Huichen Li

huichenli.cs@gmail.com • huichenli.net

Education

Aug. 2018 - now: **Ph.D. student** *Computer Science*.
Department of Computer Science, University of Illinois Urbana-Champaign, US
- GPA: 4.0/4.0

2014 - 2018: **Bachelor of Engineering** *Computer Science and Technology*.
ACM Honors Class, Zhiyuan College, Shanghai Jiao Tong University, China
- GPA: 3.78/4.3;

Publications

Progressive-Scale Boundary Blackbox Attack via Projective Gradient Estimation,
Jiawei Zhang*, Linyi Li*, Huichen Li, Xiaolu Zhang, Shuang Yang, Bo Li.
- To appear at ICML2021.

Nonlinear Projection Based Gradient Estimation for Query Efficient Blackbox Attacks,
Huichen Li*, Linyi Li*, Xiaojun Xu, Xiaolu Zhang, Shuang Yang, Bo Li.
- Appeared at AISTATS2021 (paper link).

Detecting AI Trojans Using Meta Neural Analysis,
Xiaojun Xu, Qi Wang, Huichen Li, Nikita Borisov, Carl A. Gunter, Bo Li.
- To appear at IEEE Symposium on Security and Privacy (Oakland) 2021 (arXiv link).

QEBA: Query-Efficient Boundary-Based Blackbox Attack,
Huichen Li*, Xiaojun Xu*, Xiaolu Zhang, Shuang Yang, Bo Li.
- Appeared at CVPR2020 (paper link);

A Machine Learning Approach To Prevent Malicious Calls Over Telephony Networks,
Huichen Li, Xiaojun Xu, Chang Liu, Teng Ren, Kun Wu, Xuezhi Cao, Weinan Zhang, Yong Yu, Dawn Song.
- Appeared at IEEE Symposium on Security and Privacy (Oakland) 2018 (paper link);
- My conference talk (YouTube link).

The symbol * indicates equal contribution.

Preprints and Submissions

Exploring Adversarial Robustness of Multi-Sensor Perception Systems in Self Driving,
James Tu, Huichen Li, Xinchen Yan, Mengye Ren, Yun Chen, Ming Liang, Eilyan Bitar, Ersin Yumer, Raquel Urtasun.
- In submission (arXiv link).

Data Poisoning Attack against Unsupervised Node Embedding Methods,
Mingjie Sun, Jian Tang, Huichen Li, Bo Li, Chaowei Xiao, Yao Chen, Dawn Song.
- In submission (arXiv link).

Internships

Jun. 2020 - Aug. 2020: **Uber ATG** *Multi-modality Adversarial Robustness*, Research Intern.

Jun. 2019 - Aug. 2019: **Ant Financial** *Adversarial Attack on Image Recognition*, Research Intern.

Jun. 2018 - Jul. 2018: **Tencent Technology** *Adversarial Attack on Graph*, Research Intern.

Experience

Aug. 2018 - May. 2020: **Research Assistant** *Adversarial Machine Learning*, Prof. Bo Li, University of Illinois Urbana-Champaign, US.

Jun. 2017 - Dec. 2017: **Research Intern** *Low Rank Optimization*, Prof. Madeleine Udell & Prof. Nathan Kallus, Cornell University, US.

Sep. 2017 - Nov. 2017: **Research Intern (Remote)** *Large-scale Phone Call Network Analysis and Malicious Call Prevention*, Prof. Dawn Song, University of California, Berkeley, US.

Sep. 2016 - May. 2017: **Research Intern** *Early Spam Detection in Phone Call Network*, Prof. Yong Yu & Prof. Weinan Zhang, Shanghai Jiao Tong University, China.

Honors

Chirag Foundation Graduate Fellowship in Computer Science *The Department of Computer Science*, University of Illinois Urbana-Champaign, US.

Outstanding Graduates, Shanghai Jiao Tong University, China.

Kaiyuan Scholarship, Shanghai Jiao Tong University, China.

Scholarship of SJTU, Shanghai Jiao Tong University, China.

Zhiyuan Honored Scholarship *Zhiyuan College*, Shanghai Jiao Tong University, China.

Awards

1st Prize *Deep Learning and Security Innovation Hackathon @ Singapore*.
`http://sgcsc.sg/event-2017-02-cybercamp.html`.

Champion *China Collegiate Programming Contest Female Final (CCPC-FF) 2016*.

Honorable Mention *2017 Mathematical Contest In Modeling*.

Academic Services

Conference Paper Reviewer / Program Committee Member: NeurIPS 2020/2021; CVPR 2021; ICCV 2021; AAAI 2020/2021; AISTATS 2021; SSMLS (workshop) 2021; AdvML (workshop) 2020; SPML (workshop) 2019.

Journal Reviewer: Transactions on Computer-Aided Design of Integrated Circuits and Systems;

Teaching Assistant: Graduate course Advanced Computer Security, UIUC, 2020; Undergraduate course Compiler Principle, SJTU, 2017.

Language and Arts

English:
- TOEFL iBT: Total 109/120, Reading 26/30, Listening 29/30, Speaking 27/30, Writing 27/30
- GRE General Test: Verbal 159/170, Quantitative 170/170, Analytical Writing 4/6

Erhu: A traditional Chinese bowed string instrument. Professional Level A with certificate from Zhejiang Province Musicians Association in China.

Latest update date: May 10, 2021