UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

From Hardware to Software: Defending the Next Generation of Artificial Intelligence and Machine Learning Applications

by

Brooks Olney

For the Ph.D. degree in Computer Science and Engineering

The growing energy costs of artificial intelligence (AI) and machine learning (ML) workloads have motivated research efforts into low-power acceleration platforms. One popular platform is field-programmable gate arrays (FPGAs), due to their low-power and in-field reconfigurability. As the use of these specialized hardware platforms becomes more prevalent, concerns around the security of these systems have intensified. This has led to a significant body of research in adversarial machine learning, aimed at securing both the software and hardware components of ML applications. This dissertation focuses on hardware security in the context of FPGA-based ML systems. I explore the unique security risks associated with deploying ML applications on FPGAs and present novel methods for securing these systems against various cyberattacks, including IP theft. To ensure the overall security and integrity of FPGA-based ML systems, this work addresses security concerns at every level of the hardware stack, from the hardware abstraction layer up to the ML algorithm itself.

Examining Committee

Ismail Uysal, Ph.D., Chairperson
Robert Karam, Ph.D., Major Professor
Srinivas Katkoori, Ph.D.
Mehran Mozaffari Kermani, Ph.D.
Yasin Yilmaz, Ph.D.
Jean-François Biasse, Ph.D.

March 24th, 2023
10am-12pm
Hybrid (ENB 313 and Online)

THE PUBLIC IS INVITED

Publications

1) **B. Olney** and R. Karam, "Bits to BNNs: Reconstructing FPGA ML-IP with Joint Bitstream and Side-Channel Analysis", in IEEE Hardware Oriented Security and Trust (HOST). 2023 (to appear)
2) **B. Olney** and R. Karam, "Protecting Deep Neural Network Intellectual Property with Architecture-Agnostic Input Obfuscation", in Proceedings of the 2022 Great Lakes Symposium on VLSI (GLSVLSI).
3) **B. Olney**, S. Mahmud, and R. Karam, "Efficient Nonlinear Autoregressive Neural Network Architecture for Real-Time Biomedical Applications", in Proceedings of the 2022 IEEE AI Circuits and Systems (AICAS) Conference, 2022
4) **B. Olney**, S. Mahmud, M. A. Zaman, and R. Karam, "An EDA Framework for Design Space Exploration of on-chip AI in Bioimplantable Applications", in 2022 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS), 2022
5) **B. Olney** and R. Karam, "Diverse, Neural Trojan Resilient Ecosystem of Neural Network IP", ACM Journal on Emerging Technology for Computing Systems, Jun. 2021, issn: 1550-4832.
6) **B. Olney** and R. Karam, "WATERMARCH: IP Protection Through Authenticated Obfuscation in FPGA Bitstreams", IEEE Embedded Systems Letters, vol. 13, no. 3, pp. 81–84, 2021
7) **B. Olney** and R. Karam, "Tunable FPGA Bitstream Obfuscation with Boolean Satisfiability Attack Countermeasure", ACM Transactions on Design Automation for Electronic Systems, vol. 25, no. 2, Feb. 2020, issn: 1084-4309.

Robert Bishop, Ph.D.
Dean, College of Engineering

Ruth H. Bahr, Ph.D.
Dean, Office of Graduate Studies

Disability Accommodations:
If you require a reasonable accommodation to participate, please contact the Office of Diversity & Equal Opportunity at 813-974-4373 at least five (5) working days prior to the event.