Grant Hernandez

grant.hernandez@ufl.edu • https://hernan.de/z • https://github.com/grant-h

Education

University of Florida — Gainesville, FL (2015 - Present)
GPA: 3.83 • Ph.D. Computer Engineering — Expected Summer 2020

University of Central Florida — Orlando, FL (2011 - 2015)
GPA: 3.81, Magna Cum Laude • B.S. Computer Engineering — Awarded August 2015

Skills

Programming Languages: C, Python 3, C++03, LaTeX2ε, JavaScript, Scala, Go, Verilog, Java

Vulnerability Research

- **Tools:** IDA Pro (IDAPython), QEMU, GDB, GHIDRA, Binary Ninja, OllyDBG
- **Techniques:** Shellcoding & ROP (x86/x86_64 & ARM), ASLR bypassing, kernel exploitation
- **Fuzzing:** libFuzzer, AFL, CERT BFF/FOE
- **Special:** Firmware analysis & unpacking, binary lifting (VEX IR), SMT (Z3), symbolic execution (angr), custom emulation

Embedded Systems

- Extensive programming experience with AVR microcontrollers in C/C++
- Designed and fabricated 2-layer, SMT board with KiCAD (microcontroller, radio, and display)
- Designed full-custom VLSI gate library and CRC-32 module using Cadence and fabricated through MOSIS

Industry Experience

Google, Android Platform Security Intern — Mountain View, CA – Summer 2019

- Created a libFuzzer fuzz target for Android's MTP server, discovering a stack-based buffer overflow and a denial of service
- Discovered, triggered, and patched a denial of service USB bug in a Linux kernel driver with the help of syzkaller
- Contextualized the USB attack surface of the Android platform for the platform security team

Facebook, Security Foundation Intern — Menlo Park, CA – Summer 2014

- Extended internal 2FA PHP frontend to enable auditing and management of employee Yubikey tokens
- Crafted Python job to stream employee Duo 2FA API statistics to an internal log ingester and visualizer
- Improved C Duo Linux PAM module to become IPv6-ready and improve network timing fault tolerance
- Performed site-wide zmap/nmap scanning to assess SSH version distribution
- Built a Debian SSH package, with custom patches, to update entire $100,000+$ machine fleet using Chef

Raytheon CSI, Intern — Melbourne, FL – Summer 2013

- Engineered a multi-threaded socket protocol and logger in C on a Linux ARM development board for remote control
- Created custom wire harnesses to interface with target hardware platform and ARM development board
- Reverse engineered and extracted BGA flash memory firmware through chip-off technique
- Wrote a Python proof-of-concept exploit to demonstrate an undisclosed router command injection vulnerability

Research Experience

University of Florida, Research Assistant with FICS — Gainesville, FL – Fall 2015 - Present

- **Advisor:** Dr. Kevin R. B. Butler, **Area:** Systems security
- **Thesis:** Developing methodologies for automatically analyzing embedded binary firmware.
- Emulating cellular basebands to improve security testing and fault detection
- Performed large-scale analysis of Android firmware to explore hidden USB interfaces and examine device security policies
- Analyzed USB firmware using symbolic execution to automatically detect BadUSB devices

– Employed Intel SGX to balance Secure Function Evaluation (SFE) security with performance

Selected Publications

1. **Poster: G. Hernandez**, K. Butler. Basebads: Automated Security Analysis of Baseband Firmware. *ACM Security & Privacy in Wireless and Mobile Networks (WiSec), 2019*
2. D. Tian, **G. Hernandez**, J. Choi, V. Frost, P. Johnson, and K. Butler. LBM: A Security Framework for Peripherals within the Linux Kernel. *IEEE S&P, 2019.*
3. D. Tian, **G. Hernandez**, J. Choi, V. Frost, C. Ruales, K. Butler, P. Traynor, H. Vijayakumar, L. Harrison, A. Rahmati, and M. Grace. ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem. *USENIX Security, 2018.*
4. **G. Hernandez**, F. Fowze, D. Tian, T. Yavuz, and K. Butler. FirmUSB: Vetting USB Device Firmware using Domain Informed Symbolic Execution. *ACM CCS, 2017.*
5. **G. Hernandez**, O. Arias, D. Buentello, and Y. Jin. Smart Nest Thermostat: A Smart Spy in your Home. *Black Hat USA, 2014.*

Selected Vulnerability Disclosures

1. CVE-2019-13631 – Buffer overflow during parsing of HID report in Linux's GTCO driver (July 17, 2019) (Reported and patched)
   Writeup: https://patchwork.kernel.org/patch/11040813/
2. LVE-SMP-180001 – LG Electronics USB AT Command Vulnerability (July 2018) (Disclosed to and fixed by LG)
   Writeup: https://atcommands.org/
3. Counter Strike: Global Offensive BSP ZIP Buffer Overflow (July 19th, 2018) (Disclosed and fixed by Valve, $12,000)
   Writeup: https://blog.path.network/fuzzing-cs-go-bsp-files/
4. Counter Strike GoldSrc BSP Map Buffer Overflow (July 10th, 2017) (Disclosed and fixed by Valve)
   Writeup: https://bit.ly/2Dqo24j

Professional Services

– System Administrator for the Florida Institute of Cyber Security (FICS). Responsible for user management, patching, hardening, and monitoring 9 business-critical servers. (2015 – present)
– Helped develop, organize and run SwampCTF, a 48 hour international Capture the Flag competition, for the Student InfoSec Team (UFSIT). Built infrastructure using Ansible, Docker, AWS, and Netdata. Over 1,200 registered teams enjoyed our 28 hand-crafted cyber security challenges (March 2018, 2019).
– Founded, advised and trained the University of Florida's Collegiate Cyber Defense Team (UFCCDC) under UF's Registered Student Organization (RSO) the Student InfoSec Team (UFSIT) (2016 – 2017).

Honors & Awards

University of Florida Gainesville, FL – Fall 2015 - Present

– **Best poster:** "ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem." (*SEC Academic Conference, Apr. 2018.*)
– CISE Graduate Scholarship (2017, $1,000)
– 3rd place at the Southeast Regional Collegiate Cyber Defense Competition (SECCDC) (2017)
– **Best poster:** "FirmUSB: Vetting USB Device Firmware using Domain Informed Symbolic Execution." (*FICS Conference, Mar. 2017.*)
– Appointed as Florida Institute of National Security (FINS) Fellow (2015, $6,000)

University of Central Florida Orlando, FL – Fall 2011 - 2015

– Winner of the National Collegiate Cyber Defense Competition (NCCDC) out of 180 schools (April 2014)
– 1st place at the Southeast Regional Collegiate Cyber Defense Competition (SECCDC) (2013 and 2014)
– 6th place and 5th place at CSAW CTF finals (2013 and 2014 respectively)
– UCF President's Honor Role, 4.0 GPA (Fall 2011, Spring 2012, Fall 2012)