

# DONGFANG ZHAO

✉ zhdongfang@outlook.com ☎ +1 (812)-327-6361 🔗 [linkedin.com/in/dongfang-zhao-483224174](https://www.linkedin.com/in/dongfang-zhao-483224174)

## EDUCATION

<b>Indiana University Bloomington, IN, US</b> Major: System Security and Privacy Minor: Applied Machine Learning <i>PhD in Computer Science</i>	<i>Aug 2018 - 2026</i>
<b>Indiana University Bloomington, IN, US</b> <i>Master of Science in Computer Science</i>	<i>Aug 2018 - Dec 2024</i>
<b>Shandong University, Shandong, China</b> <i>B.Eng. in Computer Science and Technology</i>	<i>Sept 2014 - June 2018</i>

## TEACHING EXPERIENCE

<b>Instructor on Record, Indiana University Bloomington</b> CSCI-C 291 / INFO-E 111 System Programming with C and Unix	<i>Spring 2026 &amp; Spring 2025 &amp; Spring 2024</i>
<b>Instructor on Record, Indiana University Bloomington</b> CSCI-B 430 / INFO-I 430 Security for Networked Systems	<i>Fall 2025</i>
<b>Assistant Instructor, Indiana University Bloomington</b> B430/I430 Security for Networked Systems	<i>Fall 2024 &amp; Fall 2023</i>
<b>Assistant Instructor, Indiana University Bloomington</b> I521/B546 Malware: Threat and Defense	<i>Fall 2021 &amp; Fall 2020</i>
<b>Assistant Instructor, Indiana University Bloomington</b> B547/I533 Systems & Protocol Security & Information Assurance	<i>Spring 2021 &amp; Spring 2020</i>

## SKILLS

- Programming and development: Python, PHP/HACK, MySQL, C/C++, Java, JavaScript, HTML, CSS, Node.js, Apache, flutter, AWS, Perl
- Platforms/Tools: Linux, Git, Docker, Wireshark
- Machine Learning: PyTorch, Keras, Scikit-Learn, Natural Language Processing(NLP)
- Specializations: Security Assessment, Data Privacy, Artificial Intelligence, Software Engineering, Web Analysis, Internet of Things (IoT)

## WORK EXPERIENCE

<b>Fullstack Software Engineer Intern — M·CAM International LLC (Remote)</b> Maintained and improved DOORS™ (web-based IP analysis) across frontend/backed; focused on robustness and security. <ul style="list-style-type: none"><li>• Stabilized PostgreSQL XML ingestion pipeline (parser fixes, correctness validation, AWS Batch/manual run workflow).</li><li>• Eliminated recurring functioning errors and improved throughput via profiling, indexing, and concurrency tuning.</li><li>• Built CI/CD-backed test coverage, Dockerized dev environment, verification scripts, and maintainer-facing documentation.</li></ul>	<i>May–Jul 2025</i>
<b>Meta (Facebook) — Software Engineer PhD Intern (Infrastructure), Menlo Park, CA</b> Develop Platform-level Filtering Funnel for integrity <ul style="list-style-type: none"><li>• Developed a high-performance filtering funnel capable of handling million-level QPS(~2.4M queries per second at peak) to optimize traffic flow and reduce load on downstream resource-intensive models, achieving significant savings in resource costs.</li><li>• The system efficiently fetches lightweight model results and features from the featureStore, applying custom thresholds</li></ul>	<i>June 2022 - Aug 2022</i>

and user-defined strategies for refined traffic filtering, complemented by comprehensive logging mechanisms for effective monitoring and debugging post-unit testing.

PUBLICATIONS

\* denotes a co-primary authorship

**Alexa, is the skill always safe? Uncover Lenient Skill Vetting Process and Protect User Privacy at Run Time**  
*Dongfang Zhao\**, Tu Le\*, Zihao Wang, Xiaofeng Wang, Yuan Tian  
*The 46th International Conference on Software Engineering (ICSE 2024)*  
Voice Assistant(Alexa) NLP Reverse Engineering

**Who’s In Control? On Security Risks of Disjointed IoT Device Management Channels**  
Y. Jia, B. Yan, L. Xing, *D. Zhao*, X. Wang, Y. Zhang, Y. Liu, K. Zheng, Y. Zhang, D. Zou, H. Jin.  
*The ACM Conference on Computer and Communications Security (CCS), 2021*  
Access Control IoT

**Shattered Chain of Trust: Understanding Security Risks in Cross-Cloud IoT Access Delegation.**  
Bin Yuan\*, Yan Jia\*, Luyi Xing, *Dongfang Zhao*, Xiaofeng Wang, Deqing Zou, Hai Jin, Yuqing Zhang.  
*The 28th USENIX Security Symposium, 2020.*  
Identity and Access Management(IAM) Access Delegation IoT

**Burglars’ IoT Paradise: Understanding and Mitigating Security Risks of General Messaging Protocols on IoT Clouds**  
Yan Jia, Luyi Xing, Yuhang Mao, *Dongfang Zhao*, Xiaofeng Wang, Shangru Zhao, Yuqing Zhang.  
*The 41st IEEE Symposium on Security and Privacy (Oakland), 2020*  
Messaging Protocol Analysis IoT Oauth MQTT

RESEARCH IN PROGRESS

**DocuScope: Documentation-Driven Protocol Security Analysis via Loose-End Mining and Agentic LLMs**  
*Dongfang Zhao*, Wenxuan Fu, Yan Jia, Tianhao Mao, Xiaofeng Wang, Hang Zhang  
*Targeting CCS, 2026.*  
LLM RAG Protocol Analysis AI Agent

**Shining Light into the Tunnel: Understanding and Detecting Network Traffic of Residential Proxies**  
Ronghong Huang, *Dongfang Zhao*, , Xianghang Mi, Xiaofeng Wang  
*Arxiv 2024*  
Residential Proxy Machine Learning Network Analysis

HONORS & AWARDS

Indiana University Bloomington-Luddy PhD instructor award	2025
Acknowledgments for proxy network suspicious traffic analysis discoveries from different proxy providers (IPRoyal, Packetstream)	2023
Briefing on Black hat Asia	2021
Security research reported by DARKReading	2021
Apple Homekit design vulnerability: CVE-2020-9978. - Vulnerability acknowledgments on macOS and iOS	2020
Bounty for the vulnerabilities in IoT cloud delegation process - We received acknowledgments from Samsung SmartThings (\$2000 bounty), Philips Hue.	2019
Other acknowledgments for vulnerability discoveries from different platforms - The Microsoft Security Response Center(MSRC) Online Acknowledgement.(October 2019) - The vulnerabilities and design flaws found in IoT platforms and MQTT received the acknowledgments from AWS, IBM, Eclipse Mosquitto, Tuya Smart, Suning, etc.	2019