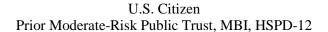# G. S. MCNAMARA, M.S.

Principal Cyber Security Engineer and Researcher, Threat Intelligence Founder, White Hat Hacker

U.S. Citizen
Prior Moderate-Risk Public Trust, MBI, HSPD-12

EDUCATION & CERTIFICATIONS

M.S. Applied Information Technology: Concentration in Intelligence Technologies 2014
B.S. Information Technology: Concentration in Information Security, Minor in Business
George Mason University: Volgenau School of Engineering, and School of Business

VMware Certified Associate - Cloud (VCA-Cloud), VMware Certified Associate - Workforce Mobility (VCA-WM), CompTIA A+, CompTIA Network+, CompTIA Security+, Data Scientist's Toolbox course from the Data Science Specialization track by Johns Hopkins University

RECOGNITION

Select articles covering independent security research and application development:
- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4958
- http://www.theregister.co.uk/2014/10/01/researcher_details_nasty_xss_flaw_in_popular_web_editor/
- http://www.theregister.co.uk/2013/11/28/thousands_of_ror_sites_leave_logins_lying_around/
- https://threatpost.com/security-issue-in-ruby-on-rails-could-expose-cookies/102413/
- https://threatpost.com/ruby-on-rails-cookiestore-vulnerability-plagues-prominent-websites/103038/
- https://threatpost.com/security-vulnerability-in-django-could-allow-attackers-access-to-cookies/102501/
- https://blog.whitehatsec.com/adding-open-source-framework-hardening-to-your-sdlc-podcast/

EXPERIENCE

Principal Cyber Engineer 2015 – Present
Forcepoint, formerly Raytheon | Websense
Founding member of the Global Product Security Incident Response Team (PSIRT). Forcepoint is the synthesis of Raytheon Cyber Products, Websense, Trusted Computer Solutions, Oakley Networks, Visual Analytics, Stonesoft, and Sidewinder.

Founder 2009 – Present
Incless LLC, formerly G. S. McNamara & Co. (DBA)
Focusing on venture projects and offering specialized IT, Web logistics, design, marketing, mobile application, SEO, and security services to clients.
- ETL of legacy contact database and operating system password override
- Design, develop, and market internal research and development projects

Founder, Application-Level Security and Threat Intelligence 2015 – 2016
Disrupt6
Disrupt6, originating from MACH37, is the source for threat intelligence and next generation security for the next generation Internet.

Senior Consultant, Application Security Engineer 2014 – 2015
CGI Federal Inc., a wholly owned U.S. operating subsidiary of CGI Group, Inc.
White hat hacker member of CGI Federal's Emerging Technologies Security Practice (ETSP) serving multiple business units.
- Researched and made recommendations based on current industry trends and extensive network of contacts
- Participated in Security Controls Assessments and audits, and the Certification and Accreditation Process
- Web application security pentesting/hacking and risk/impact/vulnerability assessments as project leader
- Guided technical remediation, research, and advised on identified vulnerabilities
- Conducted proposal and business development work

Technical Co-Founder 2013 – 2015
En Route Security LLC
Based in McLean, Virginia, En Route Security specialized in mobile personal security for iOS and Android.
- Device-agnostic application development using PhoneGap / Apache Cordova
- Mobile backend as a service (MBaaS) development

Senior Consultant, Senior Analyst, Web Applications Developer 2012 – 2014
Communications Training Analysis Corp. (CTAC)
Designed, developed, and deployed Ruby on Rails MVC framework and Drupal applications with REST API architecture for federal clients in an Agile and DevOps environment. Planned, executed, and supervised the immediate or overnight implementation and deployment to a cloud environment acting as a systems administrator. Independently received, evaluated, and responded to security vulnerability reports, then implemented fixes. Communicated lessons learned back to development team and client for secure coding best practice development.
- Object-oriented business logic implementation, database design, and object-relational mapping (ORM)
- JavaScript, AJAX, API interaction, and error handling using HTTP status codes and JSON responses
- Apache Solr (Apache Lucene) open source enterprise search platform integration
- Basic FISMA and FedRAMP familiarity

Research Engineer / Intern (extension) 2010 – 2012
Invincea Labs, Invincea, Inc.
Researched and demonstrated zero-day exploits. Research projects included the DARPA CyNomiX Cyber Genome Program, NetGator network proxy-based malware detection for the Army Research Office, DLL hijacking, and malicious PDFs and Microsoft Office documents. Interfaced with research team at Center for Secure Information Systems at George Mason University as well as our partner product development team.
- Created project Paladin: Implemented a Python-based system of distributed, isolated clients testing tens of thousands of potentially-malicious URLs supplied by Google SafeBrowsing API daily against Invincea secure web browser. Recorded and synced all results in local and remote databases, managing state.
- Developed an online Labs Portal to provide real-time information and malicious in-the-wild exploit examples to distributed sales and marketing teams and VIP customers.
- Assisted in design and implementation of end-to-end, multiphase, parallel system of servers to process 3 terabytes of malware for Cyber Genome using multi-threaded Python programming
- Programmatically cataloged malware sets from different sources using industry antivirus labels and taxonomy
- Worked with sandboxes and virtual machines using VMware, VirtualBox, Sandboxie

