Yizhe Zhang Ph.D. Candidate, University of Virginia

yz6me@virginia.edu | +1(434)-987-9638 | LinkedIn: https://www.linkedin.com/in/yzzhn

Website: https://yzzhn.github.io | GitHub: https://github.com/yzzhn | Google Scholar Profile

Education

University of Virginia 01/2019 - Present

Ph.D. Candidate in Computer Engineering

University of Virginia 08/2016 - 12/2018

Master of Science in Computer Engineering

East China Normal University 09/2011 - 06/2015

Bachelor of Science in Physics

Work Experience

Research Intern | *Verisign* 05/2025 – 08/2025

- Evaluated and measured DNS integrations, including on blockchain-based systems.
- Support IETF draft.

Research Experiences

Graduate Research Assistant | *Doctoral Candidate* 01/2019 – Present

Research Focus: Network Security and Privacy, Internet Measurement, and Machine Learning (ML).

Machine Learning and GenAI for Cybersecurity *(Ongoing)*

- Apply Large Language Models (LLMs) for semantic-aware network log analysis via prompt engineering, zero/few-shot learning and fine-tuning.
- Generate synthetic network traffic with LLMs.

Anomaly Detection and Intrusion Detection *(ACSAC '23)*

- Developed a Machine Learning (ML) pipeline to detect malicious network activity in real-world campus network.
- Designed a ranking system to prioritize threats for security analysts.
- Applied time-series, graph, semantic, and historical analysis for feature engineering.
- Leveraged self-training and active learning to handle noisy and imbalanced data.
- Detected 56% more malicious activities than threat intelligence tools during a 10-month real-world deployment.

Large-scale Internet Measurement *(IMC '23, IMC '24, Sigcomm '25, IMC '25)*

- Developed an *open-source* DNS querying pipeline, processing millions of DNS logs daily for 1.5+ years.
- Evaluated DNS HTTPS resource record, Encrypted Client Hello (ECH) deployment and usage.
- Built a *reusable* network log analysis framework adopted by multiple research groups and projects.
- Analyzed security vulnerabilities and privacy risks in TLS, certificates PKI, and IoT systems.

IoT and Wearable Security *(SPW '24)*

- Identified Bluetooth protocol vulnerabilities and privacy risks in wearable devices.

Graduate Research Assistant 06/2017 – 12/2018

Cloud Computing: Applied cloud computing to enhance industrial robotic computation (IRC '18, IRC '19).

Technical Skills

Cybersecurity and Networks:

- Networks (TCP/IP, HTTP/HTTPS, DNS, SSH, SSL/TLS, PKI), BGP, traffic profiling, traffic analysis
- Intrusion detection systems (IDS), threat intelligence, malware detection, botnet detection, beaconing detection, DDoS detection and mitigation, IoT, wearable security

Machine Learning, AI and Data Analysis:

- LLM (prompt engineering, zero/few-shot, fine-tuning)
- Other machine learning or deep learning models (RF, XGBoost, CNN, LSTM, etc.)
- Feature engineering, time-series analysis, graph database, embedding, active-learning, supervised/unsupervised learning, anomaly detection

Programming and Infrastructures:

- Python, PyTorch, Scikit-Learn, Hugging Face, Pandas, Numpy, PySpark, Spark, Neo4j, Jupyter, C#
- Linux, Docker, Git, SLURM, SQL, AWS (EC2, Route 53)
- WireShark, tcpdump, Bind9, Unbound, Zeek (Bro), OpenSSL, Nginx

Research Publications

12. [**Ongoing**] Toward a Comprehensive BGP Community Dictionary Leveraging LLMs.

11. [**IMC '25 Accepted**] Inside Certificate Chains Beyond Public Issuers: Structure and Usage Analysis from a Campus Network.

10. [**Sigcomm '25**] Wirz, François, et al. "Scaling SCIERA: A Journey Through the Deployment of a Next-generation Network." Proceedings of the ACM SIGCOMM 2025 Conference. 2025.

