Yucheng Yin

4720 Forbes Ave, CIC 2223F – Pittsburgh, PA 15213
+1 (734)-680-7608 • yyin4@andrew.cmu.edu • sniperyyc.com
sniperyyc

Education

Carnegie Mellon University — **Pittsburgh, PA, USA**
Ph.D. of Electrical and Computer Engineering — *September 2018 - August 2024 (expected)*
Advisor: Vyas Sekar

University of Michigan — **Ann Arbor, MI, USA**
Bachelor of Computer Science Engineering — *September 2016 - May 2018*
GPA: 3.9/4.0. Summa cum laude

Shanghai Jiao Tong University (SJTU) — **Shanghai, China**
Bachelor of Electrical and Computer Engineering — *September 2014 - August 2018*
GPA: 3.8/4.0. Rank: 10/189. Graduation Speaker

Research Interests

Machine Learning (Deep Generative Models), Network Security

Publications

[1] **Yucheng Yin**, Seo Young Ko, Zinan Lin, Minhao Jin, Jorge Guajardo Merchan, Giulia Fanti, and Vyas Sekar. "DeepStore: A Framework for Evaluating the Viability of Deep Generative Compression for Long-Term Network Trace Storage". Under preparation.

[2] **Yucheng Yin**, Jorge Guajardo Merchan, Pradeep Pappachan, and Vyas Sekar. "CANGen: Practical Synthetic CAN Traces Generation using Deep Generative Models". Under preparation.

[3] **Yucheng Yin**, Zinan Lin, Minhao Jin, Giulia Fanti, and Vyas Sekar. "Practical gan-based synthetic ip header trace generation using netshare". In: *Proceedings of the ACM SIGCOMM 2022 Conference*. 2022, pp. 458–472.

[4] **Yucheng Yin**, Zinan Lin, Minhao Jin, Giulia Fanti, and Vyas Sekar. "PcapShare: Exploring the Feasibility of GANs for Synthetic Packet Header Trace Generation". In: *Fourteenth InternationalConference on COMmunication Systems and NETworkS(COMSNETS) (demo)*. 2022.

[5] Soo-Jin Moon, **Yucheng Yin**, Rahul Anand Sharma, Yifei Yuan, Jonathan M Spring, and Vyas Sekar. "Accurately measuring global risk of amplification attacks using ampmap". In: Proceedings of the 30th {USENIX} Security Symposium. 2021.

[6] Soo-Jin Moon, **Yucheng Yin**, Rahul Sharma, Yifei Yuan, Jonathan Spring, and Vyas Sekar. *Accurately Measuring Global Risk of Amplification Attacks using AmpMap*. Technical Report CMU-CyLab-19-004. Carnegie Mellon University, 2020.

[7] Qi Alfred Chen, **Yucheng Yin**, Yiheng Feng, Z Morley Mao, and Henry X Liu. "Exposing congestion attack on emerging connected vehicle based traffic signal control." In: *Network and Distributed System Security (NDSS) Symposium*. 2018.

[8] Qi Alfred Chen, **Yucheng Yin**, Yiheng Feng, Z Morley Mao, and Henry X Liu. "Exposing Falsified Data Attacks on CV-based Traffic Signal Control". In: *Proceedings of the 26th {USENIX} Security Symposium (Poster)*. 2017.

[9] Fan Xia, Tian Xia, Li Xiang, Sujuan Ding, Shuo Li, **Yucheng Yin**, Meiqi Xi, Chuanhong Jin, Xuelei Liang, and Youfan Hu. "Carbon Nanotube-Based Flexible Ferroelectric Synaptic Transistors for Neuromorphic Computing". In: *ACS Applied Materials & Interfaces* 14.26 (2022), pp. 30124–30132.

Honors and Awards

- Carnegie Institute of Technology Dean's Fellow 2018
- CRA Outstanding Undergraduate Researcher Honorable Mentions 2018
- UM-SJTU Joint Institute Dean's List FA2014/SU2015/FA2015/SU2016
- University of Michigan Dean's List, University Honors FA2016/FA2017/WN17
- SJTU Outstanding Scholarship (B) 2015
- Outstanding Assistant Class Advisor (UM-SJTU Joint Institute) 2015
- National Chemistry Contest for High School Students, first prize 2013

Professional Experiences

Research Intern, Bosch Research **Pittsburgh, PA, USA**
Mentor: Jorge Guajardo Merchan *May 2022 - December 2022*

- Synthetic Controller Area Network (CAN) Trace Generation by Deep Generative Models

Graduate Research Assistant, Carnegie Mellon University **Pittsburgh, PA, USA**
Advisor: Vyas Sekar *September 2018 - Present*

- Trustworthy Sketch-based Measurement in Software Switches using SGX
- Measurement of amplification attack risk at a global scale
- Application of Deep Generative Models to Synthetic Network Trace Generation

Research Assistant, University of Michigan **Ann Arbor, MI, USA**
Advisor: Z. Morley Mao, Dimitra Panagou *May 2017 - August 2017*

- Security Analysis of CV-based Traffic Control System
- A Simulation Environment for Multi-Agent Trajectory Planning

Invited Talks

Practical GAN-based Synthetic IP Header Trace Generation using NetShare (web demo)

- FloCon 2023, Santa Fe, NM (talk slides) January 2023
- ZeekWeek 2022, Austin, TX (talk video) October 2022
- CyLab Partners Conference 2022, Pittsburgh, PA October 2022
- SIGCOMM 2022, Amsterdam, the Netherlands (talk video) August 2022

Trustworthy Sketch-based Measurement in Software Switches using SGX

- CONIX Student-Liaison Seminar, CMU, Pittsburgh, PA October 2019
- "Tuesday" Networking Seminar, CMU, Pittsburgh, PA January 2019

Teaching Experiences

18731 Network Security **Pittsburgh, PA, USA**
Teaching Assistant, CMU *Spring 2022, Spring 2023*

- Made and graded homework and exam problems. Held weekly office hours.

VE280 Programming and Elementary Data Structures **Shanghai, China**
Teaching Assistant, SJTU *Summer 2018*

- Gave recitation class. Graded homework. Made exam problems. Held weekly office hours.

Skills

Programming Languages

C, C++, Python, Java, MATLAB, Mathematica, PHP, JavaScript, HTML, CSS, SQL, Verilog, Assembly, Bash, Shell, LaTeX, etc.

Machine Learning Frameworks and Cloud Services

TensorFlow, PyTorch, Keras, AWS, GCP, Azure, OCI, etc.

Last updated on February 19, 2024.