Adrian (Shuai) Li

305 N University S, West Lafayette, IN 47907

765-775-3121 li3944@purdue.edu linkedin.com/in/adrian-shuai-li-616487107 homepage

Education

Purdue University **Expected Graduation Date: Dec 2025**
Ph.D. in Computer Science, Advisor: Elisa Bertino, GPA: 4.0/4.0 West Lafayette, IN

University of Calgary **January 2020**
M.Sc. in Computer Science, Advisor: Rei Safavi-Naini, GPA: 4.0/4.0 Calgary, Canada
Master Thesis: A Capability-based System to Enforce Context-aware Permission Sequences

Wuhan University **July 2017**
BSc. in Computer Science, GPA: 3.7/4.0 Wuhan, China

Experience

Purdue University **May 2021 – Present**
Graduate Research Assistant West Lafayette, IN

- Developed a framework using Large Language Models (LLMs) to efficiently generate functionality-preserving malware variants that bypass ML-based detection models, requiring only malware binaries and minimal human intervention - this work is funded by Cisco
- Proposed a novel cross-domain transfer learning approach for highly accurate image classification with no labeled samples from the target domain - this work is in collaboration with IBM TJ Watson Research Center (paper link)

Cisco Research **May 2023 – August 2023**
Research Intern III San Jose, CA

- Developed an automated solution for extracting control flow graphs (CFGs) from complex software binaries and implemented a pipeline to generate high-quality instruction embeddings, introducing a novel approach to improve software analysis
- Proposed a new model to mitigate data drift in malware samples by integrating graph neural networks (GNNs) and domain adaptation on control flow graphs (CFGs), resulting in twice the accuracy of state-of-the-art methods. (paper link)

Aviatrix Systems **May 2022 – August 2022**
Software Developer Intern Champaign, IL

- Implemented a pipeline that can efficiently extract, transform, and load large-scale network performance data from Elasticsearch indices as Spark data frames for ML analytics
- Created realistic network anomaly training data by replaying malicious network traces across AWS VPCs and extracting features from the traffic
- Developed a highly accurate prediction system based on Spark MLlib using different ML models for network intrusion detection

TELUS Communications **March 2020 – September 2020**
Security Research Intern Calgary, Canada

- Implemented context-aware token-based authentication in Ansible tower
- Contributed python codes to Ansible Tower's open-source project (AWX)

University of Calgary **September 2017 – January 2020**
Graduate Research Assistant Calgary, Canada

- Developed a distributed token-based authorization system that provides efficient and refined (conditional) access to data with security guarantee (paper link)
- Designed cryptographic authentication and OAuth 2.0 based authorization for a home hub that continues to provide essential services in a cloud-based smart home when the cloud is unavailable (paper link)

Publications

All publications are available on my website: https://gloryer.github.io/.

Preprints Under Review

[P1] **Li, A. S.**, Iyengar, A., Kundu, A. and Bertino, E., (2024). Improving Malware Detection with Adversarial Domain Adaptation and Control Flow Graphs. URL https://arxiv.org/abs/2407.13918. Under major revision for NDSS 2025, currently under review

[P2] **Li, A. S.**, Bertino, E., Dang, X. H., Singla, A., Tu, Y., & Wegman, M. N. (2024). Maximal Domain Independent Representations Improve Transfer Learning. URL https://arxiv.org/abs/2306.00262. Under review for TMLR

Peer-Reviewed Journal Articles

[J1] Bhardwaj, S., **Li, A. S.**, Dave, M., & Bertino, E. (2024). Overcoming the lack of labeled data: Training malware detection models using adversarial domain adaptation. Computers & Security. doi: 10.1016/j.cose.2024.103769

Peer-Reviewed Conference Papers

[C1] **Li, A. S.**, Bertino, E., Wu, R. T., & Wu, T. Y. (2023). Building Manufacturing Deep Learning Models with Minimal and Imbalanced Training Data Using Domain Adaptation and Data Augmentation. In 2023 IEEE International Conference on Industrial Technology (ICIT). doi:10.1109/ICIT58465.2023.10143099

[C2] **Li, A. S.**, Safavi-Naini, R., & Fong, P. W. (2022). A Capability-based Distributed Authorization System to Enforce Context-aware Permission Sequences. In Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies (SACMAT). doi:10.1145/3532105.3535014

[C3] Avizheh, S., Safavi-Naini, R., & **Li, S.** (2020). Secure Logging with Security Against Adaptive Crash Attack. In Foundations and Practice of Security: 12th International Symposium (FPS 2019). Springer International Publishing. doi: 10.1007/978-3-030-45371-8_9

[C4] Doan, T. T., Safavi-Naini, R., **Li, S.**, Avizheh, S., K, M. V., & Fong, P. W. (2018). Towards a resilient smart home. In Proceedings of the ACM SIGCOMM 2018 Workshop on IoT Security and Privacy (IoT S&P). doi: 10.1145/3229565.3229570

Books

[B1] Bertino, E., Bhardwaj, S., Cicala, F., Gong, S., Karim, I., Katsis, C., Lee, H., **Li, A.S.** and Mahgoub, A.Y., (2023). Machine Learning Techniques for Cybersecurity. Springer Nature. doi: 10.1007/978-3-031-28259-1

Theses

[T1] **Li, S.** (2020). A Capability-based System to Enforce Context-aware Permission Sequence. Master's thesis, University of Calgary, Calgary, Canada

Awards and Hornors

Academic and Research Standing Excellence 2024 — Purdue University Computer Science Department
[C4]. Best paper award — IoT S&P 2018
Mitacs Globalink Graduate Fellowship — Mitacs
Academic Excellence Scholarship — Wuhan University

Invited talks

Cisco Open Mic Talks — **November 2023**
Virtual

- Title: Domain Adaptation for Malware Classification Using Graph Neural Networks: Learning Semantic and Structural Features of Control Flow Graphs

Professional service

Reviewer

- WIREs Data Mining and Knowledge Discovery
- IEEE International Conference on Data Engineering (ICDE), 2024
- IEEE Global Communications Conference (Globecom), 2024
- European Symposium on Research in Computer Security (ESORICS), 2024
- Annual Computer Security Applications Conference (ACSAC), 2023, 2024
- The ACM Symposium on Access Control Models and Technologies (SACMAT), 2022, 2024
- ACM Conference on Data and Application Security and Privacy (CODASPY), 2022, 2024

Teaching

Purdue University **Spring 2023 and 2024**
Guest Lecturer: CS 59000-DSP Data Security And Privacy West Lafayette, IN

Purdue University **Spring 2021**
Graduate Teaching Assistant for CS 182 West Lafayette, IN

Other Service

University of Calgary Computer Science Graduate Society **June 2018 – May 2019**
Vice President Calgary, Canada

Security Researchers and Industry Experts Talks **September 2018**
Program Committee Calgary, Canada

The 25th Conference on Selected Areas in Cryptography **August 2018**
Student Volunteer Calgary, Canada

Technical Skills

Programming: Python, SQL, Node.js
Cloud & Networking: AWS EC2/S3/security groups, Azure, GCP, Wireshark, MININET, ONOS, OpenSSL, dnSpy, tcpreplay
ML & Data Science: Spark, MLlib, Pandas, NumPy, Tensorflow, Scikit-learn, Keras, Elasticsearch, MongoDB
General: Django, Git, Docker, Ansible, Apache JMeter, Postman

Certificate

Aviatrix Systems **May 2022**
Multi-Cloud Network Professional