LU YAN

Email: yan390@purdue.edu Tel: +86 18217262991 Website: https://lunaryan.github.io/

EDUCATION

Shanghai Jiao Tong University Shanghai, China
Undergraduate in Department of Computer Science and Engineering September 2016 – Present

- Major GPA: 3.75/4.3 Overall GPA: 3.51/4.3
- Zhiyuan Honors Program of Engineering

RESEARCH EXPERIENCES

Neural Networks Guided Fuzzing Framework Jul. 2019 – Sept. 2019
Advisor: Prof. Suman Jana Columbia University

- We designed a generic ML framework that can learn from different types of program- and input-specific information (e.g., branch distance, rare-edges) using a simple neural network, and further use a gradient-guided optimization technique to find optimal parameter values in an information-source-agnostic way.
- Measured and compared the branch distance variation during the fuzzing process of American Fuzzy Loop (AFL) and our framework, providing compelling evidence in support of our method
- Assessed the reasons behind the outstanding performance of our method by ablation study of the benefits offered by seed selection and adaptive loss (two heuristics we proposed)

Fuzzing Seeds Generation by AI Mar. 2020 – May. 2020
Mentor: Huixin Ma Tencent Keen Lab

- Proposed generating effective PNG inputs using Seq2Seq and SeqGAN with real-time feedback of program execution to increase code coverage when fuzzing libpng
- Examined the effect of generated inputs by comparing fuzzing results against random inputs and analyzing source code coverage using LLVM
- Combined Continuous Integration (CI) through fuzzing process to start runs and report results automatically

Android Apps' Privacy Leakage Risk Evaluation Dec. 2018 – Jul. 2019
Advisor: Prof. Haojin Zhu Shanghai Jiao Tong University

- Proposed benign Apps with similar functions utilize common limited permission combinations while malwares tend to require more permissions independent of their functions, evaluated it by finding frequent term sets
- Established correspondence between Apps' requested permissions and private information listed in their privacy policies, based on which introduced a new metric to evaluate privacy leakage risk of Android Apps

Dynamic Traffic Feature Camouflaging via GANs Jun. 2018 – Jul. 2018
Advisor: Prof. Haojin Zhu Shanghai Jiao Tong University

- We proposed a dynamic traffic camouflaging technique that automatically learns the features of the normal network flow, and dynamically morphs the on-going traffic flows based on the learned features by the adoption of the Generative Adversarial Networks (GAN) model
- Analyzed network flows using dpkt framework and identified each flow with 4-tuple (source address, source port, destination address, destination port)
- Transformed traffic data into normalized feature vectors; compared the effect of different generator and discriminator network structure on training result

PUBLICATION

- Dongdong She, Rahul Krishna, **Lu Yan**, Suman Jana, Baishakhi Ray, "MTFuzz: Fuzzing with a Multi-Task Neural Network". In ESEC/FSE 2020. (to appear)
- Jie Li, Lu Zhou, Huaxin Li, **Lu Yan** and Haojin Zhu "Dynamic Traffic Feature Camouflaging via Generative Adversarial Networks", in IEEE Conference on Communications and Network Security (CNS'19)

HONORS & SCHOLARSHIPS

- Hongyi Scholarship, Shanghai Jiao Tong University (Only 10 students at SJTU were awarded in 2020)
- Overseas Research Scholarship, Shanghai Jiao Tong University
- Zhiyuan Honors Scholarship, Shanghai Jiao Tong University (top **5%**)
- Zhiyuan Honors Research Program, Shanghai Jiao Tong University (The **only** EECS project out of 8 projects funded in 2018)

ADDITIONAL INFORMATION

- **Volunteer Experience**: International Volunteer teacher in Cambodia (2017) and Indonesia (2018)
- **Hobbies**: Traditional Chinese folk dance, Calligraphy