

# Haowen Liu

(+86) 152-2123-9717 | [haowen.liu@epfl.ch](mailto:haowen.liu@epfl.ch) | [mekakuactor.github.io](https://mekakuactor.github.io) | [github.com/MekAkUActOR](https://github.com/MekAkUActOR)

## RESEARCH INTERESTS

---

**Computer Security, Cyber Security, Computer Architecture, AI Security, IoT/IoV**

## EDUCATION

---

**EPF Lausanne - ETH Zurich**

*Joint Master of Science in Computer Science - Cyber Security*

Lausanne/Zurich, Switzerland

Sep. 2021 – Present

**Shanghai Jiao Tong University**

*Bachelor of Engineering in Information Security, Minor in Japanese*

Shanghai, China

Sep. 2017 – June 2021

## PROFESSIONAL EXPERIENCE

---

**Shanghai Jiao Tong University**

*Research Assistant, AI Security Lab | Supervised by Ping Yi*

Oct. 2019 – May 2021

Oct. 2019 – May 2021

- Proposed a new adversarial example defense method (DAFAR) based on feedback network (decoder).
- Implemented a prototype system of DAFAR using PyTorch and passed the acceptance check of HUAWEI.
- Wrote a paper and a patent about DAFAR.

## RESEARCH PROJECTS

---

**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

**RowHammer Mitigation Method | Computer Arch&Sec, DRAM**

Sep. 2020 – June 2021

- **Project:** IGP-C Application
- **Supervisor:** Prof. Hiroshi Sasaki (Associate Professor, Tokyo Institute of Technology)
- **Content:** Study causes and characteristics of RowHammer, the existing attack methods based on RowHammer, and RowHammer mitigation methods. Summarized about 30 impactful works about RowHammer and proposed the preliminary design of a cache-based RowHammer mitigation mechanism.

**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:** ReLU DeepPoly transformer and Verifier (PyTorch)

**Network Security:** Implementation of ACME Protocol (Python); Defend the Flag (nftables)

**System Security:** Exploiting an HTTPS webserver (Linux, Metasploit); Reverse Engineering an executable (Ghidra, z3); Writing an Intel SGX Enclave Application (C++)

**Concurrent algorithms:** Implementing a software transactional memory library (C)

**Software security:** Code review/Unit tests (C, Check); CTF; Symbolic Execution (Python); Fuzzing (C, AFL, libFuzzer)

**Database Systems:** Relational Operators and Execution Models (Scala); Implementing data processing pipelines over Apache Spark (Scala, Spark)

**TCP/IP networking:** A bunch of network practice using Mininet (Python, Mininet)

## TECHNICAL SKILLS

---

**Languages:** Python, C/C++, Verilog, JavaScript, Scala, HTML, x86 Assembly

**Frameworks:** Django, PyTorch, Tensorflow, Flask

**Developer Tools:** Git, Ghidra, IDEA, PyCharm, Vivado, L<sup>A</sup>T<sub>E</sub>X, Xcode, Sublime, libFuzzer

**Disciplines:** Computer Security, Cryptography, Computer Architecture, Deep Learning, Electronics

## 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
- 2018, **Third Prize** in 35th National College Student Physics Contest (Shanghai Area)
- 2017, **Zhiyuan Honors** Program of Engineering Scholarship