Kevin McDermott

kevin.t.mcdermott@gmail.com

Key Skills

Application Security Subject Matter Expert

- Application Security and Software Development professional with direct experience implementing a Secure-SDLC at every stage in the SDLC, and with both agile and waterfall methodologies, in a corporate, risk-based environment
- First-hand experience identifying (through code review and manual testing), exploiting (manually and with tools), and remediating (personally and through developer education) application security vulnerabilities, including the OWASP Top Ten
- Exhaustive experience developing, implementing, tweaking, and refining Application Security procedures until they are practical for the development organization but still provide the necessary reduction in accepted risk for the company
- Practical Security Architecture experience in varied corporate environments, such as self-hosted and cloud-based applications, including risk assessments and threat modeling
- Direct experience auditing software against compliance frameworks such as PCI PA-DSS, HIPAA, and EPCS
- Teaches weekly "Security Office Hours," where more junior security employees and any other interested parties in the organization have the opportunity to learn hands on penetration testing and application security techniques
- Experienced Bug Bounty hunter on BugCrowd and HackerOne, with experience managing a private bug bounty program through BugCrowd

Breadth of Knowledge Within Cybersecurity

- Talented network and mobile penetration tester with professional experience in both domains
- Consulting experience across multiple different cybersecurity knowledge domains and compliance frameworks for clients in a wide range of industries
- Professional experience in security Incident Response
- Solid understanding of network security fundamentals
- Experience with RBAC and implementing Single Sign-On
- Experience working with Public Key Infrastructure

Articulate Communicator

- Experienced trainer developing curriculum for, as well as teaching, Security Awareness and Secure Developer Training both internally and as a consultant
- Experienced presenter routinely preparing and delivering in-depth technical talks to developers about causes of, and mitigation for, Application Security vulnerabilities
- Equally comfortable teaching non-technical people complex technical concepts in a way they can understand, diving into the weeds with developers, or providing an Executive Summary to Senior Leadership

Lifelong Learner

- Demonstrable dedication to continuing education, including the required self-education to move from a career as a developer to one in application security
- Constantly striving to stay up to date with new security developments by listening to podcasts, reading blogs, and attending conferences
- Currently studying for the CISSP and taking the OSCP on August 1, 2018

Work Experience

MailChimp, Atlanta, GA (Remote Employee) *November, 2016 – Present*

Application Security Engineer/Penetration Tester

- Assist development teams in a CI/CD environment with Secure-SDLC including architecture, design, implementation, security focused code review, and vulnerability testing using both automated tools and manual testing
- Introduce new and update outdated security policies to reflect the dynamic nature of security best practices
- Conduct Application, API, Network, and Mobile (iOS and Android) Penetration Testing on MailChimp assets
- Conduct internal social engineering assessments, including phishing campaigns
- Develop and present in-depth technical talks related to security vulnerabilities to the development teams to improve overall security awareness and understanding

Work Experience, continued

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 SDLC
- 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%
- As Moderator of the Software Control Board, acted as a liaison between Engineering, Security, and IT, and responsible for vetting new technologies to be brought into the business area and presenting them to Engineering Directors.

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

Work Experience, continued

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 Memberships

OWASP – Denver Chapter

Volunteering

Arrupe Jesuit High School, Denver, CO
- Teaches an "Intro to Programming" class to students after school hours using the Python programming language

Technical Skills

Security Processes:
Manual and Automated Penetration Testing on Networks, Applications, and Mobile, Secure SDLC, Secure Application Architecture, Security Audits, Security Compliance, Static and Dynamic Analysis, Vulnerability Assessment, Secure Source Code Review, Security Process Improvement, Security Risk Assessment, Threat Modeling, Incident Response, Security Awareness Training, Secure Software Developer Training

Programming Technologies: C/C++, Python, Java, Bash, PHP, JavaScript, HTML/CSS

Conference Attendance

Blackhat/Defcon: 2013, 2014
Derbycon: 2015, 2016, 2017
SnowFROC: 2015, 2016, 2017, 2018
B-Sides Denver: 2015, 2016, 2017, 2018
B-Sides Atlanta: 2016
OWASP AppSec EU: 2018