Brooks Olney

Website: csee.usf.edu/~brooksolney
Email: brooksolney@usf.edu

Education

University of South Florida — Tampa, FL
Ph.D. in Computer Science and Engineering, Advisor: Dr. Robert Karam — 2019–Current
M.S. in Computer Engineering, GPA: 3.97/4.00 — 2021
B.S. in Computer Engineering, GPA: 3.70/4.00 — 2015–2018

Experience

University of South Florida — Tampa, FL
Graduate Research and Teaching Assistant - Interface Research Lab — 2018 –Present
Advisor: Dr. Robert Karam

- Adversarial Machine Learning
  - Implemented framework that defends neural network IP from state-of-the-art Trojan attacks
  - Developed methods of protecting neural network IP from reverse engineering and theft through input data obfuscation
- FPGA Bitstream Security
  - Implemented tunable architecture-agnostic FPGA bitstream obfuscation framework
  - Extended framework with *authenticated obfuscation*, allowing device-specific authentication and FPGA circuit unlocking capabilities
- Hardware Security Course Development
  - Completed write-up and design of several lab experiments including lab manual and source codes
  - Built general purpose hardware security tools for use by students and other researchers – most of which can be found on my Github (https://github.com/BrooksOlney)

SOFWERX — Tampa, FL
Software Engineering Intern — 2018 –2019
Supervisor: Peter Jorgensen

- CubeSat-class Satellite
  - Assisted in the design, development, testing and documentation of flight software for a CubeSat-class satellite
  - Identified, compared and recommended available core flight software systems
  - Designed, built, tested and integrated custom software modules to interface with the satellite hardware

University of South Florida — Tampa, FL
Undergraduate Teaching Assistant — 2018
Supervisor: Dr. Yu Sun

- Served as Lab Instructor for Computer Logic Design for 2 semesters
  - Responsible for administration and evaluation of labs for over 40 students

University of South Florida Tampa, FL
Undergraduate Research Assistant - Interface Research Lab 2018
Advisor: Dr. Robert Karam

- Tunable FPGA Bitstream Obfuscation
  - Explore optimizations to obfuscation framework in terms of runtime and overheads, extend framework to implement defense against Boolean Satisfiability (SAT) attack

ScaleIT USA Clearwater, FL
Software Engineer 2016 –2018
Supervisor: Jason Ford

- ScaleIT W8 - SaaS Product
  - Designed new code features and bug fixes in an Agile environment using C# with SQL backend
  - Implemented software solutions for over 30 new clients

Journal Publications

[1] **B. Olney** and R. Karam, "Diverse, neural trojan resilient ecosystem of neural network ip", *J. Emerg. Technol. Comput. Syst.*, Jun. 2021, Just Accepted, ISSN: 1550-4832.

[2] **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.

[3] **B. Olney** and R. Karam, "Tunable FPGA Bitstream Obfuscation with Boolean Satisfiability Attack Countermeasure", *ACM Trans. Des. Autom. Electron. Syst.*, vol. 25, no. 2, Feb. 2020, ISSN: 1084-4309.

Conference Publications

[0] **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.

[1] M. Keller, **B. Olney**, and R. Karam, "A Cloud-Connected Body Sensor Network Platform with Secure and Efficient Data Preprocessing", 2021.

[2] S. Mahmud, **B. Olney**, and R. Karam, "An Extensible Evaluation Platform for FPGA Bitstream Obfuscation Security", in *2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2021.

[3] **B. Olney**, S. Mahmud, and R. Karam, "Evaluating Edge Processing Requirements in Next Generation IoT Network Architectures", Mar. 2020, pp. 252–269, ISBN: 978-3-030-43604-9.

[4] S. Mahmud, **B. Olney**, and R. Karam, "Architectural Diversity: Bio-Inspired Hardware Security for FPGAs", in *2018 IEEE 3rd International Verification and Security Workshop (IVSW)*, 2018, pp. 48–51.

Under Review

[1] **B. Olney** and R. Karam, *Protecting Deep Neural Network Intellectual Property with Architecture-Agnostic Input Obfuscation*, Great Lakes Symposium on VLSI (GLSVLSI) '22, 2022.

Patents

[1] R. Karam and **B. Olney**, "Computing Hardware with Verifiable Watermarking", 2020 [Provisional Patent].