9. [**IMC '24**] Dong, Hongying*, Zhang, Yizhe*, Hyeonmin Lee, Shumon Huque, and Yixin Sun. "Exploring the Ecosystem of DNS HTTPS Resource Records: An End-to-End Perspective." In Proceedings of the 2024 ACM on Internet Measurement Conference, pp. 423-440. 2024. [*Both authors contributed equally to this work.]

8. [**IMC '24**] Dong, Hongying, Yizhe Zhang, Hyeonmin Lee, Kevin Du, Guancheng Tu, and Yixin Sun. "Mutual TLS in Practice: A Deep Dive into Certificate Configurations and Privacy Issues." In Proceedings of the 2024 ACM on Internet Measurement Conference, pp. 214-229. 2024.

7. [**SPW '24**] Liu, Qi, Yizhe Zhang, and Yixin Sun. "Intercepting Bluetooth Traffic from Wearable Health Devices." In 2024 IEEE Security and Privacy Workshops (SPW), pp. 267-273. IEEE, 2024.

6. [**ACSAC '23**] Zhang, Yizhe, Hongying Dong, Alastair Nottingham, Molly Buchanan, Donald E. Brown, and Yixin Sun. "Global Analysis with Aggregation-based Beaconing Detection across Large Campus Networks." In Proceedings of the 39th Annual Computer Security Applications Conference, pp. 565-579. 2023.

5. [**IMC '23**] Dong, Hongying, Hao Shu, Vijay Prakash, Yizhe Zhang, Muhammad Talha Paracha, David Choffnes, Santiago Torres-Arias, Danny Yuxing Huang, and Yixin Sun. "Behind the Scenes: Uncovering TLS and Server Certificate Practice of IoT Device Vendors in the Wild." In Proceedings of the 2023 ACM on Internet Measurement Conference, pp. 457-477. 2023.

4. [**ICCCN '19**] Tan, Yuanlong, Shuoshuo Chen, Steve Emmerson, Yizhe Zhang, and Malathi Veeraraghavan. "Advances in reliable file-stream multicasting over multi-domain software defined networks (SDN)." In 2019 28th International Conference on Computer Communication and Networks (ICCCN), pp. 1-11. IEEE, 2019.

3. [**IRC '19**] Zhang, Yizhe, Lianjun Li, Jorge Nicho, Michael Ripperger, Andrea Fumagalli, and Malathi Veeraraghavan. "Gilbreth 2.0: an industrial cloud robotics pick-and-sort application." In 2019 Third IEEE International Conference on Robotic Computing (IRC), pp. 38-45. IEEE, 2019.

2. [**Int. J. Semantic Comput.**] Li, Lianjun, Yizhe Zhang, Michael Ripperger, Jorge Nicho, Malathi Veeraraghavan, and Andrea Fumagalli."Autonomous object pick-and-sort procedure for industrial robotics application." International Journal of Semantic Computing 13, no. 02 (2019): 161-183.

1. [**IRC '18**] Zhang, Yizhe, Lianjun Li, Michael Ripperger, Jorge Nicho, Malathi Veeraraghavan, and Andrea Fumagalli. "Gilbreth: A conveyor-belt based pick-and-sort industrial robotics application." In 2018 Second IEEE International Conference on Robotic Computing (IRC), pp. 17-24. IEEE, 2018.

Talks

Feb. 2025	Exploring the Deployment and Usage of DNS HTTPS Resource Records *The DNS Operations, Analysis, and Research Center (DNS-OARC) 44*
May. 2024	Intercepting Bluetooth Traffic from Wearable Health Devices *IEEE Security and Privacy Workshops (SPW '24)*
Dec. 2023	Global Analysis with Aggregation-based Beaconing Detection across Large Campus Networks. *Annual Computer Security Applications Conference (ACSAC '23)*
Nov. 2023	Network Data Collection and Anonymization: Balancing Privacy and Fidelity *UVA CS4501 Privacy in the Internet Age (Guest Lecture)*
Feb. 2019	Gilbreth 2.0: an industrial cloud robotics pick-and-sort application *IEEE International Conference on Robotic Computing (IRC '19)*
Jan. 2018	Gilbreth: A conveyor-belt based pick-and-sort industrial robotics application. *IEEE International Conference on Robotic Computing (IRC '18)*