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 College of Information Sciences and Technology
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

To facilitate security-oriented program analysis through deep learning;

To detect, analyze and solve system and software problems with dynamic and static program analysis;

To deploy security strategies by modifying the operation systems and compilers;

To secure the system and software via hardware's new features (e.g., ARM ETM and AES-NI);

Research Projects

Recent Research Projects

The applications of transfer learning in solving security problem.
Deep learning assisted malware analysis and vulnerability analysis [i].
The trade-offs in control-flow integrity [ii].

Previous Research Projects

Hardware-assisted Modular Kernel Protections [1].
A effective detection model to prevent advanced buffer overflow attacks [3 [1],4]
Program obfuscation technique based on Return-oriented Programming [5].

Skills

C/Python/Java, Compiler, Linux Kernel, Program Analysis (Data Flow Analysis, Symbolic Execution, and et al.), Software and System Security, Deep Learning.

[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. 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.
2. 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)
3. **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.
4. 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.
5. 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** Li Yu, Suhang Wang, and Peng Liu. "Spotting Silent Buffer Overflows in Execution Trace through Graph Neural Network Assisted Data Flow Analysis." arXiv, 2021.

ii. **Zhilong Wang** and Peng Liu. "GPT Conjecture: Understanding the Trade-offs between Granularity, Performance and Timeliness in Control-Flow Integrity." arXiv, 2019.

[2] Obtained annually.