Yiming Zhang

Tsinghua University
Institute of Network Sciences and Cyberspace
FIT 4-204, Tsinghua University, 100084, Beijing, China

zhangyiming@tsinghua.edu.cn
+86 132-6175-0179
cypher-z.github.io

RESEARCH CAREER

2022- **Postdoctoral researcher, Tsinghua University**
Institute of Network Sciences and Cyberspace

EDUCATION

2017-2022 **Ph.D. in Computer Science and Technology, Tsinghua University**
Honored as Outstanding Graduate of Computer Science Department
Thesis: Vulnerability Analysis and Measurement Study of Authentication Mechanisms in the Mobile Communication Network Evolution
Advisor: Prof. Haixin Duan

2013-2017 **B.Sc. in Physics, Tsinghua University**
Major in Fundamental Science of Mathematics and Physics (GPA rank: 9/56)
Mnior in Computer Science and Technology

RESEARCH INTEREST

Internet Infrastructure Security; Cellular Communication System Security; Measurement Study; Data Driven Security

PUBLICATIONS

(+) is co-first author and (*) is corresponding author.

Conference Papers

11. Mingxuan Liu (+),**Yiming Zhang (+)**, Xiang Li, Chaoyi Lu, Baojun Liu, Haixin Duan, and Xiaofeng Zheng. *Understanding the Implementation and Security Implications of Protective DNS Services.* In Proceedings of the 31th Annual Network and Distributed System Security Symposium (**NDSS**), 2024.

10. Mingming Zhang, Xiang Li, Baojun Liu, Jianyu Lu, **Yiming Zhang (*)**, Jianjun Chen, Haixin Duan, Shuang Hao, Xiaofeng Zheng. *Detecting and Measuring Security Risks of Hosing-Based Dangling Domains.* In Proceedings of the ACM on Measurement and Analysis of Computing Systems (**SIGMETRICS**), 2023.

9. Mingxuan Liu, **Yiming Zhang (*)**, Baojun Liu, Haixin Duan. *Exploring the Characteristics and Security Risks of Emerging Emoji Domain Names.* In European Symposium on Research in Computer Security (**ESORICS**), 2022.

8. Shiyue Nie, **Yiming Zhang**, Tao Wan, Haixin Duan, Song Li. *Measuring the Deployment of 5G Security Enhancement.* In Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (**WiSec**), 2022.

7. Mingxuan Liu, **Yiming Zhang**, Baojun Liu, Zhou Li, Haixin Duan, and Donghong Sun. *Detecting and Characterizing SMS Spearphising Attacks.* In Annual Computer Security Applications Conference (**ACSAC**), 2021.

6. **Yiming Zhang**, Baojun Liu, Chaoyi Lu, Zhou Li, Haixin Duan, Jiachen Li, and Zaifeng Zhang. *Rusted Anchors: A National Client-Side View of Hidden Root CAs in the Web PKI Ecosystem.* In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (**CCS**), 2021.

5. Hui Gao, **Yiming Zhang**, Tao Wan, Jia Zhang, and Haixin Duan. *On Evaluating Delegated Digital Signing of Broadcasting Messages in 5G.* In 2021 IEEE Global Communications Conference (**GLOBECOM**), 2021.

4. Chaoyi Lu, Baojun Liu, **Yiming Zhang**, Zhou Li, Fenglu Zhang, Haixin Duan, Ying Liu, Joann Qiongna Chen, Jinjin Liang, Zaifeng Zhang, Shuang Hao, and Min Yang. *From WHOIS to WHOWAS: A Large-Scale Measurement Study of Domain Registration Privacy under the GDPR.* In Proceedings of the 28th Annual Network and Distributed System Security Symposium (**NDSS**), 2021.

3. **Yiming Zhang**, Baojun Liu, Chaoyi Lu, Zhou Li, Haixin Duan, Shuang Hao, Mingxuan Liu, Ying Liu, Dong Wang and Qiang Li. *Lies in the Air: Characterizing Fake-base-station Spam Ecosystem in China.*In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (**CCS**), 2020.

2. Zihan Zhang, Mingxuan Liu, Chao Zhang, **Yiming Zhang**, Zhou Li, Qi Li, Haixin Duan, and Donghong Sun. *Argot: Generating Adversarial Readable Chinese Texts.* In Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (**IJCAI**), 2020.

