Michael J. Simms

Indialantic, FL
msimms01@gmail.com

Summary of Qualifications

I am a software engineer with a long history in the cyber security field. My areas of expertise include secure programming, kernel and hypervisor development, network forensics, malicious code detection, and reverse engineering. I have also written some scientific applications as well as a few mobile applications and have even done a little bit of web development. I excel at leading small software development teams and research projects.

Languages	C, C++, Python, C#, Objective C, Java, LabVIEW, and x86 Assembly
APIs	Win32, Windows Kernel APIs, .NET, Qt / PySide, Cocoa / Cocoa Touch
Concepts	Software Design, Networking, Secure Programming, Reverse Engineering, Malware Analysis, Device Driver Development, and Hypervisors
Operating Systems	Windows, Linux (mostly Ubuntu), mac OS, and iOS
Program Management	Project Technical Leadership, Schedules, and Budgets

Professional Experience

nTessimal LLC, Melbourne, FL (09/2023 – Present)

- Ground floor startup

Freelance Software Developer, Melbourne, FL (04/2019 – Present, Part Time)

- Developed a Java webapp (under NDA) that controls specialty hardware, collects data, and performs a spectral analysis on x-ray data. (Java, HTML, CSS, USB)

“Fun-Employed”, Melbourne, FL (04/2018 – 4/2019)

- Studied machine learning through a combination of Coursera and personal projects. This includes implementing the Isolation Forest algorithm in Python, Rust, and C++. The python version is installable via pip.
- Other personal projects, some of which are on my GitHub page: github.com/msimms. These include, but are not limited to:
    - A password manager that syncs through the iCloud Drive (Swift)
    - A mobile cycling and strength training app that implements a live tracking and workout suggestions. (iOS, Objective C, Bluetooth, Python, Linux)
    - A web app that generates run training plans using tensorflow. (Python, Linux, cherrypy, flask)
- Got in better shape through distance running and triathlon.
- Finished home repair projects.

Forcepoint LLC, Melbourne, FL (07/2015 – 04/2018)
Senior Software Engineering Manager
Note: This was a transfer from Raytheon at the invite of senior leadership. Raytheon owned Forcepoint at this time.

- Researcher in the Forcepoint Innovation Labs.
- Responsible for the design and implementation of a malware sandbox built on a custom hypervisor. This involves managing a small team of development and quality engineers while also performing as an individual contributor. (C, C++, Assembly, Kernel Development, OpenStack)
- Responsible for timecards, expense reports, performance reviews, and general office management.

Raytheon Centers of Innovation, Melbourne, FL (04/2008 – 07/2015)
Cyber Security Engineer
Note: I was an early employee at a company called Security Innovation, Government Solutions which was sold to Raytheon in April, 2008.

- Project Engineer for all virtualization software. This role involved managing the schedule, budget, and product roadmaps while also performing as an individual contributor, establishing SCM procedures, and coordinating with QA (C, C++, Assembly, Kernel Development).
- Principal Investigator for a proof-of-concept bare metal hypervisor that detects malicious code execution in VMware ESXi. Implemented a network stack along with other OS services. (C, Hypervisors)
- Lead Engineer for malware sandbox technology. This included one detection product based on whole machine emulation and another that hooks Windows kernel functions. (C, C++, Win32, Windows Driver Development, wxWidgets, Deep Packet Inspection, Hypervisors) A web front-end was also developed using Django and Python.
- Performed malware reverse engineering exercises and supervised others doing the same.
- Responsible for the design and implementation of software for distributed software vulnerability testing. This includes a cross-platform debugging library and file fuzzers. (C++, Windows, Linux)
- Developed automated unit tests using the Google Test Framework.
- Engineering Lead with responsibility for staffing engineers, approving timecards and expense reports, conducting performance reviews, and mentoring new employees.
- Worked on several proposal teams and authored numerous white papers.
- Established a remote office in Austin, Texas (Real estate search, office lease, etc.).
- Worked several commercialization initiatives that grew from virtualization-based Corporate R&D projects, for which I was the Principal Investigator.

