YINGQI LIU

(+1) 765-337-3460 ⋄ liu1751@purdue.edu ⋄ naiyeleo@outlook.com
https://www.cs.purdue.edu/homes/liu1751/
https://scholar.google.com/citations?user=gOPVK2UAAAAJ&hl=en

EDUCATIION

Purdue University *Aug 2015 - Dec 2022 (Expected)*
Ph.D. Department of Computer Science Overall GPA: 3.9/4

China University of Mining and Technology *Sep 2011 - Jun 2015*
B.S. Department of Computer Science and Engineering Overall GPA: 93/100

Iowa State University *Jan 2014 - May 2014*
Exchange Student Department of Computer Science Overall GPA: 4/4

EXPERIENCE

Research Intern, JD.com USA *May 2019 - Aug 2019*
Working on research projects on trojaning attacks and defense on Recurrent Neural Networks.

Research Assistant, Purdue University *Jan 2017 - Present*
Working on research projects of adversarial machine learning, defense against backdoor/trojan attacks on NN and other AI related tasks.

Teaching Assistant, Purdue University *Aug 2015 - Dec 2016*
Leading labs and PSO, grading homeworks and projects and helping designing projects for CS18000 Problem Solving and Object-Oriented Programming and CS35200 Compilers: Principles and Practice.

RESEARCH PROJECTS

Trojaning defense on TrojAI Competition (Python, Pytorch) Jan 2020 - Present

- Participate in TrojAI competition (https://pages.nist.gov/trojai/).
- Propose several new trojan/backdoor detection methods for deep neural networks in computer vision tasks and natural language processing tasks.
- **Our team ranks the first in round 1 to 4 and round 6 to 9 out of all 9 rounds leaderboard.** Previous leaderboards can be found at https://pages.nist.gov/trojai/docs/results.html#previous-leaderboards

Trojaning attack and defense on Recurrent Neural Networks (RNN) (Python, Tensorflow) May 2019 - Aug 2019

- Propose new trojaning attacks on RNN based text classification models and Seq2Seq machine translations systems.
- Design a new neuron detection methods on RNN.
- Implement a novel detection system that detect trojaning attacks on RNN by inspecting inner neurons.

Detection trojaning attacks of Neural Networks (Python, Tensorflow,) Jan 2019 - May 2019

- Develop a detection system that can detect neural network backdoors with high confidence.
- Design a new sampling technique to scan the inner neurons of the neural network.
- Propose new feature space trojaning attack which cannot be detected by previous detection methods.
- The new detection system outperforms previous detection systems significantly especially on feature space trojaning attacks.

· Github Repo https://github.com/naiyeleo/ABS

Trojaning attacks on Neural Networks (Python, Theano, Caffe) Nov 2016 - Aug 2017

· Develop a system to generate trojan attacks for Neural Networks which can insert trojan into a benign model and generate triggers that trigger the trojan behavior in trojaned Neural Networks.
· Design a scheme to generate trojan triggers and a a scheme to reverse engineering the training data that are used for trojaning the model.
· The trojaning system can successfully trojan Neural Networks in Face Recognition, Speech Recognition, Age Recognition, Sentiment Analysis and Autonomous Driving system.
· Github repo https://github.com/PurduePAML/TrojanNN

White box multi-process program tuning framework (C, C++) Sept 2015 - Nov 2016

· Help build a system that instrument target program using LLVM and fork, schedule and collect the program hundreds of times to tune the parameters.
· The tuning system can tune a large drone software to obtain the optimal parameter for different tasks.

TECHNICAL STRENGTHS

Computer Languages	Python, Java, C/C++, MATLAB
Software & Tools	Pytorch, Tensorflow, Theano, Caffe, Latex, UNIX/Linux

RELEVANT COURSES

Machine Learning
Data Mining
Algorithm Design, Analysis, And Implementation
Operating System
Software Engineering and Program Analysis
Information Security
Compiling And Programming Systems
Principles of Programming Languages

PROFESSIONAL ACTIVITIES

Reviewing activities
Conference on Computer Vision and Pattern Recognition (CVPR 2022)
European Conference on Computer Vision (ECCV 2022)
International Journal of Computer Vision
IEEE Transactions on Information Forensics and Security
IEEE Transactions on Secure and Dependable Computing
IEEE Transactions on Evolutionary Computation
Concurrency and Computation: Practice and Experience
The Conference on Web Information Systems and Applications (WISA) 2018

SELECTED PUBLICATIONS

PICCOLO: Exposing Complex Backdoors in NLP Transformer Models

· **Yingqi Liu***, Guangyu Shen*, Guanhong Tao, Shengwei An, Shiqing Ma, Xiangyu Zhang
· Proceedings of the 43rd IEEE Symposiums on Security and Privacy **(S&P 2022)**

Complex Backdoor Detection by Symmetric Feature Differencing

· **Yingqi Liu***, Guangyu Shen*, Guanhong Tao, Zhenting Wang, Shiqing Ma, Xiangyu Zhang
· IEEE/CVF Conference on Computer Vision and Pattern Recognition 2022 **(CVPR 2022)**

