Mabon Manoj Ninan

513-850-6582 | ninanmm@mail.uc.edu | www.linked in.com/in/ninanmm | mabonmn.github.io

EDUCATION

Bachelor of Science | ***Computer Engineering, Minor Computer Science*** **Graduating: May 2024**

- **University of Cincinnati** **GPA: 3.933/4.00**
- **Honors and Awards:** Highest Math Placement Score
- **Scholarships:** UC International Scholarship, CEAS Outreach Scholarship, CEAS Research Grant

PUBLICATIONS AND POSTERS

Published Papers

- Chenggang Wang, *__Mabon Ninan__, Shane Reilly, Joel Ward, William Hawkins, Boyang Wang, John M Emmert, "**Portability of Deep-Learning Side-Channel Attacks against Software Discrepancies**," In Proceedings of the 16th ACM (WiSec'23), May 29-June 1, 2023, Guildford, **United Kingdom** *(DOI 10.1145/3558482.3590177)*
  - ***Presented** this paper at the 16th ACM WiSec Conference at Guilford, United Kingdom
  - www.youtube.com/watch?v=h-T1jcrd0IU&t=791s

Accepted Papers

- Haipeng Li, *__Mabon Ninan__, Boyang Wang, John M Emmert, **"TinyPower: Deep-Learning Side-Channel Attacks with Tiny Neural Networks"**, In Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2024 *(Preprint available on personal website)*
- Andrew Kosikowsk, Daniel Cho, **Mabon Ninan**, Anca Ralescu, Boyang Wang, **"EvilELF: Evasion Attacks on Deep-Learning Malware Detection over ELF Files,"** In Proceedings of the 22nd IEEE International Conference on Machine Learning and Applications (ICMLA), 2023 *(Preprint available on personal website)*

Posters Presentations

- **Mabon Ninan**, John M Emmert, Boyang Wang, "**Robust Cross Side-Channel Attacks",** CHEST. Semi Annual Conference, University of Cincinnati, Ohio, May 17- May 18, 2023. (Role: **Presenter**)
- **Mabon Ninan**, Evan Nimmo, John M Emmert, Boyang Wang, "**Side Channel Attacks across Different EM probe locations",** REU site Conference Presentation 2023, University of Cincinnati, Ohio, July 28, 2023. (Role: Presenter)

Ongoing Work

- **Mabon Ninan**, Boyang Wang, **"CrossEM: The Impact of EM Probe Locations on Deep-Learning Side-Channel Attacks"**

WORK EXPERIENCE

Deep Learning Researcher | Data Security and Privacy Lab University of Cincinnati, *OH* July 2022 - Present

- Leading research in Deep Learning based Side Channel attacks to recover AES encryption keys
- Working on reinforcement learning models to develop architectures for high noise side channel attacks
- Developing custom pruning algorithms using Python to reduce the size of existing deep learning models
- Implemented code for structured, un-structured and automatic pruning of neural networks
- Designed methods for statistical analysis of CNN model performance by using FLOP's as a baseline metric
- Successfully deployed and fine-tuned models on low power devices like Raspberry-pi's
- Conducted research on cross domain adaptations of models trained on source devices and developed attacks to counter software, hardware, and AES key discrepancies on different targets
- Developed pipeline using Python to capture and process high sampling rate data from both EM and Power traces
- Leading a team of 2 undergraduate students in acquisition of 3.3 million traces of high-quality data for studies
- Optimized existing binary classification models for side channel attacks using TensorFlow and Keras

NSF-REU Research Assistant | University of Cincinnati, *OH* May 2023 – July 2023

- Investigated evasion attacks on end-to-end deep-learning malware detection over ELF binaries using pytorch

- Collaborated with a team of two students to develop a pipeline to modify ELF binaries such that a well-trained neural network is misled and predicts the file as benign
- Tested modified binary files using deep-learning detectors MalConv and FireEye along with 62 real world detectors using VirusTotal
- Proposed five techniques to create malicious ELF binaries with unchanged functionalities, successfully evading end-to-end deep learning malware detection, and proposed retraining methods to enhance detection resilience

Software Engineer | College of Engineering and Applied Sciences (UC), *OH* May 2022 – July 2022

