

---

## Research Interest

My research interest intersects Adversarial Machine Learning, Graph Learning and Software Security.

---

## Education

- Sep 2017-Mar 2022 **Pennsylvania State University**, *United States*,  
*College of Information Sciences and Technology*,  
Ph.D. degree advised by Dr. Dinghao Wu.
- Feb 2019-Jul 2019 **Ecole Polytechnique Fédérale de Lausanne (EPFL)**, *Switzerland*,  
*School of Computer and Communication Sciences*,  
Visiting PhD student at [Very Large Scale Computing Lab](#).
- Sep 2016-Feb 2017 **University of Strathclyde**, *United Kingdom*,  
*Department of Computer Science*,  
Visiting student advised by Dr. John Levine.
- Sep 2013-Jul 2017 **B.E. University of Electronic Science & Technology of China**,  
*Dept. of Computer Science and Technology, major in Information Security*,  
Advised by Dr. Hong Qu. Thesis: Robustness Improvement on Spiking Neural Network,  
GPA: 3.88/4.0.

---

## Work Experience

- Mar 2022-Present **Visa Research**, *Staff Research Scientist*.
- May 2021-Aug 2021 **Visa Research**, *Research Intern*, Active Graph Learning.  
Exploring a more sophisticated method to incorporate active learning to graphs so as to solve the data shortage challenge.
- May 2020-Aug 2020 **ByteDance Inc**, *Research Intern*, Statically Analyzing critical C++ projects.  
Investigating a couple of static analysis tools including CppCheck, Flawfinder, etc., on C++ projects. We use **Clang Static Analyzer** to adapt to company's unique compile framework and develop customized checkers to meet specific detection requirements and to reduce false positives in code testing.

---

## Publication

- RecSys 2022 Huiyuan Chen, **Xiaoting Li**, Kaixiong Zhou, Xia Hu, Chin-Chia Michael Yeh, Yan Zheng, Hao Yang, TinyKG: Memory-Efficient Training Framework for Knowledge Graph Neural Recommender Systems. *In Proceedings of 16th ACM Conference on Recommender Systems*.
- RecSys 2022 Huiyuan Chen, Yusan Lin, Menghai Pan, Lan Wang, Chin-Chia Michael Yeh, **Xiaoting Li**, Yan Zheng, Fei Wang, Hao Yang, Denoising Self-Attentive Sequential Recommendation. *In Proceedings of 16th ACM Conference on Recommender Systems*.
- SecureComm 2022 **Xiaoting Li**, Lingwei Chen, Dinghao Wu, Adversary for Social Good: Leveraging Attribute-Obfuscating Attack to Protect User Privacy on Social Networks. *In Proceedings of 18th EAI International Conference on Security and Privacy in Communication Networks*.
- ICICS 2022 **Xiaoting Li**, Xiao Liu, Lingwei Chen, Rupesh Prajapati, Dinghao Wu, FuzzBoost: Reinforcement Compiler Fuzzing. *In Proceedings of 24th International Conference on Information and Communications Security*.
- SIGIR 2022 Quan Li, **Xiaoting Li**, Lingwei Chen, Dinghao Wu, Distilling Knowledge on Text Graph for Social Media Attribute Inference. *In Proceedings of International ACM SIGIR Conference on Research and Development in Information Retrieval*.
- SDM 2022 Lingwei Chen, **Xiaoting Li**, Dinghao Wu, Adversarially Reprogramming Pretrained Neural Networks for Data-limited and Cost-efficient Malware Detection. *In Proceedings of SIAM International Conference on Data Mining*.

|                |  |
|----------------|--|
| IAAI 2022      | <b>Xiaoting Li</b> , Xiao Liu, Lingwei Chen, Rupesh Prajapati, Dinghao Wu, AlphaProg: Reinforcement Generation of Valid Programs for Compiler Fuzzing. <i>In Proceedings of 34th Annual Conference on Innovative Applications of Artificial Intelligence</i> .         |
| IJCNN 2021     | <b>Xiaoting Li</b> , Lingwei Chen, Jinquan Zhang, James Larus, Dinghao Wu, Watermarking-based Defense against Adversarial Attacks on Deep Neural Networks. <i>In Proceedings of International Joint Conference on Neural Networks</i> .                                |
| ICSE 2021      | Qinkun Bao, Zihao Wang, <b>Xiaoting Li</b> , James Larus, Dinghao Wu, Abacus: Precise Side-Channel Analysis. <i>In Proceedings of 43rd International Conference on Software Engineering</i> .  |
| SDM 2020       | <b>Xiaoting Li</b> , Lingwei Chen, Dinghao Wu, Turning Attacks into Protection: Social Media Privacy Protection Using Adversarial Attacks. <i>In Proceedings of SIAM International Conference on Data Mining</i> .   |
| ECML-PKDD 2020 | Lingwei Chen, <b>Xiaoting Li</b> , Dinghao Wu, Enhancing Robustness of Graph Convolutional Networks via Dropping Graph Connections. <i>In Proceedings of European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases</i> . |
| AAAI 2019      | Xiao Liu, <b>Xiaoting Li</b> , Rupesh Prajapati, Dinghao Wu, DeepFuzz: Automatic Generation of Syntactically Correct C Programs for Fuzz Testing. <i>In Proceedings of 33th AAAI Conference on Artificial Intelligence</i> .   |

---

## Other Experience

|                |  |
|----------------|--|
| ICDM 2022      | Conference PC member.  |
| ECML-PKDD 2022 | Conference PC member.  |
| ECML-PKDD 2021 | Conference PC member.  |
| KDD 2021       | Conference external reviewer.  |
| ICDM 2021      | Conference external reviewer.  |
| ICSE 2021      | Conference external reviewer.  |
| ECML-PKDD 2020 | Conference PC member.  |
| CCS 2019       | Conference external reviewer.  |
| Spring 2020    | Teaching Assistant, IST336: <i>Cyber Security in Windows Malware analysis</i> , Penn State University. |
| Fall 2018      | Teaching Assistant, IST140: <i>Application Development in Java</i> , Penn State University.            |

---

## Selected Honors and Awards

|           |   |
|-----------|---|
| Feb 2022  | AAAI Conference Student Travel Grant Award.                           |
| Jul 2021  | Grace Hopper Conference (GHC) Scholarship.                            |
| Apr 2020  | Women in Cyber Security (WiCyS) Scholarship.                          |
| Jan 2019  | AAAI Conference Student Travel Grant Award.                           |
| Apr 2018  | Women in Cyber Security (WiCyS) Scholarship.                          |
| Sept 2016 | National Scholarship for Outstanding Undergraduates.                  |
| Apr 2016  | Honorable Mention in 2016 Mathematical Contest in Modeling.           |
| Sept 2015 | Provincial Second Prize in National Mathematical Contest in Modeling. |
| May 2015  | Award of Excellence in National Mathematical Modeling Contest.        |

---

## Computer Skills

|                   |   |
|-------------------|---|
| Language          | Python, Scala, Java, Shell, C, R, Matlab, SML |
| Substantial skill | Keras, Tensorflow, Vim, Linux                 |