# Grant Hernandez

grant.hernandez@ufl.edu • https://hernan.de/z
Last updated July 30, 2020

## Education

**University of Florida** — Gainesville, FL (2015 - 2020)
**GPA: 3.83** • Ph.D. Computer Engineering — Awarded August 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.
- Studied and improved the methodologies around cellular baseband security testing
- Performed large-scale analysis of Android firmware to explore hidden USB interfaces and device security policies
- Analyzed USB firmware using symbolic execution to automatically reason about device functionality
- Employed Intel SGX to balance Secure Function Evaluation (SFE) security with performance

**University of Central Florida**, Undergraduate Research Assistant — Orlando, FL – Summer 2013 - 2014

- **Advisor:** Dr. Yier Jin
- **Area:** Internet of Things security
- Discovered a USB entry point into Google's Nest Thermostat allowing full-root access
- Published findings at Black Hat USA 2014 entitled "Smart Nest Thermostat: A Smart Spy in your Home"

**University of Central Florida**, EXCEL Undergraduate Research — Orlando, FL – Spring 2013

- **Advisor:** Dr. Mingjie Lin
- **Area:** Reconfigurable Hardware
- Explored Verilog through working with a hardware JPEG decoder

## Publications & Academic Work

Academic Conferences

1. ProXray: Protocol Model Learning and Guided Firmware Analysis. *International Conference on Software Engineering (ICSE), 2020.*
   F. Fowze, D. Tian, **G. Hernandez**, K. Butler, and T. Yavuz.
2. BigMAC: Fine-Grained Policy Analysis of Android Firmware. *USENIX Security, 2020.*
   **G. Hernandez**, D. Tian, A. Yadav, B. Williams, and K. Butler.
3. Kiss from a Rogue: Evaluating Detectability of Pay-at-the-pump Card Skimmers. *IEEE S&P, 2019.*
   N. Scaife, J. Bowers, C. Peeters, **G. Hernandez**, I. N. Sherman, P. Traynor, and L. Anthony.
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. A Hybrid Approach to Secure Function Evaluation Using SGX. *ACM Asia CCS, 2019.*
   J. Choi, D. Tian, **G. Hernandez**, C. Patton, B. Mood, T. Shrimpton, and K. Butler.
6. A Practical Intel SGX Setting for Linux Containers in the Cloud. *ACM CODASPY, 2019.*
   D. Tian, J. Choi, **G. Hernandez**, P. Traynor, and K. Butler.
7. 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.

8. FirmUSB: Vetting USB Device Firmware using Domain Informed Symbolic Execution. *ACM CCS, 2017.*
   **G. Hernandez**, F. Fowze, D. Tian, T. Yavuz, and K. Butler.
9. CPAC: Securing Critical Infrastructure with Cyber-Physical Access Control. *ACSAC, 2016.*
   S. Etigowni, D. Tian, **G. Hernandez**, S. Zonouz, and K. Butler.

Industry Conferences

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. *SRC TECHCON, 2019.*
   **G. Hernandez**, D. Tian, A. Yadav, B. Williams, and K. Butler.
3. Smart Nest Thermostat: A Smart Spy in your Home. *Black Hat USA, 2014.*
   **G. Hernandez**, O. Arias, D. Buentello, and Y. Jin.

Journals

1. ProXray: Protocol Model Learning and Guided Firmware Analysis. *IEEE Transactions on Software Engineering (TSE), 2019. (Also selected to appear at International Conference on Software Engineering (ICSE), 2020.)*
   F. Fowze, D. Tian, **G. Hernandez**, K. Butler, and T. Yavuz.
2. Taming the Costs of Trustworthy Provenance through Policy. *Transactions on Internet Technology (TOIT), 2016.*
   A. Bates, D. Tian, **G. Hernandez**, T. Moyer, K. Butler, and T. Jaeger.

Magazine Articles

1. 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.

Posters

1. Basebads: Automated Security Analysis of Baseband Firmware. *ACM Security & Privacy in Wireless and Mobile Networks (WiSec), 2019*
   **G. Hernandez** and K. Butler.
2. Android Escalation Paths: Building Attack-Graphs from SEAndroid Policies. *ACM Security & Privacy in Wireless and Mobile Networks (WiSec), 2018*
   **G. Hernandez** and K. Butler.
3. ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem. *SEC Academic Conference, Apr. 2018.* (**Best Poster**)
   **G. Hernandez**, D. Tian, J. Choi, V. Frost, C. Ruales, K. Butler, P. Traynor, H. Vijayakumar, L. Harrison, A. Rahmati, and M. Grace.
4. ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem. *FICS Conference, Mar. 2018.*
   Same as above.
5. FirmUSB: Vetting USB Device Firmware using Domain Informed Symbolic Execution. *FICS Conference, Mar. 2017.* (**Best Poster**)
   **G. Hernandez**, F. Fowze, D. Tian, C. Metcalf, T. Yavuz, and K. Butler.
6. SSL Certificate Verification Enhancements for the Server. *FICS Conference, 2016*
   **G. Hernandez**, A. Bates, and K. Butler.
7. Smart Nest Thermostat: A Smart Spy in your Home. *UCF Showcase for Undergraduate Research, 2015*
   **G. Hernandez** and Y. Jin.

