Andrew McKenna – Senior Security Engineer

Andrew brings a pragmatic development, security, and rich skillset to Security Innovation – he has extensive software and web development experience. Leveraging these skills, Andrew leads the company's Embedded/IoT Center of Excellence (CoE) that conducts ongoing research on emerging threats and technologies in the machine-to-machine (M2M) and internet-enabled world. This yields continual skills and methodology improvement, as well as the development tools that allow us to conduct specialized testing and provide informed remediation advice for our clients.

As a senior engineer, Andrew's primary responsibility at Security Innovation is conducting thorough software assessments for the company's clients, which often entail threat modeling, design and code review, and application penetration testing. He actively conducts research on hardware devices to better understand attack vectors and ways to reduce exposure. Additionally, Andrew is a lead developer for the company's client services portal that is deployed on Linux, developed in Django (Python), and has a complex codebase.

Andrew's deep experience as a software developer at Boeing helped him understand the challenges of integrating security activities into projects with tight deadlines and large teams. His vast knowledge of the plethora of programming languages in use today, coupled with his strong curiosity in exploit development, malware, and web exploitation, allows him to conduct security assessments through the eyes of an attacker *and* provide expert coding remediation advice to the company's clients when vulnerabilities are identified.

Andrew has broad experience in the IT Security field, as well – both from a "hands-on" perspective as well as management and policy viewpoint. He possesses pragmatic knowledge of information infrastructure at levels varying from small projects to large policy changes, and has led teams through consensus building and problem solving activities, with an emphasis on effective implementation. Andrew also honed his critical thinking and articulation skills through years of debate experience.

Personal highlights from recent Security Innovation client projects include reverse engineering a desktop application using IDA Pro disassembler and a penetration test that found vulnerabilities in both the web application being tested as well as in the Firefox browser, which were responsibly disclosed to Mozilla.

Andrew is an adjunct professor for the Information School at the University of Washington, where he's been teaching software security in the spring semester for the last several years

Experience

While at Boeing Corporation, Andrew was responsible for the design and coding of a Java based application for flammability certification and parts management for the 787 aircraft (agile development process). Specific responsibilities included managing change requests, security testing on critical application components, and vulnerability remediation. He was also responsible for creating requirements and implementing a secure, repeatable development process for the application security auditing team within the IT Product Standards group. Additionally, Andrew worked closely with the Boeing mobile security team to conduct security assessments on applications of varying levels of complexity, development languages, and frameworks.

Prior to Boeing, Andrew was a Technology Analyst for the Equities Technology Group at Goldman Sachs. While there, he designed and coded a web application to automate and centralize risk reporting which comprised of Perl, PHP, SQL, JQuery, HTML, and CSS.

Andrew further cultivated his communications and project management skills while serving as a Teaching Assistant at University of Washington. He assisted in the instruction of cyber-security and web development classes while creating and teaching hands-on labs for JavaScript enabled Web applications and other cyber-security topics. Previously at the University, he was a technology assistant responsible for IT security, reliability and maintenance for five computer labs where he maintained and configured networking equipment, servers, and desktops.

Research & Interests

To keep his skills current and relevant, Andrew regularly attends security conferences, takes specialized security courses, and completes security certifications. He also regularly reads books, whitepapers, and blogs on the various subjects including hardware hacking, software defined radio, and binary exploitation.

Andrew has performed security assessments on HSMs and conducted NFC device firmware fuzzing and testing. Additionally he created a hardware hacking learning lab framework and lessons for testing and teaching embedded security to other security professionals.

Skills & Recognitions

- Development languages: Python, Java, PHP, Ruby
- Web/IT technologies: XML, SQL, JavaScript, JQuery, HTML/CSS
- Platform: Microsoft Active Directory, Microsoft Deployment Services, Windows Server 2003, Windows Server 2008, XP, Vista, 7, and various Linux distributions
- Network: Cisco routers/switches, routing protocols, and network infrastructure
- Cisco Certified Network Associates Certification Course
- Reverse engineering and systems design
- Certifications: Offensive Security Certified Professional (OSCP), Stanford Software Security Foundations Program
- Courses: Software Exploitation via Hardware Exploits (Blackhat 2014), Software Defined Radio (Toorcon 2013), Corelan Live Win32 Exploit Development (Derbycon 2012)
- President of the University of Washington (UW) Network and Information Security Club, UW cyber forensics 2012 winning team, 2011 Deloitte Case Competition Winner, Junior Statesmen of America 18 time best speaker

Andrew earned a B.S. in Informatics and a B.A. in Political Science from the University of Washington. While pursuing his degree with a concentration in Information Security & Assurance, Andrew made Dean's List eight quarters.