1. Baojun Liu, Zhou Li, Peiyuan Zong, Chaoyi Lu, Haixin Duan, Ying Liu, Sumayah Alrwais, Xiaofeng Wang, Shuang Hao, Yaoqi Jia, **Yiming Zhang**, Kai Chen and Zaifeng Zhang. *TraffickStop: Detecting and Measuring Illicit Traffic Monetization Through Large-scale DNS Analysis.* In 2019 IEEE European Symposium on Security and Privacy (**EuroS&P**), 2019.

Journal Articles

2. Mingxuan Liu, Zihan Zhang, **Yiming Zhang**, Chao Zhang, Zhou Li, Qi Li, Haixin Duan and Donghong Sun. *Automatic Generation of Adversarial Readable Chinese Texts.* In IEEE Transactions on Dependable and Secure Computing (**TDSC**), 2022.

1. Yu Wang, **Yiming Zhang**, Jia Zhang, Haixin Duan. *Study on Promotional Infections Hosting on Educational Websites.* In Journal on Communications, 2018.

Workshop Paper

1. **Yiming Zhang**, Mingxuan Liu, Mingming Zhang, Chaoyi Lu, Haixin Duan. *Ethics in Security Research: Visions, Reality, and Paths Forward.* In Proceedings of the 1st International Workshop on Ethics in Computer Security (**EthiCS**), 2022. (**Best Student Paper**)

PATENTS

1 Jiachen Li,**Yiming Zhang**, Baojun Liu, Chaoyi Lu, Haixin Duan, Haoming Wang.*Method and device for server security checking based domain name lists.* Chinese patent (202310539001.2.)

FUNDING

2023 National Natural Science Foundation of China (NSFC), Youth Science Foundation Program. **Project Leader**. 300K RMB. No.62302258 (2024.1-2026.12)

TEACHING

2022 Guest Lecturer, Graduate Course, Tsinghua University
Topic: Reading, Writing and Presentation of Papers on Cyberspace Security

2020 Guest Lecturer, Graduate Course, Tsinghua University
Topic: Technology of Computer Network Security

INVITED TALKS

2021 **Ethics in Cybersecurity and Network Measurement Research.**
Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China.

2020 **Lies in the Air: Characterizing Fake-base-station Spam Ecosystem in China.**
Tsinghua University, Beijing, China.

CONFERENCE ACTIVITY

Conference Papers Presented[1]

2021 **Yiming Zhang**, Baojun Liu, Chaoyi Lu, Zhou Li, Haixin Duan, Jiachen Li, and Zaifeng Zhang. *Rusted Anchors: A National Client-Side View of Hidden Root CAs in the Web PKI Ecosystem.* In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (**CCS**), 2021.

2020 **Yiming Zhang**, Baojun Liu, Chaoyi Lu, Zhou Li, Haixin Duan, Shuang Hao, Mingxuan Liu, Ying Liu, Dong Wang and Qiang Li. *Lies in the Air: Characterizing Fake-base-station Spam Ecosystem in China.*In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (**CCS**), 2020.

Invited Panelist

2021 **Ethical Considerations in Cyberspace Security Research.**
International Forum for Security Research. Beijing, China.

[1]Oral presentation as the speaker

HONORS AND AWARDS

2022 Shuimu Tsinghua Scholar, Tsinghua University.

2022 Outstanding Graduate of Computer Science and Technology, Tsinghua University.

2022 Best Student Paper Award, EthiCS' 22 (Euro S&P Workshop).

2019 State Scholarship Fund, China Scholarship Council.

2019 First Prize in Next Generation Internet Technology Innovation Competition, CERNET.

2018 Tsinghua-Samsung Scholarship, Tsinghua University.

2018 Outstanding Student Cadre, Tsinghua University.

2016 National Scholarship, Ministry of Education, China.

ACADEMIC SERVICE

Program Committee

SecureComm, Technical Program Committee, 2023

CoNEXT, Artifacts Evaluation Committee, 2023

External Review

NDSS 2020, 2022

DSN 2020

ESORICS 2018, 2019

ICICS 2019

MEDIA

2022 **APNIC Blog**. Investigating hidden root certificates in the wild.

2021 **The Register**. Web trust dies in darkness: Hidden Certificate Authorities undermine public crypto infrastructure.

2021 **HelpNetSecurity**. Researchers shed light on hidden root CAs.

EXPERIENCE

2019 Research Intern, Industrial Internet Security Research Center, Qihoo 360, Beijing, China.

2018 Research Intern, Technology Research Institute, QI-ANXIN, Beijing, China.

2017-20 Undergraduate Student Counselor, Tsinghua University.

Updated December 2023