

AARON J. WASSERMAN

N42W28924 Imperial Drive | Pewaukee, WI 53072 | U.S. Citizen
wasserman@gatech.edu | (262) 337-3197 | www.aaronwasserman.com

Education

Georgia Institute of Technology | Atlanta, GA
Bachelor of Science in Computer Engineering, GPA: 3.78

August 2018 – Present
Expected Graduation: December 2021

Georgia Institute of Technology | Atlanta, GA
Master of Science in Electrical and Computer Engineering, GPA: N/A

Expected Start: January 2022
Expected Graduation: December 2022

Skills

Programming: C, Python, Assembly (x86, MIPS), VHDL, C++
Platforms: Windows, Linux (Parrot, Kali, Ubuntu, Raspbian)
Hardware: ChipWhisperer, STM32GX MCUs, Raspberry Pi, Arduino, Test Bench Equipment
Software: IDA Pro, Ollydbg, gdb, Metasploit, Wireshark, Snort, Grassmarlin, Microsoft Office, GitHub
Languages: English (Native), Spanish (Conversational)

Relevant Coursework

Advanced Topics in Malware Analysis: Produced custom tools for static and dynamic analysis of malicious binaries. Labs included manual static analysis of APT1's WEBC2-greencat-2 and writing IDA Pro plugins to automatically produce CFGs, DU chains, and DDGs for a given binary.

Introduction to Malware Reverse Engineering: Conducted static and dynamic analysis on a wide range of Windows malware using IDA Pro and Ollydbg. Samples included packed/encrypted binaries and polymorphic code. Labs included W32.SQLSlammer.worm, W32.Lucius, and W32.Harulf.

Introduction to Computer Security: Studied introductory topics in computer security with an emphasis on fundamental security primitives. Labs included development of an exploit to attack a program vulnerable to a buffer overflow, vulnerability assessment with Metasploit, intrusion detection (IDS) with Snort, packet analysis with Wireshark, and SCADA/ICS discovery using Grassmarlin.

Cryptographic Hardware for Embedded Systems: Fundamental topics of cryptography, authentication, and power analysis attacks. Implemented and simulated DES, 3DES, RSA, and Fibonacci and Galois LFSRs in C and/or VHDL.

Hardware-Oriented Security and Trust: Studied the design of trustworthy circuits including protection of the hardware platform against unauthorized data extraction. Focus on cryptographic primitives from a hardware perspective, authentication, and Physically Unclonable Functions (PUFs). Labs included modifying and simulating a SHA256 VHDL module and testing pseudorandom data streams using the NIST Randomness Test Suite (SP800-22).

Experience

Electrical Engineering Intern | Milwaukee Tool **June 2020 – August 2020, June 2021 – August 2021**

- Worked with the Drilling & Fastening, Outdoor Power Equipment team doing new product development
- Wrote efficient embedded firmware in C for microprocessors using timer and DMA peripherals and performed layouts in Altium to accommodate HW changes

Manufacturing Engineering Intern | HUSCO International **May 2019 – August 2019**

- Developed a system for monitoring high-level line statistics in real-time that decreased downtime and increased running yield by 2-4% on previously optimized lines
 - Utilized RSLinx and a SQL Server Integration Services (SSIS) package to store line data in a SQL table
 - Implemented conditional alerts through Microsoft Flow and a dashboard through Microsoft Power BI
- Developed new quality control program for Cognex ISM-1100 cameras to detect poor welds on valve bodies

Leadership & Activities

Georgia Tech Solar Racing **Team Member: September 2018 – Present**

- Managed team's social media accounts reaching 1,000+ followers **Solar Lead: August 2019 – January 2020**
- Conducted aggressive spring recruitment cycle **Outreach Lead: January 2020 – September 2021**
 - Reached 34 recruits, 5x more than Spring 2019
- Organized involvement in public-facing events including the Atlanta International Auto Show
- Led a team of 5 other students as Solar Power Systems Lead focusing on solar-related projects including a characterization study of solar cells with different damage modes using Python and MATLAB