MABON NINAN

+1-513-850-6582 | ninanmm@tamu.edu | HomePage

Mabon-Ninan | mabonmn | Mabon-Ninan

College Station Texas, USA

EDUCATION

- **Doctor of Philosophy in Computer Science** *August 2024 – Present*
  Texas A&M University, GPA: 4.00/4.00; Advisor: Dr. Marcus Botacin College Station, USA
  Thesis: Algorithms and Advanced Machine Learning for Cybersecurity
  Committee: Dr. James Caverlee, Dr. Nitesh Saxena, Dr. Eman Hammad

- **Bachelor of Science in Computer Engineering** *August 2020 – April 2024*
  University of Cincinnati, Summa Cum Laude (3.953/4.00); Advisor: Dr. Boyang Wang Cincinnati, USA
  Thesis: Domain Adaptation for Deep Learning Models and Tiny Neural Networks

PUBLICATIONS C=CONFERENCE, T=THESIS, J=JOURNAL,PP= PRE-PRINT BC=BOOK CHAPTER * PRESENTED PAPER

C.[8] **Mabon Ninan**, Ashwin Menon, Marcus Botacin. **"SoK: If "Real Attackers Don't Compute Gradients," What Do They Do? Revisiting Adversarial Malware Evasion Using In-the-Wild Malware"**.

C.[7] **Mabon Ninan**, Nhat Minh Nguyen, Soumyajyoti Dutta, Sidharth Anil, Marcus Botacin. **"AutoPYara: Next-Gen YARA Rule Gen"**. *In Submission 29th Symposium on Research in Attacks, Intrusions and Defenses, (RAID) 2026*.

C.[6] **Mabon Ninan**, Ryan Evans, Logan Reichling, Nirnimesh Ghose, Boyang Wang (2025). **"TinyRadio: Tiny Neural Networks for Fingerprinting Radio Frequency Signals** . *IEEE National Aerospace and Electronics Conference NAECON 2025*. DOI: 10.1109/NAECON65708.2025.11235437

C.[5] Logan Reichling, Ryan Evans,**Mabon Ninan**, Phuc Mai, Boyang Wang, Yunsi Fei and John Emmert . (2025).**MicroPower: Micro Neural Networks for Side-Channel Attacks**. In *2025 IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2025)*. DOI: 10.1109/HOST64725.2025.11050048

C.T [4] *__Mabon Ninan__, Evan Nimmo, Shane Reilly, Channing Smith, Wenhai Sun, Boyang Wang, and John M. Emmert. (2024). **A Second Look at the Portability of Deep Learning Side-Channel Attacks over EM Traces**. In *RAID '24: The 27th International Symposium on Research in Attacks, Intrusions and Defenses*, pp.630-643. ACM, New York, NY, USA, 30,September 2024, Padua, Italy. DOI: 10.1145/3678890.3678900

C.[3] * Haipeng Li, **Mabon Ninan**, Boyang Wang, John M. Emmert. (2024). **TinyPower: Side-Channel Attacks with Tiny Neural Networks**. In *2024 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 320-331. IEEE. 06 June 2024, Tysons Corner, VA, USA. DOI: 10.1109/HOST55342.2024.10545382
BEST STUDENT PAPER

C.[2] Andrew Kosikowski, Daniel Cho, **Mabon Ninan**, Anca Ralescu, Boyang Wang.**EvilELF: Evasion Attacks on Deep-Learning Malware Detection over ELF Files**. In *2023 International Conference on Machine Learning and Applications (ICMLA)*, pp. 1702-1709.IEEE. Jacksonville, FL,USA DOI: 10.1109/ICMLA58977.2023.00258

C.[1] * Chenggang Wang, **Mabon Ninan**, Shane Reilly, Joel Ward, William Hawkins,Boyang Wang, and John M. Emmert. (2023). **Portability of Deep-Learning Side-Channel Attacks against Software Discrepancies**. *In Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'23)*, pp. 227-238. New York, NY, USA. 06 June 2023, Guildford, United Kingdom. DOI: 10.1145/3558482.3590177

BC.[1] Logan Reichling, **Mabon Ninan**, Boyang Wang, John M. Emmert. (2026). **Deep Learning Side-Channel Attacks: Challenges and Opportunities**. - Advancements in Hardware Design and Trust. [Chapter] [Book]

J. [1] Shruti Hegde, **Mabon Ninan**, Jonathan R. Dillman, Shireen Hayatghaib, Elanchezhian Somasundaram. **Evaluating Clinical NLP Services for Chest Radiograph Report Labeling: A Comparative Study on an Independent Pediatric Dataset**. Journal of Imaging Informatics in Medicine, June 2026.

