Haowen Liu

(+41) 762693736 | E-mail: haowen.liu@epfl.ch | Homepage | LinkedIn

Interests

Computer Security, Trustworthy AI, Cyber Security, Computer Networks, IoT/IoV

Education

EPF Lausanne - ETH Zurich Lausanne/Zurich, Switzerland
Joint Master of Science in Computer Science - Cyber Security *Sep. 2021 – Present*

Shanghai Jiao Tong University Shanghai, China
Bachelor of Engineering in Information Security, Minor in Japanese *Sep. 2017 – June 2021*

Professional Experience

École Polytechnique Fédérale de Lausanne Jan. 2023 – Present
Research Assistant, Distributed Computing Lab | Supervised by Prof. Rachid Guerraoui *Jan. 2023 – Present*

- Develop a strong benchmark for attacks in Byzantine ML.
- Implement and play with two-dimensional mean estimation toy example. Explore using heuristics, NLP solver, RL model
- Depending on results, scale up to standard tasks: MNIST, CIFAR-10

Shanghai Jiao Tong University Oct. 2019 – May 2021
Research Assistant, AI Security Lab | Supervised by Prof. Ping Yi *Oct. 2019 – May 2021*

- Proposed a new adversarial example defense method (DAFAR) based on feedback network (decoder).
- Wrote a paper and a patent about DAFAR.

Research Projects

Benchmark to Certify Byzantine-robustness in ML | *Distributed System, ML* Jan. 2023 – Present

- **Project:** Semester Research Project
- **Supervisor:** Prof. Rachid Guerraoui (Full Professor, EPFL), Youssef Allouah (Doctoral Student)
- **Content:** Multiple attacks have been proposed to instantiate a Byzantine adversary in distributed ML. While these attacks have been successful against known defenses, it remains unknown whether stronger attacks exist. As such, a strong benchmark is needed, to go beyond the cat-and-mouse game illustrating the existing research. Ideally, similar to other ML subfields such as privacy-preserving ML or adversarial examples, the desired benchmark should guarantee that no stronger attack exists. Goal: Develop a strong benchmark for attacks in Byzantine ML.

Attack Graph Generation Technique for V2X Internet of Vehicles | *IoV Security* Jan. 2021 – June 2021

- **Project:** Bachelor Thesis
- **Supervisor:** Prof. Jin Ma (Associate Professor)
- **Content:** Design a real-time security information collection protocol in IoV to conduct real-time security situation awareness. Implement a prototype system of IoV attack graph generation system based on causality to analyze and assess risks in the system.
- **Output:** 1 Graduation Thesis, a prototype

Adversarial Example Defense Based on Feedback Network | *Security in ML* Oct. 2019 – May 2021

- **Project:** Cybersecurity Innovation Joint Lab HUAWEI-SJTU, YBN2019105168-SOW06, $100,000
- **Supervisor:** Prof. Ping Yi (Associate Professor), Dr. Hsiao-Ying Lin (Senior Researcher, Huawei International)
- **Content:** Propose a new adversarial example defense method based on a feedback network, which uses the feedback network to eliminate or detect the adversarial disturbance in input. Implement a prototype system.
- **Output:** *Outstanding Individual Award*, 1 manuscript, 1 patent (published), a prototype

A Semi Passive Security Analysis Tool for ICS | *Network Security, Attack Graph* Oct. 2019 – Sep. 2020

- **Project:** The 13th National College Student Information Security Contest
- **Supervisor:** Prof. Gongshen Liu (Professor)

- **Content:** Propose a semi-passive method to dynamically collect network security information in ICS and conduct real-time situation awareness by Bayesian Attack Graph by improving MulVAL and Grassmarlin. Implement a prototype.
- **Output:** *National First Prize*, 1 patent (published), a prototype system

Retinal Scanning Display for Mixed Reality | *AR, Optics, Waveguide, Laser* April 2018 – Sep. 2019

- **Project:** 34th Participation in Research Program (PRP) project, T030PRP34068
- **Supervisor:** Prof. CHAO PING CHEN (Associate Professor)
- **Content:** Present a design of a contact lens display, which features an array of collimated light-emitting diodes and a contact lens, for augmented reality. The resolution of light-emitting diodes is foveated to match the density of cones on the retina.
- **Output:** 1 journal paper (published), 1 conference paper (published), 1 patent (published)

Publications

Manuscript

[1]. **Haowen Liu**, Ping Yi, Hsiao-Ying Lin, Jie Shi, Weidong Qiu. DAFAR: Defending against Adversaries by Feedback-Autoencoder Reconstruction. *arXiv preprint arXiv:2103.06487*, 2021.