- Lead the development and deployment of the University's auto grading solution using GradeScope and its integration to multiple courses across the EECE and CS departments with cost savings of $10,000 per course
- Created a docker based auto-grader utilizing Otter to grade Python Notebooks integrated with GradeScope
- Constructed a server-based coding IDE with an integrated auto-grading system, demonstrating proficiency in both server-side development and unit testing tools for auto-grading
- Deployed Jupyter Hub with an integrated auto-grader (Nbgrader) and reduced grading time by 90%

Research Assistant | Video Summarization Lab University of Cincinnati, *OH* Jan 2022 – July 2022

- Processed videos using pretrained machine learning models like CLIP and GoogLe-Net to extract features for video summarization and video classification using PyTorch
- Developed a pipeline to extract frames, preprocess images and run specified computer vision models on frames, followed by generating frame probabilities utilizing python
- Created video segments using Knapsack clustering to generate a summary of video's
- Trained versions of the existing computer vision models identifying layers that provide valuable features
- Created a program to classify frames from surgical videos into informative and non-informative categories

Research Intern | Spatio-Temporal Data Analytics Lab University of Cincinnati, *OH* Nov 2021 - Jan 2022

- Utilized JULIA to preprocess data from simulations, creating of matrices and data frames for research purposes
- Produced clear and organized CSV files and graphical representations (using MAKIES) of the data
- Conducted comprehensive analysis of large data sets, summarizing findings, and recommending techniques to compress data for future research
- Identified areas for improvement in the data collection process and recommended changes to optimize quality
- Maintained documentation of data analysis methods, results, and conclusions for future reference and replication

TEACHING EXPERIENCE

Supplementary Instructor Department Coordinator | University of Cincinnati, *OH* July 2021 – Dec. 2022

- Facilitated and lead interactive group learning sessions for Chemistry and Calculus-based Physics 2, supporting a class size of 650 students per semester
- Developed and implemented engaging teaching strategies to enhance understanding and comprehension of complex concepts while coordinating with the course instructors
- Served as the Department Coordinator, overseeing 35 other Supplementary Instructor leaders provided guidance and support, ensuring effective delivery of course content
- Conducted performance reviews, provided feedback, maintained time charts and payroll, and facilitated various administrative functions within the department

Peer Leader | University of Cincinnati, *OH* July 2021 – Dec. 2021

- Led weekly Learning Community meetings, providing academic support and mentorship
- Conducted individual and group mentoring sessions to address students' academic needs and interests
- Collaborated with faculty, advisors, and organizations to enhance the Learning Community experience and prepare students for future academic accomplishments

CAMPUS INVOLVEMENT AND VOLUNTEERING

Production Volunteer | Cross-Roads Church, *OH* Nov. 2021 – Present

- Operated cameras to create an immersive concert experience, capturing live musicians and on-stage speakers

- Prioritized capturing high-quality footage and ensuring audience satisfaction while maintaining professionalism and ethical standards

English Tutor | ENGin, Online Aug. 2020 – May 2020

- Tutored students in Ukraine, providing personalized English language instruction to improve their speaking, listening, reading, and writing skills
- Developed engaging lesson plans and utilized interactive teaching methods to make learning effective

PROJECTS

Structured And Unstructured Pruning for Deep Learn Models

Developed custom tool for Structured and Unstructured pruning of trained CNN models – **GitHub**

High Sampling Data Collection Tool

Developed a robust framework to facilitate collection of high sampling power traces from microcontrollers with custom auto-scaling tool to enable data compression on the fly – **GitHub**

Image Feature Extractor

Created a framework to analyze and extra features from images using multiple pre trained models and provided simultaneous comparison of model performance – **GitHub**

SKILLS SUMMARY

- **Programming Technologies:** Python, C++, C, Julia, JAVA, MATLAB, LabView, **LaTeX**, CSS, Flask
- **Frameworks:** TensorFlow, PyTorch, Scikit, Pandas, Numpy, Numba, Open-CV, cuDNN
- **Data Analysis and Visualization:** Matplotlib, Plotly, Seaborn, Tensor Board
- **Other Technologies:** Docker, SSH, Bash, Unix/Linux, AWS, Azure, GCP, GIT
- **Soft Skills:** Leadership, Public Speaking, Teamwork, Communication, Thinking and Problem Solving, Initiative and Follow-through