Security Software Engineer Intern at Mountain View, Bytedance Inc. *May 2022 - Aug. 2022*

- **Automatic vulnerability discovery:** taint analysis based fuzz target discovery (TAFTD) to find memory bugs.
- The developed tool discovered more than 50 software vulnerabilities.

Security Engineer – Security Assurance, Bytedance Inc. *Jan. 2024 - Current*

- **Security Assurance:** code review, penetration testing for code base of web application, Android, IOS apps.
- **Automatic code analysis:** static code analysis to for vulnerability of web application bugs (SQL injection, SSRF, and etc.) and logic bugs.

Awards & Honors

- Outstanding Graduates of Nanjing University, 2019.
- Shenzhen Stock Exchange Fellowship, 2018.
- First-Class Academic Scholarship of Nanjing University, 2016.
- The First Prize of Program Testing Competition of Henan Province, 2015.
- First-Class Scholarship of Zhengzhou University, 2013 & 2015 & 2016.
- Certification of Software Capability by China Computer Federation (CCF) : 330 Points (Top 5.11%)
- The First Prize of Microsoft Wheeled Micro-Robot Simulation Competition in China Robot Competition, Beijing, 2014.
- National Scholarship, 2014.

Publications

1. **Zhilong Wang** and Peng Liu. "GPT Conjecture: Understanding the Trade-offs between Granularity, Performance and Timeliness in Control-Flow Integrity." *Cybersecurity*, 2021.
2. Yunlan Du, Zhenyu Ning, Jun Xu, **Zhilong Wang**, Yueh-Hsun Lin, Fengwei Zhang, Xinyu Xing, and Bing Mao. "HART: Hardware-assisted Kernel Module Tracing on Arm." In Proceedings of The *25th European Symposium on Research in Computer Security (ESORICS)*, 2020.
3. Yoon-Ho Choi, Peng Liu, Zitong Shang, Haizhou Wang, **Zhilong Wang**, Lan Zhang, Junwei Zhou and Qingtian Zou. "Using Deep Learning to Solve Computer Security Challenges: A Survey." *Cybersecurity*, 2020. (The authors of this paper are listed in alphabetic order)

[1] Source Code: https://github.com/zhilongwang/PolymorphicCanaries

4. **Zhilong Wang**, Xuhua Ding, Chengbin Pang, Jian Guo, Jun Zhu and Bing Mao. "To Detect Stack Buffer Overflow With Polymorphic Canaries." In *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2018.

5. Jun Zhu, Weiping Zhou, **Zhilong Wang**, Dongliang Mu, and Bing Mao."DiffGuard: Obscuring Sensitive Information in Canary Based Protections." *International Conference on Security and Privacy in Communication Systems (SecureComm)*. Springer, Cham, 2017.

6. Dongliang Mu, Jia Guo, Wenbiao Ding, **Zhilong Wang**, Bing Mao, and Lei Shi." ROPOB: Obfuscating Binary Code via Return Oriented Programming." *International Conference on Security and Privacy in Communication Systems (SecureComm)*. Springer, Cham, 2017.

Arxiv Preprints

i. **Zhilong Wang**, Yebo Cao and Peng Liu. "Hidden You Malicious Goal Into Benign Narratives: Jailbreak Large Language Models through Logic Chain Injection" arXiv, 2024. (**Ongoing**)

ii. Haizhou Wang, **Zhilong Wang**, and Peng Liu. "A Hybrid LLM Workflow Can Help Identify User Privilege Related Variables in Programs of Any Size" arXiv, 2024.

iii. **Zhilong Wang**, Lan Zhang, Chen Cao, and Peng Liu. "The Effectiveness of Large Language Models (ChatGPT and CodeBERT) for Security-Oriented Code Analysis." arXiv, 2023.

iv. **Zhilong Wang***, Haizhou Wang*, Hong Hu, and Peng Liu. "Identifying Non-Control Security-Critical Data in Program Binaries with a Deep Neural Model." arXiv, 2021. (* equal contribution)

v. **Zhilong Wang**, Li Yu, Suhang Wang, and Peng Liu. "Spotting Silent Buffer Overflows in Execution Trace through Graph Neural Network Assisted Data Flow Analysis." arXiv, 2021.

Books

i. Peng Liu, Tao Liu, Nanqing Luo, Zitong Shang, Haizhou Wang, **Zhilong Wang**, Lan Zhang, and Qingtian Zou, "AI for Cybersecurity: A Handbook of Use Case." 2022.

Public Services

Reviewer

- The Journal of Computer Security *2021*
- The Journal of Computer Security *2022*
- The European Conference on Computer Systems (EuroSys) *2022*
- Scientific Reports *2022*
- IEEE/IFIP International Conference on Dependable Systems and Networks *2022*
- IEEE/IFIP International Conference on Dependable Systems and Networks *2023*
- The Journal PeerJ Computer Science *2023*
- The Journal of Supercomputing *2024*
- Transactions on Information Forensics & Security *2024*
- The International Conference on Security and Cryptography *2024*

External Reviewer

- IEEE/IFIP International Conference on Dependable Systems and Networks *2021*
- European Symposium on Research in Computer Security. *2022*