Limin Yang

liminy2@illinois.edu +1 (540)998-9158 https://liminyang.web.illinois.edu/ GitHub: whyisyoung

Education

University of Illinois Urbana-Champaign, Ph.D. in Computer Science, Advisor: Gang Wang *Aug.2019 – May 2024*

Virginia Tech, Ph.D. in Computer Science, Advisor: Gang Wang *Aug.2018 – Aug.2019*

East China Normal University, Masters Study in Computer Science *Sep.2015 – Jun.2018*

East China Normal University, B.E. in Computer Science *Sep.2011 – Jun.2015*

Research Interests

Machine learning security, measurement, and explainable AI.

Conference Proceedings

[USENIX Security'21] Limin Yang, Wenbo Guo, Qingying Hao, Arridhana Ciptadi, Ali Ahmadzadeh, Xinyu Xing, Gang Wang. "CADE: Detecting and Explaining Concept Drift Samples for Security Applications". In Proceedings of *The 30th USENIX Security Symposium*, Vancouver, Canada, August 2021. Artifact Evaluated.

[USENIX Security'20] Shuofei Zhu, Jianjun Shi, Limin Yang, Boqin Qin, Ziyi Zhang, Linhai Song, Gang Wang. "Measuring and Modeling the Label Dynamics of Online Anti-Malware Engines". In Proceedings of *The 29th USENIX Security Symposium*, Boston, MA, August 2020. Artifact Evaluated.

[IMC'19] Peng Peng, Limin Yang, Linhai Song, Gang Wang. "Opening the Blackbox of VirusTotal: Analyzing Online Phishing Scan Engines." In Proceedings of *The ACM SIGCOMM Internet Measurement Conference*, Amsterdam, Netherlands, October 2019.

[USENIX Security'18] Dongliang Mu, Alejandro Cuevas, Limin Yang, Hang Hu, Xinyu Xing, Bing Mao, Gang Wang. "Understanding the Reproducibility of Crowd-reported Security Vulnerabilities." In Proceedings of *The 27th USENIX Security Symposium*, Baltimore, MD, August 2018.

[Globecom'17] Limin Yang, Xiangxue Li, Yu Yu. "VulDigger: A Just-in-time and Cost-Aware Tool for Digging Vulnerability-Contributing Changes." In Proceedings of *IEEE Global Communications Conference (GLOBECOM)*, Singapore, December 2017.

Journal Articles / Workshop Proceedings

[DLS'20] Limin Yang, Arridhana Ciptadi, Ali Ahmadzadeh, Gang Wang . "BODMAS: An Open Dataset for Learning based Temporal Analysis of PE Malware", In Proceedings of *4th Deep Learning and Security Workshop*, in conjunction with IEEE Symposium on Security and Privacy (Oakland), May 2021.

[SafeThings'20] Hang Hu, Limin Yang, Shihan Lin, Gang Wang. "A Case Study of the Security Vetting Process of Smart-home Assistant Applications", In Proceedings of *IEEE Workshop on the Internet of Safe Things*, in conjunction with IEEE Symposium on Security and Privacy (Oakland), San Francisco, CA, May 2020.

[PPNA'17] Minhui Xue, Limin Yang, Keith W. Ross, and Haifeng Qian. "Characterizing user behaviors in location-based find-and-flirt services: Anonymity and demographics." In *Peer-to-Peer Networking and Applications (PPNA)*, 2017.

Research Experience

Concept Drift Detection and Explanation, Research Assistant, UIUC *Jan.2020 – Jun.2020*

- Implemented a novel system (CADE) with contrastive learning to detect concept drift in security applications.
- Built an explanation module to offer semantically meaningful reasoning of CADE's decision with new metrics.
- CADE is 2 times faster and achieves higher detection rate (F1 = 96%) than state-of-the-art method Transcend (F1 = 80% or lower) on Android malware and network intrusion datasets.
- CADE also worked well on Blue Hexagon's PE malware database and identified 161 out of 165 unseen families.

Explaining Unsupervised Deep Learning Models, Research Assistant, UIUC *Aug.2019 – Dec.2019*

- Defined two definitions of machine learning explanation (perturbation-based and gradient-based).
- Built a unified explanation framework for explaining both clustering and anomaly detection models.
- Achieved 20% $\sim$ 90% higher success rate than existing white-box explanation methods (vanilla gradients and integrated gradients) and black-box method (LIME) on different fidelity tests.

Reliability of VirusTotal, Research Assistant, UIUC *Sep.2019 – Nov.2019*

- Surveyed 115 papers on how researchers use VirusTotal.
- Measured the label dynamics of 14,000+ PE malware via daily snapshots over one year and analyzed the correlations and causalities between VirusTotal engines.
- Identified questionable methodologies and offered suggestions on the usge of VirusTotal.

VirusTotal Phishing URLs Scanning, Research Assistant, Virginia Tech *Jan.2019 – May 2019*

- Controlled 66 phishing websites to understand the quality and reliability of security scanners and VirusTotal.
- Submitted phishing sites to VirusTotal and 18 security scanners periodically and observe the incoming traffic.
- Provided insights on the poor detection performance of VirusTotal and scanners' own APIs and suggestions to utilize VirusTotal more properly on URL labelling.

Smart Home Assistants Cloud Spoofing, Research Assistant, Virginia Tech *Aug.2018 – May 2019*

- Understand the authentication mechanism in smart home assistant systems (Amazon Alexa and Google Home).
- Developed an Amazon Alexa skill and a Google Home action for finding authentication issues.
- Verified that replay attack and SQL injection attack are feasible with proof-of-concept experiments.

Internships

The Pennsylvania State University, Research Intern, Pennsylvania, US *Sep.2017 – Feb.2018*

- An empirical study to unveil the reproducibility of vulnerabilities using crowdsourcing information.
- Manually reproduced 368 real-world memory corruption bugs based on 6,000+ crowd-sourced reports.
- Obtained quantitative evidence on the prevalence of missing information in vulnerability reports and low reproducibility. Validated that crowdsourcing could ease the effort of vulnerability reproduction.

XuebaJun, Search & Rank Intern, Shanghai, China *Sep.2016 – Oct.2016*

- Helped reduced 33% of the response latency by debugging the searching of XuebaJun app.
- Finished a comprehensive code report (10,000+ SLOC of Java).

Peking University, Exploit Intern, Beijing, China *Jul.2015 – Aug.2015*

- Focused on practical training like binary vulnerability discovery/exploit (Windows).
- Extracted fingerprints for industrial control systems like Siemens S7-1200 with Nmap.

Awards

- ECNU Graduate Student Overseas Research Scholarship *2017*
- ECNU Top-notch Innovative Personnel Training Plan **(4/91)** *2013 – 2015*

Teaching

- CS-4264 Principles of Computer Security, Virginia Tech, Teaching Assistant *Spring 2019*
- CS-3114 Data Structures and Algorithms, Virginia Tech, Teaching Assistant *Fall 2018*

Professional Services

- **[Oakland]** IEEE Symposium on Security and Privacy, Student PC *2021*
- [Patterns] Patterns by Cell Press, Reviewer *2021*