Yiwei Hou

No.30 Shuangqing Road, Haidian District, Beijing, 100084, P.R.China
houyw22@mails.tsinghua.edu.cn · https://m1-llie.github.io · (+86) 17773695058
M.Sc., Tsinghua University, System Security

- Security researcher focusing on real-world computer security and privacy topics.
- Interested in measuring security risks empirically, maintainer of the large-scale ransomware dataset MarauderMap.
- Passionate about developing practical security tools emphasizing vulnerability detection and defense.
- Interested in security issues of new scenarios such as LLMs.
- Able to work both independently and as a supportive team member.

Education

M.Sc. in Software Engineering, Tsinghua University, Beijing, China Sep. 2022 – Expected Jun. 2025

Software System Security Assurance Group, advised by Prof.Yu Jiang.
System Security, Software Security, Security & Privacy, Program Analysis

B.S. in Cybersecurity, Sichuan University, Chengdu, China Sep. 2018 – Jun. 2022

GPA: 3.95 / 4.0, Ranking: 1 / 172. Advised by Prof. Haizhou Wang.
Thesis: Design and Implementation of Binary Program Testing Tools based on Fuzzing

Summer School, University of California, Berkeley, CA, USA Jul. 2019

Undergraduate summer school in EECS

Publications

An Empirical Study of Data Disruption by Ransomware Attacks

Yiwei Hou, Lihua Guo, Chijin Zhou, Yiwen Xu, Zijing Yin, Shanshan Li, Chengnian Sun, and Yu Jiang
2024, The 46th IEEE/ACM International Conference on Software Engineering (ICSE'24)

Limits of I/O Based Ransomware Detection: An Imitation Based Attack

Chijin Zhou, Lihua Guo, **Yiwei Hou**, Zhenya Ma, Quan Zhang, Mingzhe Wang, Zhe Liu, and Yu Jiang
2023, The 44th IEEE Symposium on Security and Privacy (S&P'23)

MIDAS: Safeguarding IoT Devices Against Malware via Real-Time Behavior Auditing

Yiwen Xu, Zijing Yin, **Yiwei Hou**, Jianzhong Liu, and Yu Jiang
2022, The 22nd ACM SIGBED International Conference on Embedded Software (EMSOFT'22)

Identification of Chinese Dark Jargons in Telegram Underground Markets Using Context-oriented and Linguistic Features

Yiwei Hou, Hailin Wang, and Haizhou Wang
2022, Information Processing and Management (IP&M 59(5))

Research Experience

Software System Security Assurance Group, Tsinghua University Sep. 2022 – Current

Graduate Student Researcher, advised by Prof. Yu Jiang

- **Research Topics:** Ransomware Imitation Attacks, Data Disruption, Runtime Behaviors, Mitigation Strategies. Worked on *Animagus* as the third author and *MarauderMap* as the lead researcher and first author.
- Conducted an effectiveness experiment in the *Animagus* project, prepared the experimental pipeline, tested the newly presented ransomware sample against six state-of-the-art detection techniques, and analyzed the results.
- Constructed a real-world dataset comprising 7,796 active ransomware samples, analyzed their behaviors in disrupting data within victim systems, gathered perspectives from six categories of runtime behaviors, and presented six critical findings spanning three phases of ransomware attacks' data disruption.
- Proposed ransomware mitigation strategies, designed and executed evaluation experiments, analyzed the results and wrote the *MarauderMap* paper.

Software System Security Assurance Group, Tsinghua University Nov. 2021 – Sep. 2022

Research Assistant, advised by Prof. Yu Jiang

- **Research Topics:** IoT Malware, Embedded Firmware, Adaptive Safeguard, Behavior Auditing, Program Analysis, Hardware Debugging. Worked on *Midas* as the third author.
- Extended the anti-malware safeguard framework with a real-time behavior auditing mechanism to adapt more Linux-based IoT devices, developed the backend system for OpenWrt, and compiled corresponding firmware.
- Evaluated tool practicality on an EZVIZ W3 Router by disassembling the router, establishing TFTP serial port communication with a USB to TTL adapter and DuPont cables, and physically updating the firmware for routers.
- Deployed large-scale virtual IoT devices worldwide to examine the performance of our tool over malware, operated compromised devices, and empirically analyzed results.

Wang Research Group, Sichuan University Jun. 2020 – Nov. 2021

Undergraduate Student Researcher, advised by Prof. Haizhou Wang

- **Research Topics:** Jargon identification, Information Forensics, Feature Engineering, Word Embedding, Transfer Learning, Vectors Projection. Worked on *CJI-Framework* as the lead researcher and first author.
- Developed a legitimate crawler to collect chat history from Telegram groups related to the underground market and constructed the corpus TUMCC, the first Chinese corpus in jargon identification.
- Proposed an approach to generate high-quality word vectors based on a relatively small scale of chat history and applied a transfer learning method to enhance vectors' quality further, effectively capturing and utilizing the context of jargon to improve identification performance.
- Extracted seven new features across three categories to identify jargon from commonly used words, ran a statistical outlier detection to determine whether a word qualifies as jargon, analyzed the results, and authored the paper.

Honors & Awards

- **Tsinghua-Jining Scholarship**, Tsinghua University Oct. 2023 & Nov. 2022
- **Outstanding Undergraduate Award**, Sichuan Province Jun. 2022
- **Top 10 Undergraduate of 2022**, Sichuan University (Top 0.03%) Jun. 2022
- **National Scholarship**, Ministry of Education of China (Top 0.2% in China) Dec. 2019 & Dec. 2020
- **Cybersecurity Merit Student Scholarship**, Sichuan University Dec. 2019

Others

- **Programming:** Python, C/C++, HTML/CSS, LaTeX, SQL
- **Language:** English (proficient, IELTS 7.0), Mandarin (native)
- **Personal Interests:** Table tennis; Science fictions; Running; Travelling, enjoy the beauty of nature