Zhiqing Rui (芮志清)

Last Update: Oct. 15th, 2020
Revision: Dec. 2020
zhiqing.rui@gmail.com | (+86)188-1152-0398 | https://m2kar.cn/cv
Male | Oct. 1997 | Married | Beijing, China

Education

- **University of Chinese Academy of Sciences** **Beijing, China**
  Master in Computer Technology *Sep. 2018 – Jul. 2020*
  Advisor: Professor Jingzheng Wu (Institution of Software, China Academy of Science)
  GPA: 3.74/4.0 (Top 5%)
- **China Medical University** **Liaoning, China**
  Bachelor in Forensic Medicine *Sep. 2013 – Jul. 2018*

Publication

- [1] **Zhiqing Rui**, Jingzheng Wu, Yanjie Shao, Tianyue Luo, Mutian Yang, Yanjun Wu, Bin Wu." PassEye: Sniffing Your Password from HTTP Sessions by Deep Neural Network." *2020 China Cyber Security Annual Conference (CNCERT 2020)*, Beijing, China, 2020. (*Accepted*)
- [2] **Zhiqing Rui**. “Design and Implementation of Web Camera Security Threat Detection System.” University of Chinese Academy of Sciences. 2020. (Thesis)
- [3] Xu Duan, Jingzheng Wu, Shouling Ji, **Zhiqing Rui**, Tianyue Luo, Mutian Yang, Yanjun Wu." VulSniper: Focus Your Attention to Shoot Fine-Grained Vulnerabilities." *Proceedings of the 28th International Joint Conference on Artificial Intelligence (IJCAI-19)*. Macao, China, 2019.
- [4] **Zhiqing Rui**, Jingzheng Wu, Tianyue Luo, Xu Duan, Hang Zhao, Changyu Chen. " A new Approach for Detecting Inheritance Vulnerabilities based on Atomic Control Flow Graph. " *Symposium on Software Security and Reliability Technology for Manned Space Engineering*. Beijing, China. 2019. (**Second Prize Awards**)
- [5] **Zhiqing Rui**, Jingzheng Wu, Tianyue Luo. “A new Approach for Detecting Inheritance Vulnerabilities based on Atomic Control Flow Graph,” CN. 201811562246.2. (Patent).
- [6] Changyu Chen, **Zhiqing Rui**, Jingzheng Wu, Tianyue Luo,” Firmware Version Detection Method Based on Graph Association Analysis”. CN. 201910836177.8. (Patent)

Project Experiences

- **RevEye: Defend Hidden Camera by Active Detection** *Feb. 2020 – Now*

This project is an extended version of SentryEye (see below), and the main purpose is to **detect dormant hidden cameras** in LAN. Sometimes, Hidden cameras go to sleep status and have no activity record in network traffic. To solve this problem, this project got cameras’ features by analyzing the firmware and associated mobile app, then send broadcast packets to all cameras. I am the major contributor to this project.

- **SentryEye: A Web Camera Security Threat Detection System** *Jul. 2019 – May. 2020*

This project’s purpose is to defend against hidden camera attacks in Intranet. Hidden cameras send video stream to outside and pose a great privacy threat to institutions. To defend against the attack, this project analysis the network traffic characteristics of hidden cameras and design an Intrusion Detection System (IDS) to find the

cameras in a high-speed Intranet's mirror port. This project is a part of my master degree's thesis and I play the roles of designer and implementor in it.

- **IoT Firmware Vulnerability Analysis System** *Sep. 2018 – Jun. 2019*

  Design an IoT firmware security analysis and vulnerabilities mining system. To increase the success rate of existing tools we use a variety of IoT firmware analysis techniques. I completed the documentation, developed the IoT rate firmware unpacking module, dynamic analysis module, and firmware reverse module.

- **Mobile Internet Data Protection Technology Pilot Demonstration Project** *Oct. 2018 – Now*

  This project is a national key research and development project, the main goal is to pilot and demonstrate the data protection technology of the mobile Internet. The terminal high-security threat identification and data protection is a sub-project of the research group of the person. I participated in the research of vulnerability analysis based on attention neural network and vulnerability knowledge graph and will publish a report on mobile security analysis technology.

- **Domain-specific Software Source Code Flaw Automatic Repair System** *Oct. 2018 – Jul. 2019*

  This project proposed to detect and automate security flaw repair in domain-specific C/C+ + source codes. Security specifications including hundreds of rules concerning data processing, control flow, and memory are applied as well as additional software compliance.

- **2018 World Intelligence Drive Challenge** *Apr. 2018*

  Information Security Group Excellence Award. Our team figured out the vehicle CAN bus control protocol in 1 day. Through the packet analysis of the bus transfer data in 30 minutes, we cracked three vehicle's control commands and obtained a great score.

Working Experiences

- **Institution of Software, China Academy of Science** **Beijing, China**
  Security Engineer *Aug. 2020 – Now*
  Duties: IoT Security Research, Network Traffic Analysis
  Supervisor: Professor Jingzheng Wu

Skill

- **Python**
  - 4 years of Python experience, familiar with Python advanced grammar.
  - Develop scripts for web crawling, vulnerability scanning, system maintenance, etc.
  - Build a deep neural network framework using TensorFlow, PyTorch.
- **Linux**
  - Proficiency in bash scripting and system maintenance under Linux
  - Proficiency in Kali Linux platform for vulnerability analysis, network penetration.
- **Programming language**: Python，C，C++.
- **Other Skills:** Git, Docker, Reverse Engineering, Penetration test.
- **China Qualification Certificate of Computer and Software Technology Proficiency**:
  - Network Engineer
  - Software Design Engineer