Josh Rabinowitz

Chicago, IL 60647 | **(847) 650-5057** | **jrabinowitz2@gmail.com** | **w: jrabinowitz2.github.io**

SKILLS

- Administering and securing operating systems including Linux (Ubuntu, Kali, Mint, CentOS), OS X, Windows, Android; virtualization using VMware, Virtualbox; configuring production level enterprise networks using Cisco IOS (routing & security)
- Programming in Assembly, C/C++, Java, Ruby, PHP, SQL, web languages (HTML, CSS, JavaScript); scripting in Python, Bash
- Penetration testing web/mobile applications using Burp Suite, SQLmap, Nessus, dirb, Drozer, dex2jar, apktool; strong knowledge of OWASP Top 10
- Network penetration testing using nmap, Wireshark, Metasploit, netcat, scapy, openssl
- IoT & embedded security; using software/tools including U-Boot, BusyBox, Yocto, dd, binwalk, fastboot, ADB, flashrom, OpenOCD
- Interfacing with hardware/firmware using protocols such as UART, JTAG, SPI, I2C, ICSP; wireless protocols including Bluetooth, Zigbee, LoRaWAN, RF; tools including JTAGulator, Shikra, Bus Pirate, ApiMote/Killerbee, Ubertooth One, Saleae logic analyzer, oscilloscope, multimeter, digital inspection microscope
- Analog/digital signal processing, signal interception, waveguide/antenna design; Software Defined Radio using RTL-SDR, HackRF One, GQRX, GNU Radio
- PCB design, soldering, chip removal, component identification, firmware extraction/analysis, datasheet analysis; offensive tooling using EAGLE, KiCAD, DipTrace, LTSpice, Arduino, Teensy, Raspberry Pi, 3D Printing
- Reverse engineering & malware analysis using IDA Pro, Ghidra, GDB, OllyDBG, WinDBG, Radare2
- Exploit development, source code review, architecture review, fuzz-testing/RCA, fuzzer design, threat modeling, automation
- Familiar with use of cryptography in modern applications, as well as basic cryptanalysis and steganalysis tools & techniques
- Red team tools & techniques (physical security, social engineering; lockpicking, phishing, 'evil twin' attack, etc.)

PROFESSIONAL EXPERIENCE

UL, LLC *Northbrook, IL*
TS Security Analyst *October 2021-Present*

- Provide full suite of UL CAP services: Advisory, Testing & Certification based on highly-recognized UL 2900 Series of Standards
- Evaluate security of network-connectable devices including Medical, Automotive, Industrial, Smart-Home & Infrastructure using customized penetration tests
- Acquiring proficiency with high-end commercial scanning/fuzzing platforms including AppSpider, beSTORM, Coverity, Defensics, Nessus, Protecode and more
- Developed sophisticated SDR-based test bench for auditing the security of 'LoRa'/'LoRaWAN' devices
- Performed Comparitive Analysis of competing Opal (self-encrypting) SSD's from 3 leading chip manufacturers via hardware teardown, firmware extraction and reverse-engineering
- Created and oversaw week-long training courses on Hardware & Wireless Hacking for KSA, totaling 40+ hours of instruction, demonstrations and hands-on lab exercises
- Designed custom bed-of-nails test jig for 'on-chip debugging' SSD controller via proprietary JTAG connector

NCC Group *Chicago, IL*
Associate Security Consultant *June 2019-April 2021*

- Lead security assessments including penetration tests, architecture reviews, threat modeling, reverse engineering, malware analysis, staff augmentation and training, providing clients with clear, organized deliverables
- Provided services on-site and remote for wide range of clients, from small startups to 'Big Four' tech giants & major film studios
- Assisted with interview and hiring of new security consultants; developed training exercises to teach embedded security

Security Intern *February 2019-June 2019*

- Gained consulting experience, testing web/mobile applications and reporting to clients with recommended mitigations
- Conducted research on the security of a popular IoT product, crafted whitepaper documenting methodology and results
- Collaborated with seasoned security experts from across the globe and clients from a wide range of industries

Upwork *Remote*
Freelance Consultant *May 2018-August 2018*

- Tested full stack web applications for common web vulnerabilities (e.g. OWASP Top 10) and authored patches
- Interpreted results from commercial vulnerability scanners such as Nessus and ZAP, determining false positives using a mix of code review and dynamic analysis

CERTIFICATIONS & AWARDS

- Cisco CCENT Certification
- James Scholar Honors Student (UIUC)
- Illinois State Scholar

EDUCATION

DePaul University
Major: Cybersecurity; Minor: Computer Science
Relevant Coursework:
- Information Security Engineering I & II
- Host-Based Security
- Applied Networks & Security
- Telecomm/Network Sec. Practicum

University of Illinois Urbana-Champaign
Major: Electrical Engineering
Relevant Coursework:
- Computer Engineering
- Digital Signal Processing
- System Programming
- Microelectronic Circuits Lab