

# Zhilong Wang

Phone: (814)699-2248

Email: [zzw169@psu.edu](mailto: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

---

The application of deep learning and transfer learning in program analysis, system & software security and other problems.

## SKILLS

---

**I have some research and working experience in system & software & security, program analysis, and deep learning. My specialties include but are not limited to:**

- Deep learning (especially familiar with graph neural networks, and transfer learning), and its application in security.
- Program analysis (especially familiar with dynamic code analysis, e.g., data-flow analysis, symbolic execution, and etc) and its application in security .
- Development of compiler plugin, Linux kernel driver and software protection mechanisms.
- Security related hardware features, e.g., Intel Software Guard Extensions (SGX), ARM Embedded Trace Macrocell (ETM) and etc.

## WORK EXPERIENCE

---

### R&D Intern at JD.COM Silicon Valley Research Center

*May 2021 - Aug. 2021*

- Develop and deploy PPML (Privacy-Preserving Machine Learning) solution - TensorFlow Serving Cluster with Graphene-SGX.
- Develop transparent data encryption with Intel SGX enclave.

Mentor: [Yanhui Zhao](#)

## RESEARCH PROJECTS

---

### Recent Research Projects

- Proposed a new transfer learning model in binary code analysis.
- The application of graph neural network in vulnerability analysis [ii]. I proposed a new type of Graph Neural Network, e.g., (Relational Graph Neural Network with Bi-directional Propagation) to facilitate data flow analysis.
- The application of deep learning in critical variable identification [i] and malware analysis.

### Previous Research Projects

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

## AWARDS & HONORS

---

- Outstanding Graduates of Nanjing University, 2019.
- Scholarship of Shenzhen Stock Exchange, 2018.
- Second-Class Academic Scholarship of Nanjing University, 2017 &<sup>2</sup> 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.

---

<sup>1</sup>Source Code: <https://github.com/zhilongwang/PolymorphicCanaries>

<sup>2</sup> Obtained annually.

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**<sup>\*</sup>, Haizhou Wang<sup>\*</sup>, Hong Hu, and Peng Liu. “Identifying Non-Control Security-Critical Data in Program Binaries with a Deep Neural Model.” arXiv, 2021. ( <sup>\*</sup> 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.