# QINYING WANG（王琴应）

🖂 wangqinying@zju.edu.cn
Rm. 320, Cao Guang Biao Main Building, Yuquan Campus, Zheda Road 38, Hangzhou, China, 310027

## EDUCATION

**Zhejiang University**, Hangzhou, China ........ September 2018 - Present
Ph.D. in Cyber Security, College of Computer Science and Technology
Advisor: Shouling Ji.

**Hunan University**, Changsha, China ........ September 2014 - June 2018
B.E. in Information Security, College of Computer Science and Electronic Engineering GPA: 86.82/100.00, 2/28

## RESEARCH INTERESTS

I am broadly interested in software and system security, IoT security and fuzzing. Recently, my research focuses on developing novel technologies to understand the risks of modern and emerging systems.

## PUBLICATIONS & MANUSCRIPTS

[1] **MPInspector: A Systematic and Automatic Approach for Evaluating the Security of IoT Messaging Protocols.** Qinying Wang, Shouling Ji, Yuan Tian, Xuhong Zhang, Binbin Zhao, Yuhong Kan, Zhaowei Lin, Changting Lin, Shuiguang Deng, Alex X. Liu, Raheem Beyah.

In *Proceedings of the 30th USENIX Security Symposium* (**USENIX Security**), August 2021.

> This research presents *MPInspector*, the first automatic approach for vetting the security of IoT messaging protocols (MPs). *MPinspector* utilizes pattern matching, NLP and automata learning to infer the state machine of an MP implementation, then detects property violations on the state machine by customized protocol verification. We evaluate MPInspector on 3 popular MPs implemented on 9 leading IoT platforms. The experiment results show that MPInspector successfully detects 252 property violations, and further identifies 11 types of attacks. This research has been integrated into the IoT platform of Tuya Smart.

**[2]** **A Large-Scale Empirical Analysis of the Vulnerabilities Introduced by Third-party Components in IoT Firmware.** Binbin Zhao, Shouling Ji, Jiacheng Xu, Yuan Tian, Qinying Wang, Qiuyang Wei, Chenyang Lyu, Xuhong Zhang, Changting Lin, Jingzheng Wu, Reheem Beyah.

In *Proceedings of the 31st ACM SIGSOFT International Symposium on Software Testing and Analysis* (**ISSTA**), July 2022

> This research conducts the first large-scale analysis of the vulnerable third-party components (TPC) problem in firmware. It utilizes syntactical and CFG features to detect the TPCs at the version level and identify the corresponding vulnerabilities. For evaluation, we construct a large firmware dataset, including 34,146 firmware images. We detect 584 TPCs and identify 128,757 vulnerabilities caused by 429 CVEs at the end.

**[3]** **State-of-the-Art Survey of Open-source Software Supply Chain Security.** Shouling Ji, Qinying Wang, Anying Chen, Binbin Zhao, Tong Ye, Xuhong Zhang, Jingzheng Wu, Yun Li, Jianwei Yin, Yanjun Wu.

In *Journal of Software*, 2022.

> We present a detailed survey of open-source software supply chain security. We try to define the new open-source software supply chain model and by studying publicly documented exploits and vulnerabilities as well as related pieces of literature (169 references), we further conclude related attack vectors and safeguards.

## SERVICE

External reviewer of the ACM Conference on Computer and Communications Security (**CCS**) 2019, IEEE International Conference on Communications (**ICC**) 2019, IEEE Transactions on Dependable and Secure Computing (**TDSC**) 2019, the European Symposium on Research in Computer Security (**ESORICS**) 2021, and the IEEE Conference on Dependable and Secure Computing (**DSC**) 2022.

## SKILLS

**Vulnerability discovery**: Proficient in fuzzing and protocol verification.
**Program analysis techniques**: Automata learning, software reverse engineering, and MCU debugging.
**Natural language processing**: Preliminary in dependency parsing, word embedding, and Part-of-Speech tagging.
**Programming language**: Proficient in C/C++, Python, Java, Go and x86_64 assembly language.
**Languages**: English (proficient, CET-4: 590, CET-6: 557), Chinese (native), German (beginner, College German Test Band 4)

## SELECTED HONORS AND AWARDS

| | |
|---|---|
| **Best Conference Paper**, Chinese Institute of Electronics | 2021 |
| **Second Class Prize,** The 4th "Zongheng Cup" Cyberspace Technology Innovation Competition | 2021 |
| **Glodon Scholarship,** College of Computer Science and Technology of Zhejiang University (11/1695) | 2020 |
| **Outstanding Freshman Scholarship,** Zhejiang University | 2018 |
| **Outstanding Graduate Student of Hunan Province,** The Education Department of Hunan Province | 2018 |
| **Cyber Security Scholarship,** China Internet Development Foundation (The highest award for undergraduates majoring in Cyber Security in China) | 2017 |
| **Second Class Prize**, The 10th National College Student Information Security Contest (Top 17%, 41/246) | 2017 |
| **National Scholarship,** China Ministry of Education (Top 3%, 1/28) | 2015 |

## TALK

**2021. 08** **Presenter, IoT Session, USENIX Security 2021**

*MPInspector: A Systematic and Automatic Approach for Evaluating the Security of IoT Messaging Protocols*

## INTERNSHIP EXPERIENCES

**Tuya Smart**, Hangzhou, China ................................................................................ October 2019 - September 2020

- Security Engineer: detecting vulnerabilities in smart home devices by static and dynamic analysis.

## REFERRERS

**Dr. Shouling Ji (Master Advisor)**

Professor
Zhejiang University
🌐 https://nesa.zju.edu.cn/
✉ sji@zju.edu.cn

**Dr. Xuhong Zhang (Publication Co-advisor)**

Professor
Zhejiang University
🌐 https://nesa.zju.edu.cn/
✉ zhangxuhong@zju.edu.cn

**Dr. Yuan Tian (Publication Co-advisor)**

Assistant Professor
University of California, Los Angeles
🌐 https://www.ytian.info
✉ yuant@ucla.edu

**Dr. Raheem Beyah (Publication Co-advisor)**

Professor
Georgia Tech
🌐 https://rbeyah.ece.gatech.edu/
✉ raheem.beyah@ece.gatech.edu