MINGXUAN LIU

+86 18800151375 ◇ liumx18@mails.tsinghua.edu.cn ◇ liumx.net

FIT 4-206, Tsinghua University, 100084, Beijing, China

EDUCATION AND EXPERIENCE

Education

Ph.D. Tsinghua University
(2018-2023(expected)) *Institute for Network Sciences and Cyberspace at Tsinghua University* *Advisor: Prof. Haixin Duan*

B.S. Communication Engineering from Beijing University of Posts and Communications (BUPT)
(2014-2018) *Telecommunications Engineering and Management (Double Degree)* *GPA: 91.6*

Internship

Internship QI-ANXIN Security Company *Tsinghua University - QI-ANXIN Joint Research Center*
(2021-Now) ** Detection of Phishing Domains and Traffic Analysis*

Internship Fundamental Security department of Ant Group Company *Leader: Yi dao and Bo lin*
(06/2020-10/2020) ** Intelligence and Security Group - Encrypted Traffic Analysis*

RESEARCH AREA

Network Security; AI Security; Data Driven Security; Measurement Study;

PUBLICATIONS

Conference Papers

- **Mingxuan Liu**, Yiming Zhang, Baojun Liu, Haixin Duan. *Exploring the Characteristics and Security Risks of Emerging Emoji Domain Names.* In 27th European Symposium on Research in Computer Security (ESORICS), 2022.
- **Mingxuan Liu**, Yiming Zhang, Baojun Liu, Zhou Li, Haixin Duan, Donghong Sun. *Detecting and Characterizing SMS Spearphising Attacks.* In Proceedings of the 37th Annual Computer Security Applications Conference (ACSAC), 2021.
- *Zihan Zhang, ***Mingxuan Liu (* co-first author)**, Chao Zhang, Yiming Zhang, Zhou Li, Qi Li, Haixin Duan and Donghong Sun. *Argot: Generating Adversarial Readable Chinese Texts.* In Proceedings of the 29th International Joint Conference on Artificial Intelligence (IJCAI) Main track, 2020.
- Zhuoqun Fu, **Mingxuan Liu**, Yue Qin, Jia Zhang, Yuan Zou, Qilei Yin, Qi Li, Haixin Duan. *Encrypted Malware Traffic Detection via Graph-based Network Analysis.* In Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2022.
- Yiming Zhang, **Mingxuan Liu**, Mingming Zhang, Chaoyi Lu, Haixin Duan. *Ethics in Security Research: Visions, Reality, and Paths Forward.* In Proceedings of IEEE European Symposium on Security and Privacy (EuroS&PW) 1st Workshops of Ethics, 2022.
  * Best Student Paper Award
- Chuyun Deng, **Mingxuan Liu**, Yue Qin, Jia Zhang. *ValCAT: Generating Variable-Length Contextualized Adversarial Transformations using Encoder-Decode.* In Proceedings of Annual Conference of the North American Chapter of the Association for Computational Linguistics (NAACL), 2022.
- 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.

- Hao Yang, Kun Du, Yubao Zhang, Shuang Hao, Zhou Li, **Mingxuan Liu**, Haining Wang, Haixin Duan, Yazhou Shi, Xiaodong Su, Guang Liu and Zhifeng Geng. *Casino Royale: A Deep Exploration of Illegal Online Gambling.* In Proceedings of the 35th Annual Computer Security Applications Conference (ACSAC), 2019.
- Kun Du, Hao Yang, Zhou Li, Haixin Duan, Shuang Hao, Baojun Liu, Yuxiao Ye, **Mingxuan Liu**, Xiaodong Su, Guang Liu, Zhifeng Geng, Zaifeng Zhang and Jinjin Liang. *TL;DR Hazard: A Comprehensive Study of Level-squatting Scams.* In Proceedings of International Conference on Security and Privacy in Communication Systems (SecureComm), 2019, (pp. 3-25). Springer.

Journal Papers

- **Mingxuan Liu**, Zihan Zhang, Chao Zhang, Yiming 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), doi: 10.1109/TDSC.2022.3164289, 2022.

PROJECTS

- Automatic Adversarial Generation Project — Huawei Technologies Co., Ltd.
  ** Research on attack and defense technologies on adversarial texts.*
  ** Resulted in a patent.*
- Detection of Underground Website based on Natrual Langurage Processing (NLP) — Tsinghua University
  ** Completion of the website detection section based on semantic similarity comparison;*
  ** This detection system has been deployed in Tsinghua Campus Network and QI-ANXIN, and has been running continuously for more than 500 days, detecting thousands of blackmail pages per day.*
- Detection of Malicious Traffic based on Machine Learning Technology — Huawei Technologies Co., Ltd.
  ** Completion of detection based on features extracted from HTTP traffic;*
  ** Resulted in a patent and a detection model that can be run at the gateway.*
- Detection of Malicious Encrypted Traffic — QI-ANXIN
  ** Completion of detection system based on TLS flow features;*
  ** Resulted in a patent (pending) and a detection system running at the gateway.*

HONORS AND AWARDS

- **Best Student Paper Award** of EthiCS 2022 — 2022
- The **First Prize** of Smart password cracking competition of Qiang Wang Bei 2021 — 2021
- The **Third Prize** in the competition of Visual invisible track of GeekPwn 2019 — 2019
- The **First Class Scholarship**, BUPT — 2016-2017
- **National Scholarship**, Ministry of Education, China — 2015-2016
- **National Scholarship**, Ministry of Education, China — 2014-2015

SERVICES

Academic Conference External Review

- National Down Syndrome Society (NDSS) 2020, 2022
- Dependable Systems and Networks (DSN) 2020
- European Symposium on Research in Computer Security (ESORICS) 2018, 2019
- International Conference on Information and Communications Security (ICICS) 2019

Security Competition Organisation

- The 1st Security Analytics of Big Data Competition (DataCon) 2019, QI-ANXIN
  ** Participation of the Traffic Analysis Track as the Jury members*
  ** Verification of the Domain Name System (DNS) Track*
- The 2nd Security Analytics of Big Data Competition (DataCon) 2020, QI-ANXIN
  ** Participation of the Traffic Analysis Track as the Jury members*
- The 3rd Security Analytics of Big Data Competition (DataCon) 2021, QI-ANXIN
  ** Verification of the Traffic Analysis Track*