PP. [1] Shruti Hegde, **Mabon Ninan**, Jonathan R. Dillman, Shireen Hayatghaibi, Lynn Babcock, Elanchezhian Somasundaram. **Can Modern NLP Systems Reliably Annotate Chest Radiography Exams? A Pre-Purchase Evaluation and Comparative Study of Solutions from AWS, Google, Azure, John Snow Labs, and Open-Source Models on an Independent Pediatric Dataset**. DOI: 10.21203/rs.3.rs-6772394/v1

Co-Advised Students

- **Ryan Evans** (May 2023 – June 2024, NSF REU Site), University of Cincinnati First Job: Machine Learning Engineer, Medpace Publications: HOST 2025, NAECON 2025
- **Muhib Khan** (Dec 2023 – June 2024), University of Cincinnati, Class of 2025 First Job: Platform Engineer, IBM
- **Evan Nimmo** (May 2023 – July 2023, NSF REU Site), University of Cincinnati, Class of 2025 First Job: Junior Hardware Embedded Security Engineer, Riverside Research Publications: RAID'24
- **Andrew Kosikowski** (May 2023 – July 2023, NSF REU Site), Rose-Hulman Institute of Technology, Class of 2024 First Job: EO/IR Systems Engineer, MIT Lincoln Laboratory Publications: ICMLA'23
- **Daniel Cho** (May 2023 – July 2023, NSF REU Site), Hamilton College, Class of 2025 Publications: ICMLA'23

Talks

- **CSCE Graduate Seminar Texas A&M University (CSCE682)** *February 2026*
  Automatic threat hunting rules generation College Station, USA
- **AI for Cybersecurity Research at Texas A&M University** *February 2025*
  Deep Learning Side-Channel Attacks College Station, USA
- **27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)** *September 2024*
  Padua, Italy
  - *A Second Look at the Portability of Deep Learning Side-Channel Attacks over EM Traces*
  - *Cross-Regional Malware Detection via Model Distilling and Federated Learning, Marcus Botacin, Heitor Gomes*
  - *What do malware analysts want from academia? A survey on the state-of-the-practice to guide research developments, Marcus Botacin*
- **Center for Hardware and Embedded System Security and Trust (CHEST) Annual Conference** *July 2024*
  Side-Channel Attacks And Tiny Neural Networks Connecticut, USA
- **IEEE International Symposium on Hardware Oriented Security and Trust (HOST)** *May 2024*
  TinyPower: Side-Channel Attacks with Tiny Neural Networks Washington DC, USA
- **16th ACM Conference on Security and Privacy in Wireless and Mobile Networks** *May 2023*
  Portability of Deep-Learning Side-Channel Attacks against Software Discrepancies Link Surrey, United Kingdom

Research and Work Experience

- **Texas A&M University [🌐]** *August 2024 - Present*
  Research Assistant: PhD Student Texas, USA
  - Conceptualized novel malware detection methods introducing new paradigms for zero-overhead detectors.
  - Researching multi-model machine learning approaches for software-based malware detection.
  - Built agentic malware detection systems, creating self-healing LLMs designed to be robust against concept drift.
  - Investigating explainability (XAI) of security models to improve transparency and trust in threat detection.
  - AutoPYara: Optimized threat-hunting rule generation through Augmented K-means and sub-clustering, achieving a 14% performance increase and 8% better generalization in low-sample environments. [C7]
- **Cincinnati Children's Medical Hospital [🌐]** *May 2024 - August 2024*
  Research Scientist Cincinnati, USA
  - Proposed a multimodal system to evaluate and provide feedback to radiologists for CXR report generation.
  - Created foundational models for CXR imaging, enhancing interpretability in pediatric clinical settings.
  - Quantified uncertainty introduced by pediatric data on state-of-the-art clinical models and developed methods to better adapt models for pediatric data.
  - Evaluated performance variations across commercial NER services (Google Cloud, AWS, Spark NLP by John Snow Labs) and compared them with local medical NER models (CheXpert, CheXbert).
  - Leveraged BERT models to classify and label pediatric reports into twelve common diseases.
- **University of Cincinnati Data Security and Privacy Lab [🌐]** *July 2022 - August 2024*
  Research Assistant Cincinnati, USA
  - Developed custom pruning algorithm to reduce model complexity by up to 98% and designed custom kernels to deploy on microcontrollers (Jetson Nano, RbPi-4 and FPGA). [C3,C5,C6]
  - Research on Domain adaptation of Deep Learning models to reduce discrepancies across noisy data. [C4,C1]
  - Conceptualized new method for unsupervised training "On-the-Fly labeling" for data without labels. [C4]
  - Proposed a new method for Side Channel trace simulation and capture using Electromagnetic Traces. [C4]
  - Supervised team of three undergraduate students for acquisition of the largest public EM side channel dataset. [C4]
  - Reinforcement learning-based architecture search to develop optimized models for high-noise data. [C3]
  - Fine-tuned deep-learning detectors MalConv and FireEye with modified malicious binary files. [C2]
- **College of Engineering and Applied Sciences at University of Cincinnati** *May 2022 - August 2022*
  Software Engineering Intern Cincinnati, USA
  - Led the development of the University's auto grading solution using GradeScope and its integration.
  - Created a Docker based auto-grader utilizing Otter to grade Python Notebooks integrated with GradeScope.

Academic Service

1. PC Member, 29th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2026)
2. PC Member, 28th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2025)
3. Reviewer, Computers & Security (COSE), 2026
4. PC Member, The 41st ACM/SIGAPP Symposium On Applied Computing
5. Artifact Evaluator: CCS 2025

DSN 2026

Technical Skills

Languages: Python, C/C++, Assembly, SQL
Machine Learning: PyTorch, TensorFlow, LLMs (Transformers), Scikit-learn, Computer Vision, NLP
Security & Tools: Malware Analysis, Reverse Engineering (ELF), AWS, Google Cloud, Azure, Docker, Git, Linux