ZHIYU ZHANG

https://zhiyu.netlify.app ◇ Github: QGrain

(+86) 189 7122 9081 ◇ zhangzhiyu1999@iie.ac.cn

EDUCATION

Ph.D.	**Chinese Academy of Sciences**	*Sep 20021 - Present*
SKLOIS, Institute of Information Engineering — Overall GPA: 3.68/4.0

B.S.	**Huazhong University of Science and Technology**	*Sep 2017 - Jun 2021*
School of Electric Information and Communications — Overall GPA: 3.76/4.0   Rank: 3/26

RESEARCH EXPERIENCE

Research on Parameter Combination for fuzzing   May 2022 - Feb 2023
Advisor: Prof Kai Chen   *CKGroup, IIE, Beijing*

· Proposed an NLP-based model for extracting parameter dependencies and generating effective parameter combinations using sorting algorithms for enhanced coverage in fuzzing. (UsenixSec 2023)
· I was primarily responsible for the development of the fuzzer prototype.

Research of Transferable Fuzzing Technique   Dec 2021 - Jun 2022
Advisor: Prof Kai Chen and Assis Prof Ruigang Liang   *CKGroup, IIE, Beijing*

· Proposed a lightweight approach of fuzzing for program version migration. (Cyber Securiy 2023)
· Leveraged optimized techniques to record and utilize the correlation between test inputs and program execution for multi-version programs.
· Significantly improved coverage in fuzz testing, reducing time and effort with stability and reliability.

Research of Intrusion Detection/Prevention System for APTs   Sep 2019 - Jun 2021
Advisor: Associate Prof Guihui Zhong and Chengwei Zhang   *Dian Group, HUST, Wuhan*

· Proposed a fast recoverable system for cyber range for destructive experiments. (ICTC 2020 Oral)
· Analyzed the execution principles of malware based on reverse engineering — e.g. WannaCry.
· Based on the analysis, leveraged spatial and timing features to detect malicious traffic with deep learning method — managed to almost 100% nmap detection rate. (Accepted by CyberC 2020)

An Interactive Online NS-3 Platform for Learning Network Protocols Jan 2020 - Mar 2020
Advisor: Associate Prof Xiaojun Hei   *Dian Group, HUST, Wuhan*

· Proposed and implemented an online NS-3 server with Vue, Nodejs and NS-3 engine, due to the complexity of ns3. Provided tutorial pages and relevant experiment guidelines in Web.
· Adopted polling queue to improve the efficiency of NS-3 compiling, efficiency improved around 4x (Accepted by SIMUtools 2020)

Smart City: Recovery of Damaged Structure based on Deep Learning Aug 2019 - Sep 2019
Advisor: Prof Shaofan Li   *UC Berkeley, CA*

· Adopted Finite Element Analysis method to simulate the physical principles of Cantilever. And collected the deformation dataset.
· Built deep neural network and trained the model to rebuild the initial status of the structure.

PROJECT EXPERIENCE

Binary Malware Identification Based on Modularity Analysis   Dec 2021 - May 2022
Advisor: Prof Kai Chen and Guozhu Meng   *Aliyun*

- The project aimed to perform functional module classification and identification of malware using binary program analysis and interpretable classification models. (CSCWD 2023)
- I was primarily responsible for reverse engineering and extracting malicious behaviors and module features from binary malware across multiple platforms.

Matlab Music Generator and Composer
Advisor: Prof Hao Wen
Feb 2019 - May 2019
Course Design

- Analyzed the harmonics and envelopes of several instruments for timbre simulation.
- Defined protocols to parse sheet music and generate songs according to the sheet music input.
- Designed UI for generator and composer (train our music composer AI, ongoing).

NGINX Reverse Proxy for Secure File Sharing Service
Advisor: Associate Prof Guihui Zhong
Jun 2018 - Dec 2018
Huawei

- Developed Windows Network Driver to redirect file-retrieving traffic to Nginx Server.
- Proposed a access control method by packet hook and file monitoring.
- Improved Nginx server performace by adopting epoll mechanism and set up LVS for load balancing.

PUBLICATIONS

Dawei Wang, Ying Li, **Zhiyu Zhang**, Kai Chen, "CarpetFuzz: Automatic Program Option Constraint Extraction from Documentation for Fuzzing", Proceedings of the 32th USENIX Conference on Security Symposium. 2023.

Weihao Huang, Chaoyang Lin, Qiucun Yan, Lu Xiang, **Zhiyu Zhang**, Guozhu Meng, "FMDiv: Functional Module Division on Binary Malware for Accurate Malicious Code Localization", 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2023.

Peiyuan Zong, Ruigang Liang, **Zhiyu Zhang**, Jinghua Liu, Yu Peng, "Research on Lightweight Directed Fuzzing", Journal of Cyber Security, 2023.

Zhiyu Zhang, Guohang Lu, Chengwei Zhang, Yayu Gao, Yajun Wu, Guohui Zhong, "CyFRS: A Fast Recoverable System for Cyber Range based on Real Network", IEEE Information Communication Technologies Conference, 2020. (Oral)

Dewei Zeng[1], **Zhiyu Zhang**[1], Jiye Chen, Xiaojun Hei, "An Interactive Online Programming Platform for Learning Computer Network Protocols", SIMUtools 2020.

Si Liao, Chenming Zhou, Yonghui Zhao, **Zhiyu Zhang**, Chengwei Zhang, Yayu Gao, Guohui Zhong, "A Comprehensive Detection Approach of Nmap: Priciples, Rules and Experiments", 2020 international conference on cyber-enabled distributed computing and knowledge discovery (CyberC), 2020.

HONORS & AWARDS

Outstanding Student of UCAS%	2022
Honours Degree of HUST, Top 3%	2021
National Scholarship, Top 0.2%	2021
Second Prize of Goodix Technology Scholarship, Top 5.0% among 60	2020
Technology Innovation Scholarship, Top 1.8% among 55	2018
Honorable Prize of American College Students Mathematical Modeling Competition.	2018, 2020
First Prize of Mathematical Modeling Competition of HUST, Top 1.5% among 128.	2018
Third Prize of Chinese College Students Mathematics Modeling Competition.	2018

MISCELLANEOUS

Programming Languages	C/C++, Python, Matlab, Go, LaTeX, Verilog, Assembly
Professional Skills	Fuzzing, DevOps, Tensorflow, Backend, CTF
English	TOEFL 93 CET4 610 CET6 507