ABS: Scanning Neural Networks for Back-doors by Artificial Brain Stimulation

· **Yingqi Liu**, Wen-Chuan Lee, Guanhong Tao, Shiqing Ma, Yousra Aafer, Xiangyu Zhang

· Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security **(CCS 2019)**

Trojaning Attack on Neural Networks

· **Yingqi Liu**, Shiqing Ma, Yousra Aafer, Wen-Chuan Lee, Juan Zhai, Weihang Wang, Xiangyu Zhang
· Proceedings of the 25th Network and Distributed System Security Symposium **(NDSS 2018)**

Constrained Optimization with Dynamic Bound-scaling for Effective NLP Backdoor Defense

· Guangyu Shen*, **Yingqi Liu***, Guanhong Tao, Qiuling Xu, Zhuo Zhang, Shengwei An, Shiqing Ma, Xiangyu Zhang
· Proceedings of Thirty-ninth International Conference on Machine Learning (ICML 2022)

Backdoor Scanning for Deep Neural Networks through K-Arm Optimization

· Guangyu Shen*, **Yingqi Liu***, Guanhong Tao, Shengwei An, Qiuling Xu, Siyuan Cheng, Shiqing Ma, Xiangyu Zhang
· **Proceedings of the 38th International Conference on Machine Learning (ICML 2021)**

Model Orthogonalization: Class Distance Hardening in Neural Networks for Better Security

· Guanhong Tao, **Yingqi Liu**, Guangyu Shen, Qiuling Xu, Shengwei An, Zhuo Zhang, Xiangyu Zhang
· Proceedings of the 43rd IEEE Symposiums on Security and Privacy **(S&P 2022)**

Better Trigger Inversion Optimization in Backdoor Scanning

· Guanhong Tao, Guangyu Shen, **Yingqi Liu**, Shengwei An, Qiuling Xu, Shiqing Ma, Pan Li, Xiangyu Zhang
· IEEE/CVF Conference on Computer Vision and Pattern Recognition 2022 **(CVPR 2022)**

Deep Feature Space Trojan Attack of Neural Networks by Controlled Detoxification

· Siyuan Cheng, **Yingqi Liu**, Shiqing Ma, Xiangyu Zhang
· Thirty-Fifth AAAI Conference on Artificial Intelligence **(AAAI 2021)**

NIC: Detecting Adversarial Samples with Neural Network Invariant Checking

· Shiqing Ma, **Yingqi Liu**, Guanhong Tao, Wen-Chuan Lee, Xiangyu Zhang
· Proceedings of the 26th Network and Distributed System Security Symposium **(NDSS 2019)**

Composite Backdoor Attack for Deep Neural Network by Mixing Existing Benign Features

· Junyu Lin, Lei Xu, **Yingqi Liu**, Xiangyu Zhang
· Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security **(CCS 2020)**

TRADER: trace divergence analysis and embedding regulation for debugging recurrent neural networks

· Guanhong Tao, Shiqing Ma, **Yingqi Liu**, Qiuling Xu, Xiangyu Zhang
· Proceedings of 2020 IEEE/ACM 42nd International Conference on Software Engineering **(ICSE 2020)**

MODE: Automated Neural Network Model Debugging via State Differential Analysis and Input Selection

· Shiqing Ma, **Yingqi Liu**, Wen-Chuan Lee, Xiangyu Zhang, Ananth Grama
· Proceedings of the ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engneering **(ESEC/FSE 2018)**

White-box Program Tuning

· Wen-Chuan Lee, **Yingqi Liu**, Peng Liu, Shiqing Ma, Hongjun Choi, Xiangyu Zhang, Rajiv Gupta
· Proceedings of the 2019 IEEE/ACM International Symposium on Code Generation and Optimization **(CGO 2019)**

Attacks Meet Interpretability: Attribute-steered Detection of Adversarial Samples

· Guanhong Tao, Shiqing Ma, **Yingqi Liu**, Xiangyu Zhang
· Proceedings of Neural Information Processing Systems 2018 **(NIPS 2018 Spotlight)**

Programming support for autonomizing software

· Wen-Chuan Lee, Peng Liu, **Yingqi Liu**, Shiqing Ma, Xiangyu Zhang
· Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation **(PLDI 2019)**

LAMP: data provenance for graph based machine learning algorithms through derivative computation

· Shiqing Ma, Yousra Aafer, Zhaogui Xu, Wen-Chuan Lee, Juan Zhai, **Yingqi Liu**, Xiangyu Zhang
· Proceedings of the ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engneering **(ESEC/FSE 2017)**

An Approach for Fault Localization Based on Program Slicing and Bayesian

· **Yingqi Liu**, Wei Li, Shujuan Jiang, Yanmei Zhang, Xiaolin Ju
· 2013 13th International Conference on Quality Software **(QSIC 2013)**

PAD: programming third-party web advertisement censorship

· Weihang Wang, Yonghwi Kwon, Yunhui Zheng, Yousra Aafer, I Luk Kim, Wen-Chuan Lee, **Yingqi Liu**, Weijie Meng, Xiangyu Zhang, Patrick Eugster
· Proceedings of the 32nd IEEE/ACM International Conference on Automated Software Engineering **(ASE 2017)**