Christopher Makarem

(626) 616-4528 • x24mak@gmail.com • christopher-makarem.me

Software engineering professional with 3+ years of experience in full-stack cyber security analysis and design. Most recent and relevant work has been designing and implementing cyber-resilient firmware and device drivers.

SKILLS

Languages: Python, C, C++, Java, Ada
Scripting: JavaScript, Matlab, PowerShell, Bash
Principles: Machine Learning (TensorFlow), Covert Channel Analysis, Cryptography (OpenSSL, SRP)

Web Apps: NodeJS, Angular, React, Bootstrap
Environments: Active Directory (Mac and Windows)
└Services: ADFS, ADCS, WDS, S4B, SSL VPN SharePoint, Exchange, Cisco CME

EXPERIENCE

Software Engineer — El Segundo, CA
Raytheon ▪ Space and Airborne Systems — April 2019 – Present

- Part of a cross-departmental team that provides software assurance guidance and support for large-scale programs across business sectors.
    - Lead software architect for statefull image integrity and authentication during boot strap loading.
- Designed and implemented secure code functions to ensure data remains confidential in all states (at rest, in transit, in use) as part of an internal model-driven python-based tool.

Security Analyst (SAII – SAIII) — Santa Monica, CA
The DigiTrust Group — October 2017 – April 2019

- Identified and classified key threats to client's network environments through log collection and aggregation to allow the support of new hardware devices contributing to increased client retention
    - Created PowerShell scripts to compile and standardize different log formats
    - Performed extensive DFIR research on network traffic patterns and user behavior
- Wrote JavaScript functions to automate event handling for Security Analysts, reducing click volume and increasing productivity (60%) and turnaround time on event processing

Systems Administration Intern — Los Angeles, CA
American Computers and Engineers — June 2014 – October 2017

- Developed Active Directory Environment for Windows based systems
    - Hardened environment against standard attack vectors: Pass the hash, SMB exploits, DNS poisoning, privilege escalation via poor user access and segregation
- Deployed remote access and administration through DirectAccess and RADIUS server

PROJECTS

IOCSCAN.IO
IP address and domain threat analysis

- Custom created web application that analyzes IPs and domains to determine likelihood of malicious activity
- Designed custom heuristic algorithms to determine threat score and construct easy to interpret description

UART Linux Device Driver
UART driver implementation with Integrity-BIST for Data Communication

- Based on Surendar & Gopalakrishnan 2017 paper describing a UART implementation with data integrity
- Driver implements a series of BIST to ensure correct functionality both on local hardware and on remote hardware running the driver. Additional integrity checks are implemented at the driver level

EDUCATION

University of California, Los Angeles
Henry Samueli School of Engineering — GPA: 3.1
Bachelor of Science, Electrical Engineering — March 2019