Mabon Manoj Ninan

513-850-6582 | ninanmm@mail.uc.edu
www.linked in.com/in/ninanmm | github.com/mabonmn | 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:** Deans List (All academic semesters), Highest Math Placement Score
- **Scholarships:** UC International Scholarship, CEAS Outreach Scholarship, CEAS Research Grant

PUBLICATIONS

Accepted 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 (acceptance: 24%)
- 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, 2023

Submitted Papers

- Haipeng Li, **Mabon Ninan**, Boyang Wang, **"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

Ongoing Work

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

CONFERENCE PRESENTATIONS

1. **Portability of Deep-Learning Side-Channel Attacks Against Software Discrepancies**
   "Proceedings of the 16thACM WiSec 2023", University of Surrey at Guilford, United Kingdom, May 29- June 1, 2023. (Role: Presenter)
2. **Robust Cross Side-Channel Attacks**
   "CHEST. Semi Annual Conference", University of Cincinnati, Ohio, May 17- May 18, 2023. (Role: Presenter)
3. **Side Channel Attacks across Different EM probe locations**
   "REU Site Conference Presentation 2023", University of Cincinnati, Ohio, July 28, 2023. (Role: Presenter)

EXPERIENCE

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

- Conducting 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-structed 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
- Developing and adapting deep leaning models to identify malware in ELF files, further classifying malicious binaries from benign binaries

- 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-*Cincinnati, OH* May 2023 – July 2023

- Investigated evasion attacks on end-to-end deep-learning malware detection over ELF binaries
- 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) - *Cincinnati, OH* May 2022 – July 2022

- Lead the development and deployment of the University's auto grading solution using GradeScope
- 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) to support courses that utilize notebooks
- Reduced grading time by 90% as it only required sample unit test cases allowing instructors to provide more detailed feedback to students and improving overall learning outcomes
- System proved to be a viable solution for auto grading multiple courses across the EECE and CS departments with potential cost savings of $10,000 per course

Research Assistant | Video Summarization Lab UC -*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 (UC) **-***Remote* 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

TECHNICAL SKILLS

- **Programming Technologies:** Python, JAVA, C++, C, MATLAB, LabView, HTML, CSS, Flask
- **Machine Learning:** TensorFlow, Keras, PyTorch, Sklearn, Pandas, Numba, Open-CV, cuDNN
- **Data Analysis and Visualization:** Matplotlib, Plotly, Seaborn, VBA, Tensor Board, Julia, Pandas
- **Other Technologies:** Docker, SSH, Bash, Unix/Linux, AWS, Azure, GCP, GIT

TEACHING EXPERIENCE

Supplementary Instructor and Department Coordinator | UC -*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 coordinated 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 | UC -*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 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 | ENGine 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

REFERENCES

1. Dr. Boyang Wang (Assistant Professor at the University of Cincinnati)
Phone Number: +1 513 556 4785
Email: wang2ba@ucmail.uc.edu
Website: https://homepages.uc.edu/~wang2ba/

2. Dr. Gautam Pillay (Associate Dean at the University of Cincinnati)
Phone Number: + 1 513 556 4163
Email: pillaygm@ucmail.uc.edu

3. Dr. Mehdi Norouzi (Assistant Professor at the University of Cincinnati)
Phone Number: +1 513 549 3435
Email: norouzmi@ucmail.uc.edu