Geoff Vaughan

Senior Security Engineer

Geoff is an Application & IT Security expert helping companies secure software and devices throughout all stages of development. He specializes in finding exploitable vulnerabilities in software applications as well as reverse engineering binaries to locate vulnerable code. Leveraging these skills, Geoff leads Security Innovation's Embedded/Internet of Things (IoT) Center of Excellence (CoE) which conducts ongoing research on emerging threats and technologies in the machine-to-machine (M2M) and the 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 on all things Embedded and IoT.

Additionally, his expertise span web and mobile applications, IoT devices, and numerous communication protocols. Because of his diversity of skills, Geoff is suited for testing multi-tier systems that encompass hardware in combination with stateless and stateful software.

Geoff is passionate for ensuring software is safe to use for both businesses and end-user alike. This passion drives him to continually learn new skills to help secure web applications, mobile devices, robots, infrastructure, and anything with biometrics. His strong computer science teaching background, coupled with security expertise up and down the stack, helps allows Geoff to explain complex concepts to stakeholders of varying technical levels, and helps translate that into business risk.

Intimately familiar with finding elusive vulnerabilities in modern mobile application development platforms including HTML 5, Virtual Reality (VR), and Augmented Reality (AR) frameworks. Geoff has championed several research initiatives which he has presented at conferences and universities around the world.

Geoff has a plethora of experience in industries that range from financial services, manufacturing, robotics, media, oil & gas, and healthcare. Some of the projects Geoff has led while at Security Innovation include:

- Scanning and identifying vulnerabilities on a network with over 40 million IP address
- Exploiting hardware device and mobile applications to compromise IoT devices
- Exploiting mobile fitness training applications
- Attacking applications on Apple TV and other media streaming platforms

PROFESSIONAL EXPERIENCE

Previously, Geoff was a Security Consultant with Security Compass where he led software security assessments and delivered interactive training to hundreds of software engineers. He acted as the Technical Lead for near-field communication (NFC) research, advised several large financial institutes, and managed application security assessments across all of the company's many client applications. Geoff also

published security guidelines for C-Level executives on NFC, ATM, and other payment-based platforms, helping several clients choose the right platform for their specific security and business objectives.

Prior to Security Compass, Geoff served as an educator and instructor for six years where he spearheaded instructor-led training for high schools, universities, and prisons. Primarily focused on advanced web programming and scripting class, Geoff developed more than ten curriculums to training developers and business analysts with varying degrees of technical skill and security competency. During this time, he helped students develop their skills in Python, PHP, JavaScript, HTML, and CSS through interactive lessons and rich, challenging activities all with a focus on secure coding practices.

In 2014 and 2015, Geoff designed and developed a number of technical challenges for the Battle School Initiative and presented it at ASIS 2014 and RSA 2015. The challenge involved a 6x8 foot bunker where contestants circumvented numerous security measures including lock picking, motion sensors bypass, reading data off NFC tag, and hacking a computer.

RESEARCH & SKILLS

- Application security threat modeling and enterprise application risk analysis
- Mobile application assessments and multi-deployment mobile environments
- Reverse engineering and exploitation of Android, iOS, and hardware binaries
- Cellular network and bio-metric device exploitation
- Security awareness training focused on personal security best practices and threat models
- Tor security and biometric authentication
- IMSI catchers (Stingray) detection strategies
- Threat analysis and vulnerability assessment of PAWS protocol (protocol for accessing white space database)
- Attacks on TLS encryption, injection/input fuzzing attacks, and mitigating the risks associated with these vulnerabilities
- Certificate in Advanced OSINT (Open Source Intelligence) for Social Engineers
- P1Sec training in Cellular Network Exploitation
- Programming Languages: Java, C/C++, C#, .NET, PHP, Python, JavaScript, Smali
- Web/IT technologies: XML, SQL, JavaScript, JQuery, HTML/CSS
- Linux, Metasploit, ADB, Dex2jar, SMALI, Apktool, Drozer, Jailbreaking, and Rooting of mobile devices

PRESENTATION & PUBLICATIONS

- DSS ITSEC 2016 - Security Best Practices for Regular Users
- Hackfest 2016, AltSecCon 2016, TASK Toronto - Catching IMSI Catchers
- Facebook Security@Scale – Secure Software Development
- CanSec West – Mobile Security and Exploitation Training
- OWASP Toronto – NFC exploitation
- AtlSec Con 2017 – Personal Threat Models
- CBC's The National - Demonstrated NFC hacks
- RSA 2015 – Battle School Hacker training event
- ASIS Atlanta 2014 – Battle School Hacker training event

- SC Congress Toronto 2013 and ASIS 2013 Chicago - NFC vulnerability findings
- Security Innovation - Essential Guide to Online Security
- Written and oral commentary for CBC, CTV, BNN, Vice News, Vice Motherboard, Slate Magazine, and SC Magazine

EDUCATION

Geoff holds a Masters Degree in Information Technology Security from the Ontario Institute of Technology, where he achieved top marks in his Attack and Defense, Biometrics, Cryptography, OS Security, Secure Software Development, Computer Law, Secure Network Communications, and Web Application Security courses.

Geoff also holds a B.Ed in Education from Trent University, a BSc in Computing and Computer Electronics from Wilfrid Laurier University, and an Honors Specialist in Technology In Education from Queens University