Software Development / Quality Assurance Intern (summer) 2010 – 2010
Invincea, Inc.
Evaluated effectiveness of flagship product Invincea Browser Protection against proprietary, wild, and purchased malicious software. Examined behavior of malware, secure web browser, and host operating system, and tracked successful exploitations. Collected test results and generated security-specific quality assurance reports for review by company executives.
- Developed web application integrating Google Visualization API to display test results and host malware samples for automated access by testing framework
- Tested vulnerabilities in secure web browser and generated malicious PDFs for demonstrations
- Created and recorded demonstrations of the product in use and under attack for broadcast on CNN

Lead Web Developer and Project Manager (contract) 2009 – 2010
Copyright Resources Office, George Mason University
Designed, implemented, and tested entirely new website for the Copyright Resources Office (CRO) under the direct supervision of the University Copyright Officer. Acted as manager of the entire project.

Consultant: Tech, Social Media, and Marketing 2008 – 2012
Scott A. McNamara, M.D., and Washington ENT Group
Processed confidential patient medical records into digital form. Handled problems with the computer network and conducted research in order to advise on technical needs and problems.

MaverickBlogging.com | LinkedIn.com/in/GSMcNamara | Twitter.com/GSMcNamara | Facebook.com/GSMcNamaraMS

Automotive Electrical Systems Specialist   2008 – 2008
Graphics-N-Tints LLC
Familiarity with internal communication systems messaging protocol useful for application in securing vehicle-to-infrastructure (V2I) Department of Transportation (DOT) and autonomous vehicle Internet of Things (IoT) initiatives.

Languages	Ruby, Python, XML, JSON, CSS, PHP, SQL, Java, JavaScript, C#, HTML5
Operating Systems	Kali, Linux, OS X, Microsoft Windows, Android
Applications and Frameworks	Fortify; AppScan; Burp Suite; ASP.NET; ASP; Ruby on Rails; Django; Metasploit; Social Engineering Toolkit; VMware; VirtualBox; Wireshark; Eclipse; Apache HTTP Server; Nginx; LAMP; XAMPP; D3.js
Databases	MySQL, PostgreSQL, SQLite, Solr, MongoDB, Oracle, MS Access
Content Management Systems	WordPress, Drupal, JIRA, Redmine, Joomla, Trac, CommonSpot
APIs	Google Visualization, Twitter, VirusTotal, VMware, CANBUS, REST, Amazon Web Services (AWS)
Networking	Bro IDS, LAN/WLAN/WAN, TCP/IP, Data Encryption, Bluetooth, FTP, SMTP, POP3, IMAP, SMB, SSL, DNS, Cisco

ACTIVITIES

Guest Lecturer: Cyber Intelligence Institute, and Cyber Statecraft, The Institute of World Politics 2015 - Present

Appointed Intelligence Analyst Fellow of the Private Sector, IC Analyst-Private Sector Program, Office of the Director of National Intelligence (ODNI), and Department of Homeland Security (DHS) .... 2015 - Present

Speaker: "Cyber Intent: Cybersecurity", Security B-Sides Washington DC, and Security BSides Delaware 2015

Speaker: "The Next APT: Advanced, Persistent Tracking", (ISC)² CyberSecureGov 2015

Member, Cyber Tech Symposium Planning Committee, AFCEA Bethesda Chapter 2014

Contributor, MITRE Common Weakness Enumeration (CWE), Common Vulnerabilities and Exposures (CVE), WhiteHat Security, Inc. .... 2013 - 2014

Speaker and Contributor, NoVA Hackers .... 2013 - 2014

Council Member as well as Global & Chapter Member, DC Chapter, Internet Society (ISOC) .... 2011 - 2014

Member, Armed Forces Communications and Electronics Association (AFCEA), IEEE-GMU .... 2009 - 2014

Founding Co-President, Electrical & Computer Hacking Organization (ECHO) .... 2010 - 2013

Founding President & Webmaster, Information Society Movement (ISM) .... 2009 - 2013

President & Webmaster, Mason Entrepreneurs .... 2009 - 2013

International Panelist, Social Media Impact, Global INET 2012 - Geneva, Switzerland, Internet Society 2012

Participant, National Collegiate Cyber Defense Competition.. 2011

Panelist, Lifestyle Hacking panel, Cybersecurity in a Transparent World, George Mason University 2010

AWARDS

IEEE Student Paper and Presentation Competition 2013

Undergraduate Service Award, AIT Department, Volgenau School of Engineering 2013

Science, Mathematics, And Research for Transformation Defense Scholarship for Service Program (SMART), American Society for Engineering Education (ASEE) & Department of Defense (DoD) 2011

AFCEA NOVA Scholarship Program .... 2010 - 2013

Schorling Award, AIT Department, Volgenau School of Engineering 2009

Innovation Award, Office of Student Activities, George Mason University 2009