Yuchen Yang

410-350-6041 | yc.yang@jhu.edu | homepage

Education

Johns Hopkins University — MD, United States
Doctor of Philosophy in Computer Science (Current GPA: 3.97/4.0) — *2021.1 – Present*

Johns Hopkins University — MD, United States
Master of Science in Security Informatics (GPA: 3.84/4.0) — *2019.9 – 2020.12*

Shandong University — Shandong, China
Bachelor of Engineering in Software Engineering (GPA: 4.33/5.0) — *2015.9 – 2019.6*

Publications

SneakyPrompt: Jailbreaking Text-to-image Generative Models
Yuchen Yang, Bo Hui, Haolin Yuan, Neil Gong, Yinzhi Cao. **equally contributed*
To appear in the Proceedings of the IEEE Symposium on Security and Privacy (Oakland), 2024

PrivateFL: Accurate, Differentially Private Federated Learning via Personalized Data Transformation
Yuchen Yang*, Bo Hui*, Haolin Yuan*, Neil Gong, Yinzhi Cao.
In the proceedings of USENIX Security Symposium, 2023

Fortifying Federated Learning against Membership Inference Attacks via Client-level Input Perturbation
Yuchen Yang, Haolin Yuan, Bo Hui, Neil Gong, Neil Fendley, Philippe Burlina, Yinzhi Cao.
In the proceedings of IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2023

Addressing Heterogeneity in Federated Learning via Distributional Transformation
Yuchen Yang*, Haolin Yuan*, Bo Hui*, Philippe Burlina, Neil Gong, Yinzhi Cao.
In the proceedings of European Conference on Computer Vision (ECCV), 2022

Practical Blind Membership Inference Attack via Differential Comparisons
Yuchen Yang*, Bo Hui*, Haolin Yuan*, Philippe Burlina, Neil Gong, Yinzhi Cao.
In the proceedings of Network & Distributed System Security Symposium (NDSS), 2021

Professional Services

- IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2024, Artifact Evaluation Committee
- ACM ASIA Conference on Computer and Communications Security (ASIACCS), 2024, External reviewer
- USENIX Security Symposium, 2023, External reviewer
- The ACM Conference on Computer and Communications Security (CCS) 2022, External reviewer
- IEEE Computer Security Foundations Symposium (CSF) 2022, External reviewer
- IEEE International Conference on Distributed Computing Systems (ICDCS) 2022, External reviewer

Experiences

Research Assistant — 2020.3 – Present
Advisor: Dr. Yinzhi Cao — *Johns Hopkins University*

Student Associate — 2023.10 – 2024.2
Advisor: Dr. Shao-yuan Lo — *Honda Research Institute*

Teaching Assistant — 2020.9 – 2020.12
Course: Web Security — *Johns Hopkins University*

Research Assistant — 2018.6 – 2018.9
Advisor: Prof. Yingjie Tian — *Chinese Academy of Sciences*

Projects

Master Dissertation 2020.3 – 2022.8

Advisor: Prof. Yinzhi Cao *Johns Hopkins University*

- Proposed a novel membership inference attack called *BlindMI* via differential comparison.
- Avoided depending on shadow models and kept strict black-box access with only 20 extra queries of target model.
- Improved attack F1-score by nearly 20% when compared to state-of-the-art on some datasets.
- Defeated state-of-the-art defenses and explored potential defenses.

Capture the Flag: Vulnerability Exploration and Intrusion | *Kali linux* 2019.10 – 2019.12

- Exploited and analyzed VSFTPD 2.3.4 backdoor vulnerability.
- Exploited and analyzed PHP-CGI query string parameter vulnerability.
- Exploited and analyzed Tomcat Password Brute Force and Get Webshell Vulnerability.

Yelp Fake Review Detection Based on Deep Learning | *Python* 2019.9 – 2019.12

- Developed a vectorization model based on Doc2vec and Bert.
- Compared performance of different classification models among SVM, Bi-LSTM and Bert.
- Established fake review detection model based on Bi-LSTM with pre-trained Bert model *Kashgare*.

Undergraduate Dissertation 2018.12 – 2019.6

Advisor: Prof. Yuqing Sun *Shandong University*

- Aimed at the auto-grading problem of Chinese composition in primary and secondary education.
- Designed a document vector representation model using both vocabularies' characteristics and information gain.
- Developed a grading model via Bi-directional LSTM.

Summer Research Intern 2018.6 – 2018.9

Advisor: Prof. Yingjie Tian *Chinese Academy of Sciences*

- Selected and gathered stock data with self-developed crawler.
- Preprocessed the data and extracted data features which transformed as vectors using doc2vec model.
- Optimized and developed a new SVM+ model by distinguishing the privileged vectors in SVM model.

Students Management System Based on SSM Framework | *Java, Bootstrap, MyBatis*2017.9 – 2017.12

- Put forward the function design of the system based on user requirement analysis.
- Realized the internal logical design and physical design including: MD5 encryption and user identification.
- Implemented the User Interface with Bootstrap by studying HTML, CSS and JavaScript.

Patent

A New System for Stock Volatility Prediction by Using Privileged Support Vector Machines

Yuchen Yang, Zheng Yan, Haoyang Li, Zhixuan Lv, Weiwei Zhao, Simiao Zhao.

Under IP Australia Application, No.2018101304