Security Innovation, Government Solutions, Melbourne, FL (01/2005 – 04/2008)
Software Engineer

- Ground floor startup, sold to Raytheon in April, 2008
- Developed automated vulnerability research tools. (C/C++)
- Lead engineer for a project that developed secure network routing software for a government customer. (C, C++, Windows, Linux, wxWidgets, TCP/IP sockets, AES and RSA Encryption)
- Built a web crawler that used Bayesian techniques to identify web pages that may contain malicious code. (C++)
- Worked on several proposal teams.

Harris Corporation, Melbourne, FL (05/1997 - 01/2005)
Software Engineer

- Designed and developed a COM-based messaging system and integrated it with numerous in-house and 3rd party applications. (C++, MFC, COM, C#, .NET)
- Debugged and fixed a system that encodes MP3-formatted narratives over video for use by the visually impaired. Also edited and encoded narrative audio over “It’s A Wonderful Life” for national television airing. (C++, Direct X, Adobe Premiere)

- Product Architect for STAT Console, an enterprise management tool for the STAT family of commercial network security products. Developed and managed the program schedule and was responsible for the overall software design as well as much of the coding. (UML, C++, Java, Swing)
- Designed and developed software for STAT Scanner, a commercially available vulnerability analysis tool for the Windows family of operating systems. Handled monthly product releases. Responsibilities included schedule, software design, GUI design, as well as coding. (UML, C++, COM, MFC, Win32)
- Developed LabVIEW VIs for managing GPIB and LAN-to-Serial interfaces. Prototyped LabVIEW VIs for interfacing with various hardware items, such as a Bit Error Rate Detector and an IRIG unit.
- Developed the user interface for a government command and control system. (C++, COM, Windows)
- Worked on a quick-react project in Miami, FL to resolve issues in the municipal transit software. (C)
- Coded software to control a data recorder at a satellite down-link facility while on a temporary assignment in Sunnyvale, CA. (C++, UNIX)
- Developed a Java applet that was used on the corporate intranet to manage program staffing.
- Taught C++ and LabVIEW training courses. Also mentored coworkers on these subjects.

Lockheed Martin & Sverdrup Technology, Stennis Space Center, MS (05/1993 – 04/1997)
Computer Programmer

- Reverse engineered U.S. Navy tow-tank electronics, replacing them with a software-based, real-time data acquisition system developed in LabVIEW.
- Designed and developed real-time data acquisition and analysis software to study rocket engine exhaust plumes. (C, C++, LabVIEW, Mac OS, and Windows 3.51)
- Assisted with scientific research on the spectral study of rocket engine exhaust as well as in acquiring and analyzing data from Space Shuttle Main Engine test firings.

University of New Orleans, New Orleans, LA (01/1995 - 05/1995)
Teaching Assistant

- Graded assignments and assisted students in the assembly language class.

Education

Bachelor of Science, Computer Science, May 1996
University of New Orleans, New Orleans, Louisiana

Awards

April 2010: Excellence in Engineering and Technology (EiET) - this is the highest engineering award at Raytheon, receiving for developing software to detect malicious code sent via the corporate email servers.

Patents

2017: *Technique for Hypervisor-Based Firmware Acquisition and Analysis* (US 9,785,492)
2017: *Hypervisor Based Binding of Data to Cloud Environment for Improved Security* (US 9,734,325)
2017: *Technique for Verifying Virtual Machine Integrity Using Hypervisor-Based Memory Snapshots* (US 9,696,940)
2015: *Secure Cloud Hypervisor Monitor* (US 9,146,767)
2011: *System and Method for Live Computer Forensics* (Provisional Patent)

Presentations

January 2012: DoD CyberCrime, Atlanta, GA “Full State System Extraction Using Hypervisors”

Miscellaneous

- U.S. Citizen, successfully completed the SSBI (sole-source background investigation) process

- Outside interests include: music, home renovation, running, cycling, and iOS application development