

JING LI

No.19 Shucun Road, Haidian District, Beijing, China 100084

☎ (86) 188-0527-7553 ✉ lixeon.lij@gmail.com [LinkedIn](#) [Github](#) [HomePage](#)

Profile Summary

Interested to pursue a PhD or Research Assistant in Machine Learning System, Artificial Intelligence Security, MLOps, ML for Healthcare or in an aligned area.

Education

University of Chinese Academy of Sciences **Sep. 2020 – Jun. 2023 (expect)**
Master of Science (M.Sc) in Cybersecurity [GPA: 3.54/4.0] *Beijing, China*

- Minor: Management of Technology
- Supervisor: Prof.Rui Hou. Research areas: MLSys and MLOps Security, Deep Learning Compiler
- Relevant Coursework: Cybersecurity Strategy; Computer Architecture; AI System; Critical Thinking
- Thesis: Mimic Octopus Attack: Dynamic Camouflage Coverage Adversarial Examples in Digital and Physical

Gap year **Jun. 2019 – Sep. 2020**
Shenyang, China & Nantong, China & Tieling, China

- Accompany family and travel
- During this period, manage the family's grocery store and print shop
- Nearly half the time, prepare for exams and certifications like the Chinese Gap year

Yangzhou University **Sep. 2015 – Jun. 2019**
Bachelor of Engineering (B.Eng) in Software Engineering(NIIT, bilingual) [GPA: 3.82/4.0] *Yangzhou, China*

- Supervisor: Prof.Lejun Zhang
- Thesis: Web Application Firewall based OpenResty Design and Implementation

Experience

Institute of Information Engineering, Chinese Academy of Sciences **Dec. 2020 – Jun.2023 (expect)**
Graduate Research Assistant, Advisors: Prof.Rui Hou, Assoc.Prof.Xingbin Wang *Beijing, China*

- Study and reproduction papers, 10+ Reports and Patents writing, Technical principles presentation, and Brainstorm.
- Working with authors, assessed and improved reproducibility for 4 papers using C, Python, and L^AT_EX.
- Developed a service to automatically perform a set of unit tests daily on Artificialities in development in order to decrease time needed for 60+ team members to identify and fix bugs/issues, and 2 Racks Servers operation.

MiraclePlus (former Y Combinator China) **Jul. 2022 – Aug. 2022**
Campus Scout *Remote & Beijing, China*

- Actually, I am going to start an undertaking during my PhD if possible.
- In this experience, I help complete the task of deal sourcing and due diligence.

Network Security Research Center, Yangzhou University **Apr. 2017 – Jun. 2019**
Research Assistant, Advisors:Prof.Lejun Zhang, Prof.Caikou Chen, Prof.Liucun Zhu *Yangzhou, China*

- Netgear Router Firmware development, OpenResty and Lua lightweight software WAF design and implementation.
- Collaborated with 10+ team members using Git and CI/CD to organize modifications and assign tasks.

Fatong Legal Consulting (Startup, Inc) **Apr. 2018 – Jun. 2019**
Co-founder, CIO, Computer Technical Support *Zhenjiang, China*

- Developed an automatic processing tool for legal documents using Python crawler and NLP.

Publications

Manuscript

- Mimic Octopus Attack: Dynamic Camouflage Coverage Adversarial Examples in Digital and Physical
- Improve attack Robust via application scenarios and design Confident method to defense

Journal Articles

- The Develop of Learn and Teach Online One-Stop Service Platform Based on React Native
Jing Li, Caikou Chen, Yu Lu, Zimeng Sheng, Lei Zhu, Zhentao Sui
Computer Knowledge and Technology, Vol.14, No.27, 2018.
- Research on the integration solution of information system of university students' panoramic analysis
Jing Li, Caikou Chen
Peak Data Science, No.3, 2018.

Patents

- A method of learning situation analysis based on React Native
Jing Li, Caikou Chen, Zimeng Sheng, Lei Zhu, Yu Lu, Zhentao Sui
CN108845796B, CN Invention Patent, Issued Dec 14, 2021.
- A kind of one master and multiple slaves formula intelligent video monitoring apparatus
Zhibo Guo, Yi Zhang, Yue Zhang, Jing Li, Zhangjie Gong, Xiaoyan Guo, Lian Xue
CN208241780U, CN Utility Model Patent, Issued Dec 14, 2018.

Projects

Physical Adversarial Attack and Defense Research | *Academic, PyTorch, TensorFlow* **Aug. 2021 – Present**

- Deep understanding SOTA models and methods then reproduction in the Real-world.
- Improve attack Robust via application scenarios and design Confident method to defense. [In the Manuscript]

More Security and Performance trade off GPU architecture | *Academic, TVM, NVM, gem5* **Sep. 2021 – Present**

- Study how to develop deep learning compiler and how SOTA scheduler formulates deep learning programs with CUDA.
- Design new fine-grained scheduling algorithm, and strengthen Model Privacy by the AI compiler. [In the Manuscript]

Rust TEE Homomorphic Encryption module | *Rust, Federated AI, Intel SGX* **Mar. 2021 – Aug. 2021**

- TEE-empowered computer systems research, and develop a HE module using Rust under Intel SGX.

Software Toolchain Porting for Self R&D Sunway RISC-V Processor | *QEMU, Docker, GCC, LLVM* **Jan. 2021**

- Created cross-compilation setup for only support RV64G ISA Chip to porting embedded system , then Burn into board.

Learn and Teach Online App | *JavaScript, React, Android, Prototype Design* **Jun. 2017 – Jun. 2018**

- Created an cross-platform application using JavaScript framework to manage student information in YZU.

Skills

Programming: Python, C/C++, Linux (Over 5000 lines) ; JavaScript, PHP, SQL (Over 1000 lines) ; Chisel, PWN
Languages: English(Fluent) , Chinese(Native), Shanghainese(Native), Jianghuai Mandarin(Native), Cantonese(Basic)
Qualifications: PM, CISP, Huawei Advocate, Cambricon Campus Developer, MOS Expert, ACCA, ACM Student Member
Hobbies: Photography, Popular Science Writing, History, Singing, Amateur Radio-BI1MYB, Gaming-WoW,CSGO,SLG

Extracurricular

- Led chapter of 50+ members to work towards goals that improve and promote community service, academics, and unity.
- Volunteered, organized and held more than 100 campus salons and cultural and artistic activities.
- 7 Lectures to 150+ undergraduates about how to prepare National Postgraduate Entrance Exam. [Assessment:4.63/5.0]
- 11th Capital Internet+ Competition Outstanding Winner(Analysis key features of CD-SEM photoresist sample picture).

Fun facts about me

- I don't care about work space but it's best if there are green plants.
- My favorite communication style is to tell the truth, especially when we working together, please criticize directly. And lack of integrity is a bomb for cooperation with me.
- My parents are from the north and the south of China. Although they divorced when I was 12 years old, they are always with me.
- I am not very tall, just 161 cm like President Deng Xiaoping who is also my favorite great person. And I am very healthy at least now.
- My first encounter with personal computers in 2004 and the Internet in 2006 when I was 9 years old because my family manage a print shop at that time. And since then I have had the experience of keeping the store.

Last updated on Aug. 2022