

# Yizhe Zhang

Ph.D. Candidate, University of Virginia

yz6me@virginia.edu | +1(434)-987-9638 | github.com/yzzhn | Google Scholar Profile

## Education

---

<b>University of Virginia</b> Ph.D. Candidate in Computer Engineering	01/2019 - Present
<b>University of Virginia</b> Master of Science in Computer Engineering	08/2016 - 12/2018
<b>East China Normal University</b> Bachelor of Science in Physics	09/2011 - 06/2015

## Research and Work Experiences

---

<b>Graduate Research Assistant</b>   <i>University of Virginia, USA</i> <b>Research focus:</b> network security, machine learning, and internet measurement. <ul style="list-style-type: none"><li>– Developing machine learning methods to address challenges with limited, noisy, and imbalanced data in real-world network environments.</li><li>– Leveraging large language models (LLMs) to tackle practical issues related to network security and privacy.</li><li>– Enhancing network security in large-scale, real-world networks using machine learning, time-series analysis and graph-based techniques (published in ACSAC '23).</li><li>– Conducting comprehensive assessments of network security vulnerabilities and privacy malpractices (published in IMC '23, SPW '24, and forthcoming in IMC '24).</li></ul>	01/2019 – Present
<b>Graduate Research Assistant</b>   <i>University of Virginia, USA</i> <ul style="list-style-type: none"><li>– Research experience: robotics, cloud, network (published in IRC '18, IRC '19).</li></ul>	06/2017 – 12/2018
<b>Software Engineer Intern</b>   <i>Maker Collider, Shanghai, China</i> <ul style="list-style-type: none"><li>– Smart IoT device software development using Arduino.</li></ul>	09/2015 – 12/2015

## Knowledge & Skills

---

### Network and Cybersecurity

*Knowledgeable in:*

- Core concepts of network, network security and privacy, malware, botnets, DNS (Domain Name System), certificate PKI (Public Key Infrastructure), Intrusion Detection System (IDS) and Internet of Things (IoT) security.

*Experienced in:*

- Traffic analysis, monitoring, profiling and fingerprinting.
- Privacy-preserving network traffic anonymization.
- Malware and botnet detection.
- Intrusion and anomaly detection.

### Machine Learning and Data Analysis

*Knowledgeable in:*

- Applying machine learning (ML) and deep learning (DL) models in network security and other applications.
- Leveraging time-series and graph analysis techniques to uncover patterns in network data.

*Experienced in :*

- Developing solutions for real-world imbalanced datasets using self-learning and active learning methodologies.
- Employing large language models (LLMs) for semantic parsing of network logs and time-series forecasting.
- Developing and managing end-to-end large-scale data extraction, transformation, and loading (ETL) processes.
- Conducting large-scale network traffic analysis on billions of connections.

**Programming and Software:** Python (Sklearn, JupyterLab, Pandas, PyTorch, TensorFlow, Numpy, PySpark), Spark, Zeek (Bro), Neo4j, SQL, WireShark, OpenSSL, Git, Linux, SLURM, Docker, C++, AWS.

## Research Publications

---

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 ACM Internet Measurement Conference (IMC), 2024 (forthcoming).

\*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 ACM Internet Measurement Conference (IMC), 2024 (forthcoming).
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

---

### Conferences

- 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)*
- 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)*

### Guest Lecture

- Nov. 2023 Network Data Collection and Anonymization: Balancing Privacy and Fidelity  
*UVA CS4501 Privacy in the Internet Age (Guest Lecture)*