

George M. Jones

Active TS/SCI Clearance

7057 Wintergreen Ct., Warrenton, VA, USA 20187
Cell (540) 272-7468, e-mail: gmi@pobox.com

OBJECTIVE

To contribute to the success of the organization(s) that I work for while remaining current on network security technology and practices.

QUALIFICATIONS

- Built consensus on technical security issues at an industry-wide level.
- Experience building open source software and running group development efforts.
- Broad technical background including: Large scale networking, data center security, system and network administration, software development, database, security tools, forensic analysis.
- Policy development, monitoring and enforcement.
- Experience in a broad range of sectors: On-line Services, Tier-1 ISP, Banking, Government.

PROFESSIONAL EXPERIENCE

Lead Information Systems Engineer

MITRE Corp., McLean, VA, USA 2003 – Present

- Principal Investigator on an R&D project exploring application identification combining “netflow” and machine learning.
- Initiated a consulting effort to evaluate and improve MITREs internal security.
- Lead evaluation of tools for performing full packet capture and security analysis.
- Lead a team performing DoD C&A and deployment of Sourcefire Intrusion Detection System.
- Developed white paper evaluating DNSSEC deployment options
- Updated Security Information Manager (SIM) requirements document
- Performed R&D for a major federal law enforcement agency and MITRE.
- Performed forensic analysis using open source tools (PyFlag, Sleuthkit).
- Performed system requirements and performance analysis (DNS and Internet protocols, applications of cryptography, Solaris, ZFS, Linux).
- Represented sponsor in government and international forums.
- Coordinated an internal technical forum on security topics.

Senior Network Security Engineer, Web Hosting

UUNET, Columbus, OH, USA 2000-2003

- Actively monitored security of 200+ routers and switches in 20 data centers.
- Lab testing of networking hardware for security features (stress testing, feature testing, load testing, vulnerability testing, etc.)
- Monitor vulnerabilities and threats to web hosting infrastructure
- Tool evaluation (network scanners, testing equipment, exploits)
- Interface with data center managers, network engineers, product management, backbone security.
- On-site security audits and policy development
- Provide leadership and direction within web hosting group.

IT Architect, Information Security

BankOne, Columbus, OH, USA 1999

- Created internal Computer Emergency Response Team (CERT)
- Authored web server Minimum Security Baseline (MSB)

Software Engineer/Network Security Engineer

CompuServe, Inc., Columbus, OH, USA 1992-1998

- Developed application communication library and servers (similar to Unix inetd)
- Wrote a web browser and other Internet gateway applications.
- Developed dial-up log collection and reporting system using MySQL, Perl and Apache.
- Drafted security policies, active in incident response, active in FIRST, working with other ISPs.

RECOGNITION

- Appointed “Technical Advisor” to the OPSEC working group by the IETF (the Internet standards body). This was done in recognition of my contributions in editing RFC3871. In this role I developed the working group charter, wrote the framework that guided the efforts of the working group and provided feedback to document authors.
- Appointed “Consensus Coordinator” by SANS/The Center for Internet Security. In this roll I coordinated the development of minimum security configuration standards for Cisco IOS Routers and Catalyst switches. I coordinated input from government (NSA, DISA), operators (UUNET/Verizon, Sprint, Qwest, etc.) and vendors (Cisco, Juniper).

SELECTED PUBLICATIONS

- Editor of IETF RFC 3871 (<http://www.ietf.org/rfc/rfc3871.txt>) “Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure
- <http://www.usenix.org/publications/login/2002-12/pdfs/jones.pdf> “The Case For Network Infrastructure Security”

SELECTED TALKS

- RSA Security 2005 “Operational Security Requirements for IP Network Infrastructure”
- NANOG 29: “Knobs, Levers, Dials and Switches: Now and Then”
<http://www.nanog.org/meetings/nanog29/presentations/jones.pdf>
- IETF Security Area Advisory Group Invited Talk, July 2003
- SANS Webcast: “Improving Router Security with RAT: The Top 10 List”
<https://www.sans.org/webcasts/show.php?webcastid=90421>
- SANS Webcast: “Router Audit Tool and Benchmark”
<https://www.sans.org/webcasts/show.php?webcastid=90463>

OPEN SOURCE TOOLS

- Developed the Router Audit Tool (RAT) and associated rules with cooperation from SANS, NSA, Cisco and others. RAT is a configuration checker for Cisco IOS and Catalyst devices implemented in Perl. Published as open source tool: (<http://ncat.sourceforge.net/>).
- Multiple contributions and bug fixes submitted to PyFLAG (<http://www.pyflag.net>), a Forensics and Log Analysis tool implemented in Python. Implemented Regular Expression Searching, improved keyword search, improved loading of encase images.

EDUCATION & ACTIVITIES

- BS, Computer and Information Science, The Ohio State University
- Graduate work in Computer and Information Science, The Ohio State University
- Active in IETF OPSEC working group (www.ietf.org)