Zhilong Wang

Phone: (814)699-2248
Email: zzw169@psu.edu
Website: http://zhilongwang.org

Education

Pennsylvania State University *Sept. 2019 - Present*

Ph.D. student in College of Information Sciences and Technology
Major: Cyber Security
Advisor: Peng Liu

Nanjing University *Sept. 2016 - Jun. 2019*

M.S. in Department of Computer Science and Technology
Major: System and Software Security
Advisor: Bing Mao

Pennsylvania State University *Feb. 2018 - Sept. 2018*

Visiting Research Assistant in the College of Information Sciences and Technology (Co-funded by The Pennsylvania State University and myself)
Research: ARM Security, Linux Kernel Security

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

My research goal is to leverage all kinds of techniques to protect software against various threats.

- Protecting software by customizing compiler plugin, Linux kernel.
- Adopting program analysis to analyze software defects.
- Leveraging new techniques to facilitate security-oriented program analysis.

Research Projects

Recent Research Projects

- 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 [ii].
- 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 [i].
- Encryption loop identification. We develop an automatic method to locate the encryption loop in ransomware, which is an essential step in ransomware analysis.

Previous Research Projects

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

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

Awards & Honors

- Outstanding Graduates of Nanjing University, 2019.
- Scholarship of Shenzhen Stock Exchange, 2018.
- Second-Class Academic Scholarship of Nanjing University, 2017 &[2] 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.
- The First Prize of ACM Computer Programming Contest of Zhengzhou University, 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)
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***, 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)

ii. **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.

iii. Lan Zhang, Chen Cao, **Zhilong Wang**, and Peng Liu. "Which Features are Learned by CodeBert: An Empirical Study of the BERT-based Source Code Representation Learning." arXiv, 2022.

[2] Obtained annually.

Books

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

Public Services

Shadow Program Committee Member

- The European Conference on Computer Systems (EuroSys)	*2022*

Reviewer

- The Journal of Computer Security	*2021*
- The Journal of Computer Security	*2022*
- Scientific Reports	*2022*
- IEEE/IFIP International Conference on Dependable Systems and Networks	*2022*
- IEEE/IFIP International Conference on Dependable Systems and Networks	*2023*

External Reviewer

- IEEE/IFIP International Conference on Dependable Systems and Networks	*2021*