Liuwan Zhu

[LinkedIn]

Email: liuwanz601@gmail.com
Mobile: 757-335-8193
Location: Norfolk, VA, 23508

Education

- **Ph.D. in Electrical and Computer Engineering** — USA
  Old Dominion University; GPA:3.96 — *Sept 2017 – Dec 2022(Expected)*
- **B.S. in Computer Science** — CHINA
  Hunan University; GPA:3.58(Top 10%) — *Sept 2013 – Jun 2017*

Skills Summary

- **Languages**: Python, C/C++, Bash, Java, Matlab, SQL, Git, JavaScript, HTML, CSS
- **Frameworks**: Pytorch, TensorFlow, Keras, Scikit-learn, Pandas, Numpy, SciPy, MySQL, PySpark, CUDA

Experience

- **Graduate Research Assistant**
  Old Dominion University Research Foundation — *Sept 2018 – Present*

  Actively conducted various research projects related to security, deep learning in Computer Vision(CV), and Vision-Language Multi-Modal funded by National Science Foundation(NSF), including:
  - Designed a backdoor detection model with Generative Adversarial Network to identify the backdoor attacks in the Neural Networks (CNNs), which can successfully detect hidden triggers compared to previous works.
  - Designed an innovative optimization algorithm to detect backdoors in the Vision-Language model(CLIP) by jointly searching the image and text domains, which achieved over 93% detection rate. This is the first work to detect backdoors in a Multi-Modal model without access to the training process and the downstream tasks.
  - Tech: Python, Pytorch, TensorFlow, Keras
- **Summer Camp Instructor**
  GenCyber Summer Camp[Git] (Funded by: NSF/NSA) [Targeted to K-12 students/teachers] *Jun 2022 – July 2022*
  - Led instructors to build an attendance system with the face recognition model and launch attacks on the model that demonstrates the security issues in the popular AI models.
- **Workshop Instructor**
  DeapSECURE [Git](Funded by: NSF) [Targeted to graduate students] — *May 2019 – August 2021*
  - Created lessons and hands-on labs covering High-Performance Computing(HPC) system usage and analyzing the spam emails on the IP address with PySpark.
  - Created lessons and hands-on labs for using Pandas to process mobile phone system data and further building a Machine learning model(Logistic Regression, Decision Tree) and Deep Learning model(CNNs) to identify mobile applications by analyzing resource usage statistics.

Projects

- **Malicious Cryptocurrency Mining Activities Detection System** — *Feb 2018 – July 2018*
  - Built a simple PHP-based website and injected the malicious Cryptocurrency Mining JavaScript code. Ran the malicious website and other applications simultaneously and collected the system resource utilization data.
  - Developed a machine learning model using Deep Capsule Network and SVM to detect malicious mining activities through system behavioral analysis, achieving a detection rate of as high as 99%.
  - Paper was accepted by 2019 IEEE INFOCOM, and won the Best In-session Presentation Award.[PDF]
- **Stock Analysis System** — *Feb 2021 – Apr 2021*
  - Built a stock analysis system based on TD-Ameritrade Python API for stock real-time query and analysis.
  - Created a streaming client that can automatically create a web socket connection with the TD server and receive steady real-time stock dataflow back per second based on Asyncio WebSockets.
  - Designed MySQL database to manage stock information and further analysis.

Publications

- **L. Zhu**, R. Ning, J. Li, C. Xin, and H. Wu, "Most and Least Retrievable Images in Visual-Language Query Systems", in European Conference on Computer Vision (**ECCV**), 2022. [PDF]
- **L. Zhu**, R. Ning, C. Xin, C. Wang, and H. Wu, "CLEAR: Clean-up Sample-Targeted Backdoor in Neural Networks," in IEEE/CVF International Conference on Computer Vision **(ICCV)**, 2021. [PDF]
- **L. Zhu**, R. Ning, C. Wang, C. Xin, and H. Wu, "GangSweep: Sweep out Neural Backdoors by GAN", in ACM International Conference on Multimedia **(ACM MM)**, 2020. [PDF]