Zonghao Ying

Minzhuang Load 89,Beijing, China
yingzonghao20@mails.ucas.ac.cn (+86)-18800102408 elwood.me

Education

School of Cyber Security,University of Chinese Academy of Sciences **Beijing, China**
Master in Cyber Security 09/2020–06/2023
State Key Laboratory of Information Security,Institute of Information Engineering,Chinese Academy of Sciences **Beijing, China**
Research Assistant 07/2021–06/2023
School of Computer and Communication,Lanzhou University of Technology **Lanzhou, China**
Bachelor in Internet of Things Engineering 09/2015–06/2019
Institute of Network and Information Security,Lanzhou University of Technology **Lanzhou, China**
Research Intern 09/2016–06/2019

Research Areas

Trustworthy Machine Learning, specially in backdoor attack and defense 03/2021–
Machine Learning for Cybersecurity,including encrypted traffic analysis and code analysis 06/2020–02/2021
Software Security,including Malware analysis and Forensics analysis 07/2019–05/2020
Network Security,including Red Teaming and Security of IoT 09/2016–06/2019

Publications

(i)DeeSCVHunter: A Deep Learning-Based Framework for Smart Contract Vulnerability Detection Xingxin Yu, Haoyue Zhao, Botao Hou, **Zonghao Ying**, Bin Wu. IJCNN, 2021

(ii)Encrypted Malicious Traffic Detection: A Survey (accepted by "Information Security Communication Privacy", in Chinese, 2022) **Zonghao Ying**, Jun Zhen, Jingxiao Guan and Bin Wu

(iii)Backdoor Attack on Deep Learning Models: A Survey (accepted by "Computer Science", in Chinese, 2022) **Zonghao Ying** and Bin Wu

(iv)DAT: Model-Agnostic Dynamic Backdoor Attack on Deep Learning Models (under review, 2021) **Zonghao Ying** and Bin Wu

(v)DLP: Towards Active Defense against Backdoor Attacks with Decoupled Learning Process (accepted by Cybersecurity, 2023) **Zonghao Ying** and Bin Wu

(vi)NBA: Defensive Distillation for Backdoor Removal via Neural Behavior Alignment (accepted by Cybersecurity, 2023) **Zonghao Ying** and Bin Wu

Selected Honors

Pacemaker to Merit Student, University of Chinese Academy of Sciences Beijing,2023
National Scholarship, Chinese Government Beijing,2022
Merit Student, University of Chinese Academy of Sciences Beijing,2021-2023
Cyberspace Security Expert of Winter Olympics,Beijing Organising Committee for the 2022 Olympic Beijing,2021
Honored Speaker, The Cyberspace Security Talent Education Alliance of China Wenzhou,2020
Outstanding Graduates,Lanzhou University of Technology Lanzhou,2019
National Encouragement Scholarship,Chinese Government Lanzhou,2016–2018
Merit Student, Lanzhou University of Technology Lanzhou,2016–2018

Selected Awards

Bronze National Hackathon for College Students Wuhan,06/2018
1st Prize National Cybersecurity Technology Competition Xi'an,05/2018
Champion National College Hackathon Hangzhou,05/2018
Runner-up Information Security Triathlon Northwest Division Finals Lanzhou,05/2018
Third Prize Information Security Triathlon National Finals Wuhan,09/2017

Third Prize National English Competition for College Students Lanzhou,09/2017
Runner-up Cisco Network Technology Challenge Northwest Division Finals Lanzhou,07/2017
Third Prize National English Competition for College Students Lanzhou,09/2016

Invited Talks

Security and Privacy Issues of Deep Learning System, PyCon China Online,12/2022
CIA of AI system, OWASP China Online,03/2022
Red Team's Perspective:How and Why They Target Your AI System?,360 Hackling Club Changsha,06/2021
How to attack DL system?, HUAWEI HWS Camp Dongguan,03/2021
Security of router, a perspective of a hacker,CEAC Online,03/2020
Hunters in the Network Traffic,BugBank Online,07/2019

Services

MITRE Adversarial Threat Landscape for Artificial-Intelligence Systems, Committer 10/2021
HUAWEI Hardware Security Camp, Tutor 03/2021
The first Trusted Hardware Security Competition of HUAWEI,Propositioner 03/2021
Information Security Association of LUT, Vice President 09/2016–09/2018
CTF team "k410ng", Co-founder and Tutor 09/2016–09/2018
Google Study Jam of Lanzhou,Organizer 03/2017-06/2017

Internships

QIHU TECHNOLOGIES(360) **Lanzhou, China**
Research Intern 06/2019
– Responsible for the research of TTP(Tactics, Techniques, and Procedures), and participated in the national network security actual combat exercises, including: 1) study MITRE Matrix,2) predict, detect and respond to real-time attack.

SANGFOR TECHNOLOGIES **Shenzhen, China**
Research Intern 03/2019-06/2019
– Responsible for the probe pre-research in the network security situation awareness system, including: 1) reproducing and studying the vulnerabilities of various protocols,2) Fingerprint research of operating system.

Projects

IAVSF(Intranet Asset Vulnerability Scanning Framework), Python,Shell Script 06/2019
– It scans the port of target host to get get banner and other useful information as auxiliary.User then know the version of running applications, and then uses the related POC(Proof of Concept) script in the database to verify, and finally obtains a list of vulnerable assets. It incorporated vulnerabilities that were often exploited at the time, such as WannaCry

AWD-Weapon, Python,Javascript,Shell Script 12/2016-02/2019
– It is a set of scripts based on the experience in AWD(Attack with Defense) competitions. Users can realize semi-automatic Attack and Defense confrontation in AWD competition through this project. The functions include: 1) source auditing,permission maintaining, etc; 2) WAF, attack traffic replay,etc.

Security Gateway of Internet of Things, HTML,CSS,Javascript,Python,Shell Script,Lua,Raspberry Pi Arduino ESP8266 03/2018–12/2018
– The project is funded by Provincial Government Science and Technology Innovation Fund
– It aims to build a secure gateway that monitors and analyzes traffic to determine whether connected IoT devices are being attacked.

Wall of Sheep, Python,Clang,Shell Script 06/2018
– It first compromise target AP by DoS and disconnects all connected devices. An AP with the same name is then forged, and those devices connect to the attacker's AP. Then the attacker can implement three kinds of attacks: 1) phishing, the AP will automatically pop up the phishing authentication page, so as to steal the victim's account information and display it in; 2 Sniffing, stolen valuable information,including accounts, passwords; 3. MITM(advanced and unfinished).

Secure smart Home, C,Python,Lua,Arduino 03/2017–12/2017

- The project is funded by College Students' Science and Technology Innovation Fund
- It aims to build a set of secure smart home, including physical security and network security, including the application of security coding, access control, attack detection and other technologies.

Intelligent Bicycle Auxiliary, C,Python,Lua,Arduino 03/2016–12/2016

- The project is funded by College Students' Science and Technology Innovation Fund
- It aims to transform usual bicycle into intelligent bicycle to a certain extent through the auxiliary, which has functions such as turn warning, remote controlled lock, automatic lights and so on.