Mingyi Chen

University of Chinese Academy of Sciences
No.19(A) Yuquan Road, Shijingshan District, Beijing, P.R.China 100049
my@imcmy.me

EDUCATION

University of Chinese Academy of Sciences(UCAS), Beijing, China 2016 - present
M.S., Cybersecurity
Advisor: Zhigang Lu, Jian Liu
Core courses: Software Security and Vulnerability Analysis, Network Attacks and Defenses, Statistical Machine Learning, The Design and Analysis of Computer Algorithms, Web Security, Cyber Attacks Attribution and Forensics, Malware Analysis

Sichuan University(SCU), Sichuan, China 2012 - 2016
B.E., Software Engineering, GPA: 3.6/4.0, Rank: 6/303

RESEARCH EXPERIENCE

Intrusion Detection and Visualization

Institute of Information Engineering(IIE), Chinese Academy of Sciences(CAS), **Research Assistant** 08/2017 - present

- Put forward a method to visualize the network flow and its Intrusion Detection System alert in a flow graph. And use other graphs to assist analyst to find unknown threat whose not been detected by IDS by on analyst's knowledge base.
- Proposed a way to detect lateral movement in Advanced Persistent Threat with a Host-Connection Graph generated by host connection in intranet and a semi-supervised deep learning model.
- Proposed a plan to visualize the deep learning model's neurons and layers to assist analysts to adjust the model.

Large-scale Network Search and Visualization, IIE, CAS, **Research Assistant** 02/2017 - 07/2017

- Designed a large-scale network data format conversion method without modifying other system module
- Devised and realized a high-efficient multiple conditions and hierarchy search mechanism in large-scale network

Threat Intelligence Platform and Visualization, IIE, CAS, **Research Assistant** 09/2016 - 01/2017

- Designed and realized a role based access control model and a threat intelligence log management system
- Built the security mechanism and rules for threat intelligence platform
- Provided a presentation of how to realize scattering points in parallel coordinates and visual clustering in parallel coordinates
- Provided a presentation of how to detect malicious logins in enterprise networks using visualization

Software Define Network Research, Zhejiang University, **Research Intern** 07/2015 - 08/2015

- Realized IP address Hop-Change for defensing in SDN based on OpenDayLight platform
- Provided a presentation of how to use the moving target method and dynamics machine learning to offer an effective defense

ReviewBoard, Facebook OpenAcademy Project, **Participant** 01/2015 - 06/2015

- Fixed Bug #3717
- Added infinite scroll function and read only function for diff viewer in ReviewBoard

PUBLICATIONS

- M. Chen, Y. Yao, J. Liu, B. Jiang, L. Su and Z. Lu, "A Novel Approach for Identifying Lateral Movement Attacks Based on Network Embedding," in ISPA-IUCC-BDCloud-SocialCom-SustainCom 2018, Dec 2018, pp.708-715.

LEADERSHIP AND ACTIVITIES

Open Source Software Community of UCAS(OpenCAS), UCAS, **President** 09/2017 - present

- Host and manage open source software mirror site for Chinese Academy of Sciences

LinuxStory, Beijing, **Translator and Activity Director** 09/2015 - present

- *Advanced Bash Scripting Guide* Chinese translation director
- Sichuan University and University of Chinese Academy of Sciences Activity Director

Information Security Attack and Defense Community, SCU, **President** 09/2014-09/2015

COMPETITION AND AWARDS

- National Scholarship in 2013
- National Scholarship in 2014
- National Scholarship in 2018
- Top 100 Excellent Student in Sichuan University
- Excellent Community President in Sichuan University
- Excellent Student in University of Chinese Academy of Sciences
- Third Prize of 2017 ChinaVis Data Challenge
- First Prize of 2018 ChinaVis Data Challenge
- Third Prize of Fifth China Students Service Outsourcing Innovation & Entrepreneurship Competition
- First Prize of Guiyang Big Data and Network Security Drill 2017
- Tenth Place in Tencent CTF / 0CTF (Member of NeSE Team)
- Tenth Place in XCTF 2017 (Member of NeSE Team)
- 33th Place in UCSB iCTF 2017 (Member of NeSE Team)
- 20th Place in DEFCON CTF Qualifier 2017 (Member of NeSE Team)
- 17th Place in HITCON CTF Qualifier 2017 (Member of NeSE Team)
- 13th Place in 34C3 CTF 2017 (Member of NeSE Team)

SKILLS

- Fluent in Mandarin and English
- Familiar with Python, Java and C programming language
- Familiar with Linux and Bash
- Familiar with Wireshark, SQLMap, NMap, Metasploit and so on
- Web category skills of CTF