Haowen Liu

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

Research Interests

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

Education

Shanghai Jiao Tong University Shanghai, China
Bachelor of Engineering in Information Security, Minor in Japanese | GPA 87 *Sep. 2017 – June 2021*

Professional Experience

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

- Proposed a new adversarial example defense method (DAFAR) based on feedback network.
- 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:** Graduation Thesis
- **Supervisor:** 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 find the security problems caused by the combination of vulnerabilities in the system.
- **Output:** 1 Graduation Thesis, 1 conference paper (writing), a prototype system

RowHammer Mitigation Method | *Computer Arch&Sec, DRAM* Sep. 2020 – June 2021

- **Project:** IGP-C Application
- **Supervisor:** Hiroshi Sasaki (Associate Professor, Tokyo Institute of Technology)
- **Content:** Study the 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.

Vulnerability Analysis Based on Attack Graph in IoV | *IoV Security* April. 2020 – Sep. 2020

- **Project:** Professional Practice (Information Security)
- **Supervisor:** Xiuzhen Chen (Associate Professor)
- **Content:** Analyze the vulnerabilities inside IoV based on attack graph technology using MulVAL. Find the attack dependency in IoV based on *ATT&CK* matrices.

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

- **Project:** 13th National College Student Information Security Contest
- **Supervisor:** Gongshen Liu (Professor)
- **Content:** Propose a semi-passive method to dynamically collect network security information in ICS to conduct real-time situation awareness by Bayesian Attack Graph by improving MulVAL and Grassmarlin. Implement a prototype system.
- **Output:** *National First Prize*, 1 patent application, a prototype system

Adversarial Example Defense Based on Feedback Network | *Deep Learning* Oct. 2019 – May 2021

- **Project:** Cybersecurity Innovation Joint Lab HUAWEI-SJTU, YBN2019105168-SOW06, RMB 620,000
- **Supervisor:** Ping Yi (Associate Professor), Hsiao-Ying Lin (Senior Researcher, Huawei International)
- **Content:** Propose a new adversarial example defense method based on feedback network, which uses feedback network to eliminate or detect adversarial disturbance in input. Implement a prototype system.
- **Output:** *Outstanding Individual Award*, 1 journal paper (under review), 1 patent application, 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:** 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 the augmented reality. The resolution of light-emitting diodes is foveated to match with the density of cones on the retina.
- **Output:** 1 journal paper (published), 1 conference paper (published), 1 patent (authorized)

Publications

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]. **Haowen Liu**, Ping Yi*, Hsiao-Ying Lin, Jie Shi, Weidong Qiu. DAFAR: Defending against Adversaries by Feedback-Autoencoder Reconstruction. under submission to *IEEE Transactions on Dependable and Secure Computing (**TDSC**)*, Special Issue on Software Reliability and Dependability Engineering. *arXiv preprint arXiv:2103.06487*, 2021.

[2]. 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, Application Number: PCT/CN2020/129298.

[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, Application Number: CN202011519498.4.

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

Technical Skills

Languages: Python, C/C++, Verilog, SQL, HTML, x86 Assembly
Frameworks: Django, Nginx, PyTorch, MFC
Developer Tools: Git, Visual Studio, PyCharm, Xilinx, LaTeX, Xcode, Spyder, Sublime, SolidWorks, AutoCAD
Disciplines: Cyber Science, Computer Security, Cryptography, Computer Architecture, Deep Learning, Electrics

Honors

- 2021, **Outstanding Individual Award**[1] in Cybersecurity Innovation Joint Lab HUAWEI-SJTU (RMB 20,000)
- 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

Last updated: July 25, 2021.

[1] 2 professors, 1 Ph.D. student, 1 undergraduate student