Ross Gibb

587-703-8837
rg@rossgibb.ca

Calgary, Alberta, Canada
Culver City, California, USA

An experienced computer security analyst and reverse engineer, with knowledge in all facets of computer security. Desiring to use analytical and research skills to protect, prevent, and mitigate computer security issues when the stakes are high.

KEY SKILLS

- Software reverse engineering, including reverse engineering sophisticated malware samples and software exploits. IDA Pro 6+, Ollydbg, and Windbg, to reverse x86/64 (PE and ELF), Flash, Java, and .NET
- Big data analytics skills including designing and writing big data queries to facilitate research and reporting. Technologies include: Hadoop Map/Reduce, Impala, Cascalog, Greenplum, and Splunk
- Knowledge of the theory of cryptographic primitives as well as practical skills with cryptographic libraries
- Digital forensics skills including disk image capture, disk image analysis, and reporting. Forensics technologies include: Paladin, Autopsy, Volatility, Kali, and Splunk
- Network penetration testing and reporting. Pen-testing technologies include: Kali, Nessus, and AppScan
- Good technical knowledge of Windows, Linux, AIX, Solaris and other System V based UNIX operating systems including system APIs, securing the OS, setup, tuning, and day-to-day system administration
- Enterprise programming experience with Python, Clojure, SQL, Java (J2SE and J2EE), C/C++, x86/64 assembly, JavaScript/ECMA Script, and Bash
- Project management and enterprise IT architecture experience from designing and deploying enterprise Identity Management solutions
- Very proficient at producing high quality written technical communication. Experience speaking in front of groups from presenting research at industry conferences, and mentoring computer science students

WORK EXPERIENCE

Senior Threat Analyst

Symantec Corporation
Calgary, Alberta & Culver City, California
March 2011 – Present

- Designed and deployed a successful sinkhole operation against the Zeroaccess botnet resulting in the bot-master losing control of half a million computers infected with Zeroaccess. This constitutes the largest sinkhole of a peer-to-peer botnet in the history of computing. Results were presented at the 2013 Virus Bulletin Conference.
- Created accurate and exhaustive reports on numerous malware families which are presented to customers and to the public. Reports are produced by combining malware reverse engineering, big data queries, and analytic skills to fully understand and document the malware
- Improved Symantec's customer malware protection and tactical intelligence by designing and maintaining a Python software library used to monitor active malware threats. Active threat monitoring allows Symantec to pro-actively protect customers against changes to malware observed in the field

- Researching and writing of threat analysis reports for Symantec's DeepSight Threat Management System. DeepSight reports include research from reverse engineering various vulnerabilities in commercial software in order to understand them and help customers mitigate against them
- Developed solid technical writing skills from authoring highly technical threat reports

IT Security Consultant

IBM Canada
Calgary, Alberta (also at client locations across Canada and the USA)
March 2007 – March 2011

- Worked at client sites in Canada and the United States on IT security and Identity Management projects. Project tasks include: gathering requirements, designing architecture, writing custom code, and then deploying IBM software in the client's environment.
- Performed network penetration testing and web application penetration testing for clients
- Excellent troubleshooting skills from debugging and reverse engineering software issues in the field
- Project management skills from filling in for project managers to cover vacation or other absences
- Experience integrating IBM software with SAP, ACF2, RACF, CA Top Secret, HPUX, and Active Directory
- Extensive experience with IBM products including: Tivoli Identity Manager 4.6/5.x, WebSphere 5/6/7, Tivoli Directory Server 5/6, DB2 Database 8/9, AIX 5.2/5.3/6.1, Tivoli Access Manager 6

Software Developer

Xenbase, University of Calgary
Calgary, Alberta, www.xenbase.org
May 2005 – May 2006

- Worked on a team implementing an Internet based bio-informatics database for the frog genus *Xenopus*. Project funded by the National Institute of Health (USA)
- Designed and implemented architecture of Xenbase site software and parts of the database
- Technologies include: Java/J2EE, Apache Struts and IBM tools: WebSphere 5/6, DB2 8, Rational Studio 6

EDUCATION

Degree B.Sc. First Class Honours: Computer Science (Internship)
University of Calgary, May 2005, GPA: 3.68/4.00

CONFERENCE PRESENTATIONS

"Lessons learned: Sinkholing a peer-to-peer botnet" Virus Bulletin 2013. Berlin, Germany, October 2013.

PUBLICATIONS

Gibb, R. "ZeroAccess Modifies Peer-to-Peer Protocol for Resiliency" Security Response, Symantec. August 2013

Bowes JB, Snyder KA, Segerdell E, Gibb R, Jarabek C, Noumen E, Pollet N, Vize PD: **Xenbase: a Xenopus biology and genomics resource**, in: Nucleic acids research,Oxford University Press, 2007, ISBN/ISSN: 1362-4962