Jacob Shin

linkedin.com/in/jacob-shin • github.com/jshin313 • jacobshin.com • jacobshin313@gmail.com • 267 393 0368

Education

Temple University **BS in Computer Science (3.93 GPA)** Aug 2020 - May 2024

- President Scholar: Awarded a full tuition scholarship based on academic merit
- Temple Association for Computing Machinery (ACM), Temple Hack-a-Hardware / Computer Security Club, Temple Data Science Initiative (TDSI)

Skills

Programming Languages: C, C++, Python, Javascript, x86 ASM
Other: Linux, Git/Github, Tmux, (Neo)vim, Ghidra, GDB (GNU Debugger), Binary Exploitation, Basic Reverse Engineering, Wireshark, Pwntools, Nmap

Experience

Undergraduate Research Assistant **Temple University** January 2021 - Present

- Implementing a proxy to interface with the IFTTT (If This Then That) platform and IoT (Internet of Things) devices.
- Utilized Node.js and the Express Framework to implement a Service API based on the IFTTT specifications

Intern **Princeton Plasma Physics Laboratory** Oct 2019 - Dec 2019

- Designed circuitry for a Langmuir probe, a device used to measure plasma properties like density and temperature

Projects

MITRE Embedded Security Challenge (C, AES, AVR)

- Designed a custom bootloader for an Atmega microcontroller with AES-CBC encryption and HMAC verification
- Attacked bootloaders from other teams by dumping flash via JTAG after finding out that fuse bits were incorrectly setup.

TI-Authenticator: 2-Factor Authentication With a Calculator (C, HMAC, SHA1, OTP)

- Produced the first calculator app to provide rolling passcodes similar to Google Authenticator and Duo on a TI-84+ CE graphing calculator to enhanced login security via 2-Factor Authentication
- Implemented the two types of One-Time Password (OTP) algorithms from scratch based on the RFC 4226 and RFC 6238 specifications based on a custom implementation of the HMAC algorithm (for learning purposes)

Personal Blog and Capture the Flag (CTF) Security Challenge Writeups

- Described the process of reversing using Ghidra (reverse engineering tool), bypassing exploitation mitigation techniques like NX (Non-executable stack) & ASLR (Address space layout randomization), and leveraging Return Oriented Programming (ROP) to exploit a binary.
- Wrote a writeup on utilizing a tape-drive, emoji based assembly language to implement subtraction and xor from scratch with bitwise operators.

Revere Engineering Malware Lab

- Learned reverse engineering techniques for reversing malware using Malware Unicorn's free, online reverse engineering workshops (Triage Analysis, Static Analysis, and Dynamic Analysis)

Awards

CTF (Capture the Flag Computer Security Competitions):

- 1st at castorsCTF20 (out of 500) • 2nd at OwlHacks RSM CTF • 4th at MetaCTF 2020 (out of 1017) • 4th at RACTF 2020 (out of 1047)
- 25th at PicoCTF 2019 (out of 11722) • 35th at TJCTF 2019 (out of 483) • 13th at MITRECTF 2019 (out of 262)