

Kevin McDermott

kevin.t.mcdermott@gmail.com

Key Skills

- Software Security
- Technical Presentations
- Technical Writing
- Application Pen Testing
- Mobile Pen Testing
- Security Consulting
- Network Pen Testing
- Software Development
- Reverse Engineering
- A passion for Cyber Security and a commitment to expanding my skillset

Work Experience

MailChimp, Atlanta, GA (Remote Employee) *November, 2016 – Present*
Application Security Engineer/Penetration Tester

- Conduct Application, API, Network, and Mobile Penetration Testing on MailChimp assets
- Conduct internal social engineering assessments, including phishing campaigns
- Assist Development teams with a CI/CD Secure-SDLC including security focused code review
- Develop and present in-depth technical talks related to security vulnerabilities to the development teams to improve overall security awareness and understanding

Coalfire Systems, Westminster, CO *August, 2015 – October, 2016*
Application Security Consultant, Coalfire Labs

- Provide Secure Software Development and Security Architecture best practice consulting services to customers throughout the entirety of the Software Development Lifecycle
- Perform application validation engagements for a variety of compliance frameworks including PCI PA DSS, HIPAA, and EPCS, from charter to final paper, including direct customer interaction guiding them through the assessment process
- Deliver in person Secure Software Development Training to customers' technical and management teams, covering topics such as security awareness, application security concepts, threat modeling, secure SDLC methodologies, OWASP Top 10, security tools, and exploitation demonstrations
- Continually update current content and develop new content for the Secure Software Development Training, including the development of custom curriculum at the request of customers
- Conduct network and application (web, native, and embedded) penetration tests
- Conduct security focused source code reviews

Northrop Grumman Corporation, Boulder, CO *June, 2012 – July, 2015*
Former Top Secret - SCI Clearance

Cyber Software Engineer II, Appia R&D Cyber Software Project

- Integrated Metasploit with an R&D project focused on full spectrum cyber operations from initial recon to post-exploitation automation
- Full SDLC on production code in Java using JMS, JSON, and PostgreSQL
- Worked directly with NGC Cyber experts to determine system requirements

Software Engineer II, Enterprise Software Labs, Sensor Exploitation Systems

- Development of a new, experimental, C++ tool to generate high fidelity simulations of missiles in flight reflecting modern sensor technology
- Introduced several software engineering best practices to the team including formal code-reviews, bug tracking, and a coding standard emphasizing C++ best practice coding style
- Implemented new functionality and enhancements to production code in C++
- As Software QA team lead, ran and analyzed nightly regression tests
- Improved nightly regression testing process by using Python to automate installation, launch, and initial analysis, reducing man-hours by 85% and condensing GBs of output down to easy-to-read HTML files showing %-error metrics
- Moderator of the Software Control Board, responsible for vetting new technologies to be brought into the business area and presenting them to Engineering Directors.
- Additionally, as Moderator of the Software Control Board, acted as a liaison between Engineering, Security, and IT

Work Experience, continued**Northrop Grumman Corporation**, continued*Cyber Software Engineer I, Classified Offensive Cyber Programs*

- Designed, developed, and tested a customer facing, multi-platform deployment tool written in Python which turned an extremely complex deployment process into an automated, self-documenting, easily reproducible, single step procedure for a very complex, modular system.
- As a member of the reverse engineering team, reverse engineered and researched software platforms of interest to our customers
- Wrote new software modules in C for a brand new, offensive-focused cyber project

Embedded Software Engineer I, TPS7x Radar, International Air Defense

- Full SDLC in C of a new Secondary Surveillance Radar on a land-based radar system, from designing required interfaces with a third-party contractor to hardware integration
- Implemented multiple tools to assist in testing and debugging the radar RTOS
- Designed a new network layout to support the addition of video and audio recording on all communications and radar targeting data

OECONNECTION, Columbus, OH*September, 2011 – May, 2012**Software Engineering Intern*

- Full SDLC on a web-based project using C# and ASP.Net on the front-end, and Java on the backend
- Developed a purposely vulnerable web application for in-house software security training

DEKA Research and Development, Manchester, NH*June, 2011 – September, 2011**Software Engineering Intern*

- FDA compliant software testing and hardware-software integration on a Class II medical device
- Developed test suites in C++ for a RTOS on an ARM7 chip
- Performed hardware-level debugging on experimental circuit-boards

Rockwell Automation, Cleveland, OH*January, 2010 – June, 2010**Software Engineering Intern*

- Developed software, tools, and unit test code in C++ for a production desktop application
- Developed a tool for HR and Engineering to automate significant portions of performance reviews
- Monitored, maintained, and evaluated nightly software unit tests

Education**The Ohio State University**, Columbus, OH**Graduation Date:** March, 2012

B.S. Electrical and Computer Engineering, Computer Engineering Concentration, Cum Laude

Industry

OWASP

Memberships

ISSA

Volunteering**Arrupe Jesuit High School**, Denver, CO

- Teach an "Intro to Programming" class in Python to students after school hours

Technical Skills**Programming Technologies:** C/C++, Python, Java, Bash, JSON, JMS, PostgreSQL**Programming Tools:** Visual Studio, Eclipse, Git, SVN, Ant, Clearcase, Clearquest, VIM**Operating Systems:** Windows, Linux (various distributions), VxWorks Tornado**Security Tools:** Metasploit, Nmap, NCat, Wireshark, tcpdump, Burp Suite, Nessus, OllyDbg, GDB, IdaPro, VMWare Workstation, Virtual Box, OWASP ZAP, Fortify, Veracode