Workshops

1. Efficient and Secure Template Blinding for Biometric Authentication. *Proceedings of the IEEE Workshop on Security and Privacy in the Cloud (SPC), 2016.*
   S. Deshmukh, H. Carter, **G. Hernandez**, P. Traynor, and K. Butler.

## Academic Service

Program Chair Assistant

– *Network & Distributed System Security Symposium* (NDSS) – 2017
  Assisted Ari Juels with recording HotCRP accept/reject decisions, limiting paper discussion time, and synchronizing dual-track PC meeting via custom spreadsheet.

External Reviewer

- *IEEE Symposium on Security & Privacy* (Oakland, S&P) – 2017
- *USENIX Security Symposium* (USENIX Security) – 2017, 2018
- *ACM Conference on Computer and Communications Security* (CCS) – 2016, 2017
- *ACM Asia Conference on Computer and Communications Security* (AsiaCCS) – 2017, 2018
- *Annual Computer Security Applications Conference* (ACSAC) – 2017
- *Network & Distributed System Security Symposium* (NDSS) – 2017, 2018
- *USENIX Symposium on Operating Systems Design and Implementation* (OSDI) – 2016
- *USENIX Workshop on Offensive Technologies Workshop on Offensive Technologies* (WOOT) – 2016, 2017

## 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).
- 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).
  **Reference**: Dr. Joseph Wilson (jnw@cise.ufl.edu)

## Academic Honors & Awards

**University of Florida** Gainesville, FL – Fall 2015 - 2020

- **Best poster:** "ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem." (*SEC Academic Conference, Apr. 2018.*)
- CISE Graduate Scholarship (2017)
- 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.*)
- Harris Communication Fellowship (2015)
- Appointed as Florida Institute of National Security (FINS) Fellow (2015)
- Graduate School Fellowship Award (2015 - 2019)

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

- ICubed ($I^3$) Fellow - presented Nest security research to an Advanced Painting class, inspiring their work (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)
- 2nd place at the UCONN CyberSEED Buffer Overflow competition (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)
- EXCEL Student - NSF STEM only education program with guaranteed Sophomore year research (2011 - 2013)
- 1st place at UCF's 25th annual High School Programming Tournament (2010)

## 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 communication protocol and logger in C on an ARM development board for a project demo
- 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

## Disclosures

1. CVE-2019-13631 – Buffer overflow during parsing of HID report in Linux's GTCO driver (July 17, 2019)
   **Status:** Reported and patched
   **Report:** https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13631
   **Writeup:** https://patchwork.kernel.org/patch/11040813/
2. LVE-SMP-180001 – LG Electronics USB AT Command Vulnerability (July 2018)
   **Status:** Disclosed to and fixed by LG
   **Report:** https://lgsecurity.lge.com/security_updates.html (SMR-JUL-2018)
   **Writeup:** https://atcommands.org/
3. Counter Strike: Global Offensive BSP ZIP Buffer Overflow (July 19th, 2018)
   **Status:** Disclosed to Hackerone and fixed by Valve
   **Report:** https://hackerone.com/reports/351014
   **Writeup:** https://blog.path.network/fuzzing-cs-go-bsp-files/
4. Counter Strike GoldSrc BSP Map Buffer Overflow (July 10th, 2017)
   **Status:** Disclosed to and fixed by Valve
   **Writeup:** https://bit.ly/2Dqo24j

## Press

1. "AT Command Hitch Leaves Android Phones Open to Attack"
   — ThreatPost (Quoted, August 27th, 2018)
2. "Smartphone security risk compared to 'having a ghost user on your phone' "
   — University of Florida News (Quoted, August 22nd, 2018)
3. "University Alabama Wins 2018 SEC Student Cyber Challenge Competition"
   — SECU News, Auburn, AL (Mentioned for poster competition, April 9th, 2018)
4. "Students Place Third in Cyber Defense Competition"
   — Computer & Information Science & Engineering News, University of Florida (Quoted, April 10th, 2017)
5. "CISE Students Win at 2017 FICS Research Conference on Cybersecurity"
   — Computer & Information Science & Engineering News, University of Florida (Quoted, April 3rd, 2017)
6. "17 ways the Internet of Things can go horribly wrong"
   — ZDNet (Mentioned, March 21st, 2016)
7. "UCF Cyber Defense Turns Smart Thermostat Into Potential Spy"
   — UCF Today (Mentioned, August 11th, 2014)
8. "A used thermostat could hack your house"
   — CNN Money (Interviewed (video), August 7th, 2014)
9. "Is your Watch or Thermostat a Spy? Cybersecurity Firms are on it"
   — NPR - All Things Considered (Interviewed (voice), August 6th, 2014)

10. “Nest Hackers Will Offer Tool To Keep The Google-Owned Company From Getting Users’ Data”
    — Forbes Tech (Interviewed, July 16th, 2014)
11. “UCF wins Raytheon cyber defense contest”
    — Orlando Sentinel (Mentioned, April 28th, 2014)

## Bonus

– I’m a licensed amateur radio operator – KK4QIS