WEI ZHOU

zhouw@nipc.org.cn

Phone: **(+86) 188-1021-8123**

https://weizhou.netlify.app/

EDUCATION

08/2016 - 06/2021	**University of Chinese Academy of Sciences**	Beijing/China
	● PhD. / Information Security	
	● Advisors: Yuqing Zhang	
10/2018 - 10/2020	**Pennsylvania State University**	State College/USA
	● Visiting Student	
	● Advisors: Peng Liu/Le Guan	
08/2012 - 08/2016	**Xidian University**	Xi'an/China
	● B.Eng. / Information Security	

RESEARCH INTEREST

My research interests cover a wide range of systems security, including **trusted computing and IoT systems security**. I am especially interested in **developing automatic tools** to detect and exploit **previously unknown vulnerabilities** in **IoT firmware and platforms**.

PUBILCATIONS

[1] **Wei Zhou,** Le Guan, Peng Liu, Yuqing Zhang. Automatic Firmware Emulation through Invalidity-guided Knowledge Inference. ***USENIX Security 2021*** **(CCF A).**

[2] **W. Zhou,** Y. Jia, Y. Yao, et al. Discovering and Understanding the Security Hazards in the Interactions between IoT Devices, Mobile Apps, and Clouds on Smart Home Platforms. ***USENIX Security, 2019*** **(CCF A)**

[3] **Wei Zhou,** Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu. "The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved." *IEEE Internet of Things Journal* 6, no. 2 (2018): 1606-1616. (**ESI highly cited paper**, **Top 1%**)

[4] **Wei Zhou**, Chen Cao, Dongdong Huo, Kai Cheng, Lan Zhang, Le Guan, Tao Liu, Yan Jia, Yaowen Zheng, Yuqing Zhang, Limin Sun, Yazhe Wang, Peng Liu. Reviewing IoT Security via Logic Bugs in IoT Platforms and Systems. *IEEE Internet of Things Journal* 8, no. 14 (2021): 11621-11639. (SCI IF:11.7)

[5] Yao Yao, **Wei Zhou**, Yan Jia, Lipeng Zhu, Yuqing Zhang and Peng Liu. Identifying Privilege Separation Vulnerabilities in IoT Firmware with Symbolic Execution. *ESORICS, 2019* (CCF B)

[6] **Wei Zhou**, et al. "Good Motive but Bad Design: Why ARM MPU Has Become an Outcast in Embedded Systems." arXiv preprint arXiv:1908.03638 (2019).

[7] He, Xixun, Yiyu Yang, **Wei Zhou**, Wenjie Wang, Peng Liu, and Yuqing Zhang.Fingerprinting Mainstream IoT Platforms Using Traffic Analysis. *IEEE Internet of Things Journal (2021)*.

Experiences and Projects

University of Chinese Academy of Sciences 2021.07-present

- Huazhong University of Science and Technology

University of Chinese Academy of Sciences

- Research Assistant
- Advisors: Yuqing Zhang
- Project:
  - Smart Home Security 2017.10-2019.04
    - While smart home brings unprecedented convenience and accessibility, it also introduces various security hazards to users. In this work, we conducted an in-depth analysis of five widely-used smart home platforms, and found that the complex interactions among the participating entities are vulnerable to a spectrum of new attacks, including **remote device substitution, remote device hijacking, remote device DoS, etc**. The discovered vulnerabilities are applicable to multiple widely-used smart home platforms, **including Samsung SmartThings, TP-LINK KASA, XiaoMi MIJIA**, etc. and **more than hundreds of millions** devices were affected.
    - This research has led to one paper publication in Usenix 2019.

Pennsylvania State University

- Research Assistant
- Advisors: Peng Liu
- Project:
  - Static MCU Firmware Analysis 2018.04-2019.06
    - In contrast to the traditional firmware bugs/vulnerabilities (e.g. memory corruption), we **firstly** conducted an in-depth security analysis of the privilege separation model of IoT firmware and identified a previously unknown logic vulnerability called **privilege separation vulnerability**. By combining loading information extraction, library function recognition and symbolic execution, we developed Gerbil to effectively identify privilege separation vulnerabilities in IoT firmware. So far, we have evaluated Gerbil on 106 real-world IoT firmware images and successfully detected privilege separation vulnerabilities in 69 of them.
    - This research has led to one paper publication in ESORICS 2019.
  - MCU Firmware Analysis 2019.09-2021.04
    - Emulating firmware for microcontrollers is challenging due to the **tight coupling between the hardware and firmware**. In this project, we propose and implement a new automatic peripheral modeling approach based on symbolic execution. We take

the firmware as input and infers the rules of how to respond to unknown peripheral accesses during symbolic execution. These rules are learned in a knowledge base(KB). With the returned knowledge base, our tool efficiently responds to peripheral read operations during dynamic analysis **without any hardware dependence.** Our tool achieves **a passing rate of 95%** in a set of unit tests for peripheral drivers without any manual assistance. We further integrated Fuzzer (i.e., AFL) on the top of our tool and evaluated more than 20 real-world firmware samples. Evaluation results show that µEmu is capable of emulating real-world firmware and finding new bugs.

- This research has led to one paper publication in Usenix 2021.

HONORS AND AWARDS

- Outstanding Graduate of University of Chinese Academy of Sciences. 2021
- National Cyber-security Scholarship **(only 73 winners nationwide)** 2018
- **Chinese Government Scholarship for Two-year Visiting Study** 2018
- International Mathematical Contest in Modeling (MCM) 2015
  Honorable Mention
- National Scholarship **(top 0.2% nationwide)** 2015
- Undergraduate Electronic Design Contest – Information Security Invitation Context 2014
  National Second Prize

Invited Presentations and Talks

- 30th Usenix Security Symposium Online. 2021.08
- Cyber Security Academic Lectures. Nankai University. 2021.04
- 28th Usenix Security Symposium Santa Clara, CA, USA. 2019.8
- The European Symposium on Research in Computer Security Luxembourg. 2019.9

Academic Service

IEEE Internet of Things Journal (Impact Factor 11.7)	Reviewer
ACM Computing Surveys Journal (Impact Factor 9.5)	Reviewer
CRiSIS 2021	PC Member
EAI SPNCE 2021	PC Member