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 **2021 - Present**
Ph.D. in Computer Science, Advisor: Elisa Bertino, GPA: 4.0/4.0 West Lafayette, IN

University of Calgary **Jan. 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 **Jul. 2017**
BSc. in Computer Science, GPA: 3.7/4.0 Wuhan, China

Academic Experience

Purdue University **May 2021 – Present**
Graduate Research Assistant, Advisor: Elisa Bertino West Lafayette, IN
- Topic: Transfer learning for security; feature decomposition in domain adaptation

University of Calgary **Sep. 2017 – Jan. 2020**
Graduate Research Assistant, Advisor: Rei Safavi-Naini Calgary, Canada
- Topic: Context-aware distributed authorization

Industry Experience

IBM Research **May 2021 – Present**
Collaborative Researcher, Collaborators: Mark Wegman, Yuhai Tu Yorktown Heights, NY
- Topic: Feature decomposition in domain adaptation

Cisco Research **May 2023 – Aug. 2023**
Research Intern III, Hosts: Ashish Kundu, Arun Iyengar San Jose, CA
- Topic: Graph-based model for malware detection

Aviatrix Systems **May 2022 – Aug. 2022**
Software Developer Intern, Hosts: Susan Hinrichs, Joshua Juen Champaign, IL
- Topic: Machine learning methods for network intrusion detection

TELUS Communications **Mar. 2020 – Sep. 2020**
Security Research Intern, Host: Marc Kneppers Calgary, Canada
- Topic: Context-aware token-based authentication in Ansible Tower

Publications

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

Preprints Under Review

[P1] **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

[P2] **Li, A. S.**, Iyengar, A., Kundu, A., & Bertino, E. (2024). Transfer Learning for Security: Challenges and Future Directions. URL https://arxiv.org/abs/2403.00935

Peer-Reviewed Journal Articles

[J1] **[Computers & Security]** 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] **[NDSS'25] Li, A. S.**, Iyengar, A., Kundu, A. and Bertino, E., (2024). Revisiting Concept Drift in Windows Malware Detection: Adaptation to Real Drifted Malware with Minimal Samples. Network and Distributed System Security Symposium 2025. doi:10.14722/ndss.2025.240830

[C2] **[INDIN'24]** Imtiaz Mostafiz, M., Kim, E., **Li, A. S.**, Bertino, E., Jun, M. B. G., & Shakouri, A. (2024). Adversarial Domain Adaptation for Metal Cutting Sound Detection: Leveraging Abundant Lab Data for Scarce Industry Data. In 2024 IEEE International Conference on Industrial Informatics. doi:10.1109/INDIN58382.2024.10774310

[C3] **[ICIT'23] 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. doi:10.1109/ICIT58465.2023.10143099

[C4] **[SACMAT'22] 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. doi:10.1145/3532105.3535014

[C5] **[FPS 2019]** 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. Springer International Publishing. doi: 10.1007/978-3-030-45371-8_9

[C6] **[IoT S & P]**[**Best paper award**] 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. doi: 10.1145/3229565.3229570

Book

[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

Patent

[U1] Wegman, M., Tu, Y., Dang, X. H., Singla, A., **Li, A.S.** (2024). Autoencoder with Generative Adversarial Networks for Transfer Learning Between Domains. U.S. Patent Application No. 18/129,540

Thesis

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

Awards and Honors

Internet Society NDSS Fellowship — Internet Society
Academic and Research Achievement Recognition — Purdue University Computer Science Department
[C6]. Best paper award — IoT S&P 2018
Mitacs Globalink Graduate Fellowship — Mitacs
Academic Excellence Scholarship — Wuhan University

Research Mentoring

Md Ajwad Akil (PhD), Purdue CS

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 — **Jun. 2018 – May 2019**
Vice President — Calgary, Canada
Security Researchers and Industry Experts Talks — **Sep. 2018**
Program Committee — Calgary, Canada
The 25th Conference on Selected Areas in Cryptography — **Aug. 2018**
Student Volunteer — Calgary, Canada

Invited Talks

Cisco Open Mic Talks — **Nov. 2023**
Domain Adaptation for Malware Classification Using Control Flow Graphs — Virtual

Certificate

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