Haowen Liu

(+86) 152-2123-9717 | HaowenLiew@outlook.com | mekakuactor.github.io | github.com/MekAkUActOR

Research Interests

Computer Security, Computer Architecture, Artificial Intelligence Security, Network Security

Education

Shanghai Jiao Tong University — Shanghai, China
Bachelor of Engineering in Information Security, Minor in Japanese | GPA 86.93 — *Sep. 2017 – June 2021*

NO.1 Middle School of Linchuan — Jiangxi Province, China
High School Diploma — *Sep. 2014 – June 2017*

Experience

Undergraduate Research Assistant — Shanghai Jiao Tong University, China

IoV Security Group | Supervised by Zhihong Zhou — *April. 2020 – Aug. 2020*

- Explored how to apply attack graph in IoV for security analysis
- Wrote a draft of a book chapter about summary of Attack Graph Technique
- Provided knowledge and advice about Attack Graph Technique, especially MulVAL

AI Security Lab | Supervised by Ping Yi — *Oct. 2019 – Present*

- 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 CVPR paper and a patent about DAFAR
- Explored ways to further defend against adversarial examples with high universality and accuracy

Research Projects

RowHammer Mitigation Method | *Computer Arch&Sec, DRAM* — Sep. 2020 – Present

- **Project:** Overseas Application and Research
- **Supervisor:** Hiroshi Sasaki (Associate Professor, Tokyo Institution of Technology)
- **Research Content:** Study the causes and characteristics of RowHammer, the existing attack methods based on RowHammer and mitigation methods. Try to propose an area-efficient and low-overhead mitigation method against RowHammer attack.

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

- **Project:** Graduation Thesis
- **Supervisor:** Jin Ma (Associate Professor)
- **Research Content:** Implement a prototype of IoV attack graph generation system based on causality to find the security problems caused by the combination of vulnerabilities in the system.
- **Project Output:** 1 Graduation Thesis, a prototype system (in progress)

Vulnerability Analysis Based on Attack Graph in Vehicle Internet | *IoV Security* — Aug. 2020 – Sep. 2020

- **Project:** Undergraduate Summer Internship Program
- **Supervisor:** Xiuzhen Chen (Associate Professor)
- **Research Content:** Analyze the vulnerabilities inside IoV based on attack graph technology using MulVAL. Find the attack dependency in IoV based on $ATT\&CK$ matrices.

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

- **Project:** HUAWEI-SJTU Innovation Joint Laboratory of Cyber Security, YBN2019105168-SOW06
- **Supervisor:** Ping Yi (Associate Professor)
- **Research 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.
- **Project Output:** 1 top conference paper (submitted), 1 patent (filed), a prototype system

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)
- **Research Content:** Propose a semi passive method to help network managers for security analysis of Industrial Control System based on Bayesian Attack Graph by improving MulVAL. Implement a prototype system.
- **Project Output:** First Prize, 1 patent (filed), a prototype system

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

- **Project:** 34th PRP project, T030PRP34068
- **Supervisor:** CHAO PING CHEN (Associate Professor)
- **Research 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.
- **Project Output:** 1 journal paper (published), 1 conference paper (published), 1 patent (authorized)

Publications

Conferences

[1]. Jie Chen, Lantian Mi, Chao Ping Chen, **Haowen Liu**, Jinghui Jiang, Wenbo Zhang, and 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**)

Journals

[1]. Jie Chen, Lantian Mi, Chao Ping Chen, **Haowen Liu**, Jinghui Jiang, and Wenbo Zhang, "Design of foveated contact lens display for augmented reality", *Optics Express (**OE**)*, Vol.27, No.26, pp. 38204-38219, 2019.

Patents

[1]. Ping Yi, **Haowen Liu**, Hsiao-Ying Lin, "System and Method of Adversarial Example Detection Based on Feedback Reconstruction", 2020.11, Application Number: PCT/CN2020/129298.

[2]. Jianming Guo, Gongshen Liu, Ziang Chen, **Haowen Liu**, Zihan Liu, "A Semi Passive Security Analysis Tool for Industrial Control Network using Bayesian Attack Graph Technique", 2020.12, 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++, SQL, Verilog, 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

- 2020, **Third Prize** for the 6th Qian Xuesen Cup Contest
- 2020, **First Prize** for the 13th National College Student Information Security Contest
- 2020, **Honorable Mention** for Interdisciplinary Contest In Modeling
- 2019, AY 2018-2019 **Academic Progress** Scholarship
- 2019, AY 2018-2019 **Class C** Scholarship
- 2019, **Honorable Mention** for Mathematical Contest In Modeling
- 2019, **Outstanding Project** in 34th PRP
- 2018, **Third Prize** for the 35th National College Student Physics Contest
- 2017, **Zhiyuan Honors** Program of Engineering Scholarship