Conference

[1]. Jie Chen, Lantian Mi, Chao Ping Chen*, **Haowen Liu**, Jinghui Jiang, Wenbo Zhang, Yuan Liu. A Foveated Contact Lens Display for Augmented Reality. *Proc. SPIE, Optical Architectures for Displays and Sensing in Augmented, Virtual, and Mixed Reality (AR, VR, MR) (**SPIE AR VR MR**)*, in San Francisco, California, United States, 2020. (**Oral**)

Journal

[1]. Jie Chen, Lantian Mi, Chao Ping Chen*, **Haowen Liu**, Jinghui Jiang, Wenbo Zhang. Design of Foveated Contact Lens Display for Augmented Reality. *Optics Express (**OE**)*, Vol.27, No.26, pp. 38204-38219, 2019.

Patent

[1]. Ping Yi, **Haowen Liu**, Hsiao-Ying Lin. System and Method of Adversarial Example Detection Based on Feedback Reconstruction. 2020.12, Publication Number: WO/2022/104503.

[2]. Jianming Guo, Gongshen Liu, Zi'ang Chen, **Haowen Liu**, Zihan Liu. A Semi Passive Security Analysis Tool for Industrial Control Network Based on Bayesian Attack Graph. 2020.11, Publication Number: CN112653582B.

[3]. Jie Chen, Chao Ping Chen, **Haowen Liu**, Jinghui Jiang, Lantian Mi. Intraocular Display Device Based on Retinal Scanning. 2019.12, Publication Number: CN110955063B.

Course Projects

Reliable and Trustworthy Artificial Intelligence (ETHZ): ReLU DeepPoly transformer and Verifier (PyTorch)
Software Security (EPFL): Code review/Unit tests (C, Check); CTF; Symbolic Execution (Python); Fuzzing (C, AFL, libFuzzer)
Network Security (ETHZ): Implementation of ACME Protocol (Python); Defend the Flag (nftables)
System Security (ETHZ): Exploiting an HTTPS webserver (Linux, Metasploit); Reverse Engineering an executable (Ghidra, z3); Writing an Intel SGX Enclave Application (C++)
Concurrent algorithms (EPFL): Implementing a software transactional memory library (C)
Data Visualization (EPFL): Creating a cool, interactive, and sufficiently complex D3.js (and other) data viz on a dataset (Python, JavaScript, HTML)
Database Systems (EPFL): Relational Operators and Execution Models (Scala); Implementing data processing pipelines over Apache Spark (Scala, Spark)
Cryptography and Security (EPFL): Implementing symmetric/asymmetric cryptography; Implementing homomorphic encryption
TCP/IP networking (EPFL): A bunch of network practice using Mininet (Python, Mininet)
Information Security and Privacy (EPFL): A bunch of basic security practice

Technical Skills

Programming Languages: Python, C/C++, JavaScript, Scala, SQL, HTML
Frameworks: PyTorch, Tensorflow, Django, Flask
Developer Tools: Git, docker, Ghidra, VMware, PyCharm, Vivado, LaTeX, Sublime, libFuzzer
Disciplines: Computer Security, Machine Learning, Computer Networks, Cryptography, Electrics
Language: English (professional working proficiency), Chinese (native proficiency), Japanese (limited working proficiency)

Honors

- 2021, **Outstanding Individual Award** in Cybersecurity Innovation Joint Lab HUAWEI-SJTU ($4000)
- 2020, **Third Prize** in 6th Qian Xuesen Cup Contest
- 2020, **First Prize** in 13th National College Student Information Security Contest (rate: nationwide $32/540, 6\%$)
- 2020, **Honorable Mention** for Interdisciplinary Contest In Modeling
- 2019, AY 2018-2019 **Academic Progress** Scholarship
- 2019, AY 2018-2019 Class C of **Excellent Undergraduate** Scholarship
- 2019, **Honorable Mention** for Mathematical Contest In Modeling
- 2019, **Outstanding Project** in 34th PRP Program
- 2018, **Third Prize** in 35th National College Student Physics Contest (Shanghai Area)
- 2017, **Zhiyuan Honors** Program (Engineering) Fellowship

Last updated: Feb., 2023.