[2] R. Karam and **B. Olney**, "Deploying Neural Trojan Resilient Convolutional Neural Networks", 2021 [Full Patent].

Posters & Presentations

From Hardware to Software: Securing the Next Generation of Machine Learning Applications Fall 2021
Brooks Olney
[Major Area Presentation to Dissertation Committee – accepted into candidacy]

A Secure and Efficient Cloud-Connected Body Sensor Network Platform Fall 2021
Myles Keller, Brooks Olney, Robert Karam
[Accepted Conference Paper Presentation]

Evolving Security-aware Design Paradigms for EDA Tools Fall 2021
Brooks Olney, Robert Karam
ACM/IEEE ICCAD Student Research Competition

Deploying AI Applications to an Unsafe Edge Fall 2021
Brooks Olney, Robert Karam
IBM IEEE CAS/EDS AI Compute Symposium

Introduction to Machine Learning Tools and Techniques Fall 2021
Brooks Olney
Guest lecture for Practical Hardware Security (CIS 4930/6930)

Securely Deploying Neural Network IP in an Adversarial Environment Spring 2021
Brooks Olney, Robert Karam
USF Graduate Research Symposium
[Research Category Winner]

Evaluating Edge Processing Requirements in Next Generation IoT Network Architectures Fall 2019
Brooks Olney, Shakil Mahmud, Robert Karam
IFIP International Internet of Things (IoT) Conference
[Accepted Conference Paper Presentation]

FPNN: A Modular AI Accelerator for Resource and Connectivity Constrained Platforms Fall 2019
Brooks Olney, Robert Karam
IBM/IEEE AI Compute Symposium
[Invited to present poster at IBM TJ Watson Center - Yorktown Heights, NY]

Tunable FPGA Bitstream Obfuscation with Boolean Satisfiability Countermeasure Summer 2019
Brooks Olney, Robert Karam
Design Automation Conference
[Presentation of personal research project for Richard Newton Young Fellow Award]

Protecting Intellectual Property on FPGA with Low Overhead and SAT-Resistant Bitstream Obfuscation Spring 2019
Brooks Olney, Robert Karam
Cyber Florida Cybersecurity Research Symposium

Anti Reverse Engineering for FPGA Bitstreams Using Low Overhead and SAT-Resistant Obfuscation Spring 2019
Brooks Olney, Robert Karam
Florida Institute of Cybersecurity Research Conference

A Survey of Hardware Security Primitives Using Memristors 2018
Vishalini Laguduva Ramnath, Shakil Mahmud, Brooks Olney, Srinivas Katkoori, Robert Karam
Florida Institute of Cybersecurity Research Conference

Teaching

- **Teaching Assistant** at University of South Florida — 2018 –2020
  Computer Logic Design Lab (CDA 3201L)
  Introduction to Hardware Security (CIS 4930/6930)
  Computer Architecture (CDA 4205)
  Robotics Process Automation (COP 4901)
  Practical Hardware Security (CIS 4930/6930)

Skills

- **Machine Learning:** Tensorflow/Keras, Scikit-learn, PyTorch
- **FPGA Design:** Vivado & ISE, Quartus Prime II
- **Digital Logic Design:** Cadence Virtuoso

Languages

- **Expert:** Python
- **Advanced:** C#, Verilog, VHDL
- **Intermediate:** C, C++

Awards & Honors

- USF Virtual Graduate Research Symposium Research Category Winner — Spring 2021
- NSF GRFP Honorable Mention — 2020
- Richard Newton Young Fellow Award — 2019
- USF Department of CSE Chair's List — 2018
- Dean's List Honors — 2016 –2018

Extracurricular Activities

- USF IEEE Computing Society — Fall 2021-present
  President
- Attacks on Hardware Logic Locking Obfuscation Capture The Flag — Summer-Fall 2021
  Contest finalist
- University of South Florida's CodeBreakHERs Program — Summer 2021
  Hardware Instructional Assistant
- Tuft's University Coding-101 Pre-college Program — Summer 2021
  Graduate Course Assistant
- IFIP International Internet of Things (IoT) Conference — Fall 2019
  Associate Reviewer
- Computer Science & Engineering Graduate Student Welcome Event — Fall 2019
  Executive Committee Member
- IEEE VLSI Embedded Systems Conference — Spring 2018
  Associate Reviewer