Zhiqing Rui (芮志清)

Last Update: Oct. 11, 2020
Online Version: https://m2kar.cn/cv/cv

Email:	✉zhiqing@iscas.ac.cn	Gender: Male
Github:	https://github.com/m2kar	Birth: October 1997
Website:	https://m2kar.cn/cv	City: Beijing, China
Mobile:	(+86)18811520398	

Overview

- I am a **Security Engineer** at Institute of Software, China Academic of Science.
- Previously, I have completed my **master degree** in School of Artificial Intelligence, University of Chinese Academy of Sciences and graduated in July 2020.
- Research Interests: **IoT Security, Network Traffic Analysis**.
- Published **3 papers, 1 thesis and 2 patents** and participate in several national/provincial level projects in the master stage.
- Excellent programming ability, expert in Python.

Work Experience

- **Institution of Software, China Academy of Science** **Beijing, China**
  Intelligent Software Research Center
  Security Engineer *Aug. 2020 – Now*
  Duties: IoT Security Research, Network Traffic Analysis
  Supervisor: Professor Jingzheng Wu
- **Institution of Software, China Academy of Science** **Beijing, China**
  Intelligent Software Research Center
  Intern Research Assistant *Sep. 2018 – Aug. 2020*
  Duties: IoT Security Research, Network Traffic Analysis
  Supervisor: Professor Jingzheng Wu

Education

- **University of Chinese Academy of Sciences** **Beijing, China**
  School of Artificial Intelligence
  Master in Computer Technology *Sep. 2018 – Jul. 2020*
- **China Medical University** **Liaoning, China**
  School of Forensic Medical
  Bachelor of 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.
- [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, August 10-16 2019.
- [4] **Zhqing 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. December 12 2019. (Non-public, 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 experience

- **RevEye: Defend Hidden Camera by Active Detection**

Feb. 2020 – Now

This project is a extended version of SentryEye(see below),and the main goal is to detect dormant hidden camera in LAN. Hidden cameras pose a great privacy threat to institutions. Sometimes, Hidden cameras go to sleep status and have no activity record in network traffic. To solve this problem, this project got analysis the cameras and associated mobile app send boardcast packets to all cameras.

- **SentryEye: A Web Camera Security Threat Detection System**

Jul. 2019 – May. 2020

This project's main goal is to defend hidden camera attacks in Intranet. Hidden cameras send video stream to outside and pose a great privacy threat to institutions. To defend the attack, this project analysis the network traffic charactisic of hidden cameras and design a Intrusion Detection System (IDS) to find the cameras in high speed Intranet's mirror port. My role in this project is the designer and programmer. This project are also a part of my master degree thesis.

- **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 report on mobile security analysis technology.

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

  Design an IoT firmware security analysis system, including vulnerability information management, CFG and inherited firmware vulnerability correlation, cross-platform vulnerability correlation detection, firmware information management, and other modules. I developed the IoT firmware unpacking module, dynamic analysis module, firmware reverse module, and written project documentation. A variety of IoT firmware analysis techniques have been used in this project to increase the success rate of existing tools.

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

  This project is based on the code security rules standard database, which is used to detect and repair memory, calculation, control flow, and data processing related errors in specific domain software. The test target is a domain-specific C/C++ language source code with additional software compliance and security standards. I developed a code compliance detection module based on semantic mode, and established some source code matching rules, which can realize automatic software detection and patch repair.

- **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.

Skill

- **Python**
  - 4 years Python experience, familiar with Python advanced grammar.
  - Develop scripts for web crawling, vulnerability scanning, system maintenance, etc.
  - Scientific computing using tools such as NumPy, SciPy, and matplotlib.
  - 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.
- **Network Traffic Analysis**
  - Familiar with tools like Wireshark, TcpDump, Dpkt, etc.
  - Proficiency in develops Network Intrusion Detection System (NIDS) using snort.
- **Programming language**:

  Python，C，C++，HTML，MIPS ASM，8086 ASM.
- **Other Skills:** Git, Docker, Reverse Engineering, Penetration test, etc.
- **China Qualification Certificate of Computer and Software Technology Proficiency**:
  - Network Engineer
  - Software Design Enginee
- **Courses：**

  Computer Security Technology and Practice, Introduction to Artificial Intelligence, Algorithm Introduction, Pattern Recognition, and Machine Learning, Semantic Network and Knowledge Graph, Natural Language Processing and Application, Deep Learning Theory and Application, Intelligent Robot Technology, Introduction to Big Data Technology, etc.