XINSHU MA

+44 (0)7512-184-378 • x.ma@ed.ac.uk • Homepage: sus0pid.github.io/

EDUCATION

Phd, Network Security 2021 - present
University of Edinburgh, Edinburgh, UK
School of Informatics
Supervisor: Michio Honda

Master, Cyberspace Security 2017 - 2020
Nanjing University of Aeronautics and Astronautics, Nanjing, China — Outstanding dissertation
College of Computer Science and Technology
Supervisor: Zhe Liu

Bachelor, Computer Science 2013 - 2017
Nanjing University of Aeronautics and Astronautics, Nanjing, China — GPA 91/100, Ranking 1/281
College of Computer Science and Technology

SELECTED ACADEMIC PROJECTS

A Fast , Post-Quantum Mutual TLS Authentication Architecture in Datacenters 2024 - 2025

Accelerating post-quantum authentications in TLS 1.3 handshake for intra-datadenter communications.

- Propose a fast post-quantum authentication with online-offline computation paradigm based on WOTS^{+}.
- Achieves higher handshake throughput than its existing PQTLS counterparts by 42% with mutual authentication and 40% without.
- Paper submitted to NSDI'26 (will be online soon).

Designing Message-based Transport-Level Encryption for Datacenter Networks 2023 - 2025

A message-based , encrypted and generic transport protocol with opportunistic hardware offloading based on Homa.

- Accelerating TLS 1.3 handshake protocol with pre-distributed key shares for our proposed protocol.
- Released source code (C) and preparing to resubmit the paper.

In Mixnet We Trust? REMOTE: A Verifiable Mixnet (Re)Configuration 2022 - 2023

Remove the reliance on a single trusted third party in constructing a decentralized network with outsourced resources.

- Achieves unbiased and verifiable mixnet construction, and guarantee of nodes participation fairness.
- Utilizing applied cryptographic primitives: verifiable random function, merkle tree, and threshold signature.

Defending against Malicious Mixes with Topological Engineering 2021 - 2022

Suggested re-engineering mixnet construction and using guard layer idea to lower the risk of users being de-anonymized.

- Pointed conflicting observation: almost 100% users will fall into a fully malicious path within one week.
- Published a paper at ACSAC'2022 and released source code (Python & Rust).

INTERNSHIP

Singapore University of Technology and Design (SUTD), Singapore: Research Intern Feb 2019 – May 2019

- Supervisor: Dr. Pawel Szalachowski
- Topic: **Security Analysis of PoW Consensus algorithm**
- Applied Markov Decision Process (MDP) to model the adversary's behaviour in order to find the optimal Selfish Mining Attack Strategy on the StrongChian (Usenix'19) PoW consesnsus algorithm and the maximum profit that the adversary can get.
- Authored a technical report for the complete security analysis of StrongChain.

TECHNICAL EXPERIENCE

Independent project, Edinburgh: Service Mesh deployment with Istio July 2024

- Set up a Kubernetes cluster with 1 master and 2 worker nodes; Deployed microservices into the mesh and monitored inter-service traffic using Istio's observability tools (e.g., Prometheus, Grafana).

- Gained hands-on experience in traffic routing, telemetry collection, and service-to-service communication in a production-like environment.

Sandia National Laboratories, Austin, US: TracerFIRE (Forensic and Incident Response Exercise) Dec 2022

- Performed forensic analysis on infected machines and memory images; traffic analysis via Wireshark; reverse engineering of malicious binaries with Ghidra.

Udemy, Online: Build an custom HTTP server from scratch with Rust Oct 2021 - Dec 2021

- Understood Rust such as ownership, references & borrowing, and memory model.

PUBLICATIONS

1. Tianyi Gao, Xinshu Ma, Suhas Narreddy, Eugenio Luo, Steven Chien and Michio Honda: Designing Transport-Level Encryption for Datacenter Networks. In ACM Asia-Pacific Workshop on Networking, **APNet** 2025.

2. Xinshu Ma, Florentin Rochet, Tariq Elahi: Stopping Silent Sneaks: Defending against Malicious Mixes with Topological Engineering. In Proceedings of the 38th Annual Computer Security Applications Conference, pp. 132-145. **ACSAC** 2022.

3. Xinshu Ma, Chunpeng Ge, Zhe Liu: Blockchain-Enabled Privacy-Preserving Internet of Vehicles: Decentralized and Reputation-Based Network Architecture[C]. In International Conference on Network and System Security. Springer, Cham, 2019: 336-351. **NSS** 2019. Best Paper Award

4. Xinshu Ma, Xiaojun Zhu*, Bing Chen: Exact algorithms for maximizing lifetime of WSNs using integer linear programming. In 2017 IEEE Wireless Communications and Networking Conference (pp.1-6). IEEE. **WCNC** 2017.

* PRC Patent Application No.: 201610659332.X, Publication No.: CN106131878A, A kind of data collection method for energy heterogeneous wireless sensor network, Xiaojun Zhu, Xinshu Ma and Jing Zhang, 2016.

POSTER & TALKS

1. AUTONOMY: Auto-adaptive Well-behaved Anonymous Communication Systems
PoPETS'22 Workshop on Interdependent and Multi-party Privacy (IDP),
Sydney, Australia, July 2022.

2. Defending against Malicious Mixes with Topological Engineering
SICSA'22 PhD Conference,
Glasgow, UK, June 2022.

3. Bow-Tie: Towards Secure Mix Network Topological Construction Algorithm
REPHRAIN All-Hands Meeting Poster Session, Best Poster Award
Bristol, UK, March 2022.

SELECTED AWARDS AND HONOURS

June. 2023	PoPETS Stipend (USD 1,610)
June. 2023	SICSA Research Scholarship (GBP 500)
Mar. 2022	SICSA Research Travel Funding (GBP 500)
Aug. 2020	First Prize of Jiangsu Province 'Internet Plus' Innovation and Entrepreneurship Competition
Dec. 2017	Second Prize of Information Security and Countermeasures Contest
Oct. 2017	**First Class Graduate Freshmen Scholarship** (CNY 20,000, 1/190)

TECHNICAL SKILLS

Programming: C, Python, Rust, C++ **Tools:** Kubernetes, Istio, Picotls, Picoquic **Language:** IELTS 7.0