

Objective

A life-long learning opportunity in Information Systems Security where proven experience, technical team leadership, and excellent problem solving skills can be utilized to design, implement, and operate secure network solutions.

Background Summary

Information Systems Security Professional with extensive experience in designing, implementing and operating secure network solutions.

- Extensive experience in network, and information security, communications and operating system design in an enterprise environment.
- Strong skills in firewall management, network perimeter protection, TCP/IP, and secure network architecture.
- A number of security certifications, with formal training in all aspects of information security.
- Active member of the SANS Institute, a non-profit information security research and training organization.
- Perennial peak performer with strong organizational, technical team leadership and project management skills. Three divisional awards of excellence, and a number of other excellence awards.

Professional Experience

SaskTel (Saskatchewan Telecommunications)

2004-Present

Technical Analyst – Security, SaskTel Corporate Security

Exciting role involving corporate compliance and

- Security consulting for corporate e-commerce and Internet facing products.
- Establishment of policies, procedures and best practices for use by a Computer Incident Response Team
- Security assessments and penetration testing for pre-production and production services.
- Technology assessment for IPS products.

CGI Information Systems & Management Consultants

2002-2004

Security Architect, Information Security Center of Expertise

Challenging role involving the architecture and implementation of security solutions for contracts of various sizes.

- Security Architect for a Federal Government Department. Designed a security overlay to permit transport of classified information over a non-classified network.
- Security analyst for Secure Channel project. Performed a detailed analysis of the existing security infrastructure. Documented the existing implementation with an emphasis on security gaps and recommended future improvements.
- Worked as security architect for a Federal Government Crown Institution. Designed security components involving all aspects of infrastructure security.

SANS (SysAdmin, Audit, Network, Security) Institute

2002-Present

The SANS Institute (<http://www.sans.org>) is a non-profit research, training, and certification organization for information system security professionals. I am active with the SANS Institute, both in paid and volunteer capacities, and have had the pleasure of being involved in several training, certification and research activities.

GIAC Security Essentials Certification (GSEC): Course Notes revision

Performed editorial review, rewrote certain sections, and wrote new material for the GIAC Security Essentials Certification course notes.

GCFW (GIAC Certified Firewall Analyst) Certification Advisory Board

Participate and provide input to evolution and direction of the SANS GCFW certification.

GSEC (GIAC Security Essentials) Certification Advisory Board

Participate and provide input to evolution and direction of the SANS GSEC certification.

Grader GCFW (GIAC Certified Firewall Analyst)

Grade practical assignments and provide feedback for students seeking GCFW certification. Provide input to changes to the certification practical assignment.

Technical Reviewer, OpenSSH: A Survival Guide for Secure Shell Handling

Provided editorial input and technical review for the creation of the SANS SSH Step-By-Step book. This book describes what secure shell (SSH) is, and provides deployment and usage instructions for system administrators.

GCFW (GIAC Certified Firewall Analyst) Local Mentor

Provide classroom instruction as a local mentor for the SANS GIAC Certified Firewall Analyst (GCFW) program offered in Ottawa. For this program, the students take the course material required for the certification online. The local mentor program provides them with the opportunity to get together once a week with mentors and the other students to ask questions. Besides acting as a mentor, I managed the curriculum, prepared short presentations, presented course material, and arranged guest speakers.

Top 20 Vulnerabilities Rewrite

Participate in the annual rewrites of the SANS Top 20 Vulnerabilities document (<http://www.sans.org/top20.htm>). Responsibilities include researching vulnerabilities, recommending and voting on vulnerabilities that may be included on the revised top 20 list, writing sections of the new version of the document and providing editorial feedback for the final revision.

Nortel Networks (formerly Bell Northern Research)

1989-2002

Senior Security Analyst

1998-2002

Multi-faceted role involving architecture of secure network solutions for Internet and business-to-business applications, installation and configuration of security solutions, security audits on deployed infrastructure, evaluation of security products before deployment, rotational operational and pager support on deployed security infrastructure, including firewalls, routers, virtual private networks, dual-factor authentication, single sign-on, intrusion detection servers, and Internet FTP servers.

