Grant Hernandez

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

Last updated July 30, 2020

Skills

Vulnerability Research

- **Static Analysis / Debugging:** IDA Pro (+IDAPython), GDB, GHIDRA, Binary Ninja, ImmunityDBG (+Mona)
- **Exploitation:** Shellcoding & ROP (x86/x86_64 & ARM), ASLR bypassing, kernel exploitation (Linux X86_64)
- **Fuzzing:** libFuzzer, Syzkaller, AFL, CERT BFF/FOE (custom harness)
- **Firmware Analysis:** Rehosting via QEMU / AVATAR2 (Shannon baseband), USB firmware reversing, Linux-based routers, AVR
- **Symbolic Execution:** custom CPU support in angr, custom 8051 lifter for VEX IR, interrupt support in angr
- **Scale:** Audited and diagrammed the Android platform's USB stack (platform, kernel, drivers), reversing & fuzzing Shannon baseband RTOS + 2G/3G/4G tasks (+61K functions)

Embedded Systems

- **Microcontroller:** Extensive programming experience with AVR microcontrollers in C/C++
- **Layout:** Designed and fabricated 2-layer, SMT board with KiCAD (microcontroller, radio, and display)
- **VLSI:** Designed fully-custom 0.5 μm gate library and CRC-32 module using Cadence and fabricated through MOSIS
- **RTL:** Verilog programming (synthesis on Xilinx and Altera FPGAs) - VGA driver, CRC-32, ALU
- **Hardware security:** AES power analysis, creation of hardware trojans

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

Devops: Ansible, iptables, Netdata customization, ELK Stack

Selected Vulnerability Disclosures

1. Counter Strike GoldSrc BSP Map Buffer Overflow (July 10th, 2017) (Disclosed and fixed by Valve)
   Writeup: https://hernan.de/blog/2017/07/07/lock-and-load-exploiting-counter-strike-via-bsp-map-files/
2. 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/
3. LVE-SMP-180001 – LG Electronics USB AT Command Vulnerability (July 2018) (Disclosed to and fixed by LG)
   Writeup: https://atcommands.org/
4. 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/

Employment

Qualcomm, Senior Security Engineer — San Diego, CA – July 2020 - Present

- Auditing and fuzzing modem attack surface

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

- Audited the entire USB stack of the Android platform and recommended hardening changes to the platform security team
- Created a fuzzer using libFuzzer for Android's MTP server and discovered a buffer overflow and a denial of service
- Found, reproduced, and patched a denial of service USB bug in the Linux kernel with the help of Syzkaller fuzzing

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 SI, 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

Education

University of Florida — Gainesville, FL (2015 - 2020)
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

Research Experience

University of Florida, Research Assistant with FICS — Gainesville, FL – Fall 2015 - 2020

- **Advisor:** Dr. Kevin R. B. Butler, **Area:** Systems security
- **Thesis:** Developing methodologies for automatically analyzing embedded binary firmware.
- Emulating Samsung's Shannon baseband to scale 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. Emulating Samsung's Shannon Baseband for Security Testing. *Black Hat USA, 2020.* **G. Hernandez**, M. Muench, T. Tucker, W. Zhu, H. Searle, P. Traynor, and K. Butler
2. BigMAC: Fine-Grained Policy Analysis of Android Firmware. *USENIX Security, 2020.* **G. Hernandez**, D. Tian, A. Yadav, B. Williams, and K. Butler.
3. Toward Automated Firmware Analysis in the IoT Era. *IEEE Security & Privacy (S&P Magazine), 2019.* **G. Hernandez**, F. Fowze, D. Tian, T. Yavuz, P. Traynor, and K. Butler.
4. LBM: A Security Framework for Peripherals within the Linux Kernel. *IEEE S&P, 2019.* D. Tian, **G. Hernandez**, J. Choi, V. Frost, P. Johnson, and K. Butler.
5. ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem. *USENIX Security, 2018.* D. Tian, **G. Hernandez**, J. Choi, V. Frost, C. Ruales, K. Butler, P. Traynor, H. Vijayakumar, L. Harrison, A. Rahmati, and M. Grace.
6. FirmUSB: Vetting USB Device Firmware using Domain Informed Symbolic Execution. *ACM CCS, 2017.* **G. Hernandez**, F. Fowze, D. Tian, T. Yavuz, and K. Butler.

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 (Team KnightSec - 2013 and 2014 respectively)
- UCF President's Honor Role, 4.0 GPA (Fall 2011, Spring 2012, Fall 2012)