- Technology expert for deployed base of 50 Raptor (now Symantec Enterprise) firewalls. This deployed base had an uptime of greater than 99.5%. Also deployed firewall solutions on Checkpoint Firewall-1, Contivity Stateful Firewall and CyberGuard firewalls. Total installed base was approximately 100 firewalls.
- Designed, coded, and implemented a remote upgrade process for the deployed base of firewalls that eliminated travel required for firewall upgrades. This resulted in a 90% reduction in upgrade outage interval, a 75% reduction in manpower required to do upgrades, and an initial saving of \$250,000.
- Project manager on major upgrade to deployed firewall base. This required coordinating the work of 30 people in 9 countries. The project completed two months ahead of schedule.
- Designed, coded, and implemented a remote installation process which resulted in an 80% reduction in firewall installation interval. This process was later extended to disaster recovery scenario's thus resulting in an 80% reduction in recovery interval for catastrophic hardware failures.
- Architected solutions for implementation, installation and support of secure network perimeter. This perimeter consisted of nearly 100 firewalls deployed in 40 points of presence worldwide.
- Created an installation process for Contivity Stateful Firewalls that reduced the installation interval by 50%.
- Designed and deployed a secure business-to-business architecture that substantially increased functionality.
- Performed perimeter Security Audits on in-service infrastructure. Audits performed by external auditors revealed no audit findings.
- Provided consultation to development groups on specifications and capabilities of firewall technologies. This resulted in products that were more firewall friendly, and easier to deploy in an Internet facing environment.
- Participated in incident response of unusual activities. The biggest of these was participating in Nortel's response to the Nimda and Code Red worms.

Cellular Base Design and Support

1995-1998

Positions: Team Leader, Acting Manager

Team leader responsible for the design and support of base level code in Nortel's wireless switching product.

- Design team leader for team responsible for improving the recovery time of cellular switching product peripherals. Implemented feature decreased recovery interval for out of service peripherals by 60%.
- Design team leader and manager for a team tasked with migrating cellular code to a new operating system release. All migrations performed by this team were completed ahead of schedule with no reported problems.

Operating System Programmer

1989-1995

Positions: Operating System Programmer, Support Team Leader, Assistant Software Architect

Responsible for feature design and support of the operating system on Nortel's switching products.

- Championed a new training process intended to reduce software bugs in the design process.
- Assistant software architect responsible for approving software features and eliminating unnecessary software churn to improve software quality.
- Designed and implemented system for secure real-time communications of event logs from peripherals devices to the central core.

Education

Bachelor of Science, Computer Science

1989

University of Regina, Cooperative Education Program

Workterms:

Bell Northern Research (now Nortel Networks) – two work terms.

Shell Canada – two work terms.

Cooperators Data Services (now CGI Information Systems & Management Consultants) – two work terms.

Certifications

Global Information Assurance Certification (GIAC)

Certified Firewall Analyst (GCFW)-Honors

2001

Security Essentials (GSEC)-Honors

2004

Certified Incident Handler (GCIH)-Honors

2005

Advanced Hacker Techniques (GHTQ)-Honors

2005

Reverse Engineering Malware (GREM)-Honors

2005

Special Activities

Canadian Red Cross, Disaster Services, First Aid Provisioning Team

2002-2004

Positions: Active Member, Executive Member

Active in a volunteer organization that exists to provide primary health care to injured or sick members of the public until they may be turned over to medical services. The Canadian Red Cross provides training in standard and advanced basic trauma life support (BTLT), Cardio-Pulmonary Resuscitation (CPR), airway management, emergency management, and Automated External Defibrillation (AED).

University of Regina Alumni Branch Contact, Ottawa

1990-2004

Organize events for the University of Regina Alumni in Ottawa. Through the years I organized various events including CFL Football games, informal events such as barbeques, and events for visiting dignitaries, including the Premier of Saskatchewan in 2002, and the President of the University of Regina in 2003.

Nortel Networks Mixed Softball League

1990-2004

Positions: Commissioner, Vice President of Operations

Responsible for discipline, arbitrating disputes, as well as organizing playoff umpires, general league start-up and day-to-day management duties for one of the largest corporate softball leagues in the world.

Nortel Networks Medical Incident Response Team (MIRT)

1991-2002

Positions: Team Leader, Training Officer, Active Member

Active in a company sponsored volunteer organization that exists to provide primary health care to injured or sick employees until they may be turned over to ambulance or medical services. This organization provided training in standard and advanced basic trauma life support (BTLT), Cardio-Pulmonary Resuscitation (CPR), airway management, emergency management, pediatric emergencies, behavioral emergencies, and Automated External Defibrillation (AED).