

Paul (Tony) Watson
Email: paul@paulwatson.org

Goals and Objectives

Continue to develop my technical, professional and management talents through challenging work and continuing education.

Professional Certifications

CISSP: Certified Information System Security Professional (ISC2)
CISM: Certified Information Security Manager (ISACA)
CCSP: Cisco Certified Security Professional
CCNA: Certified Cisco Network Administrator
INFOSEC: Information Systems Security Professional
CCSE/CCSA: CheckPoint Firewall-1 Certified Engineer
MCSE+Security: Microsoft Certified Systems Engineer, Security Specialist
CVS/CIS/CFS: Cisco VPN, IDS, and Firewall Specialist

Publications and Presentations

Currently untitled talk scheduled for presentation at RSA Security Conference, 2005
"Slipping in the Window: TCP Reset Attacks", research paper and presentation, BlackHat Briefings Security Conference, 2004
"Slipping in the Window: TCP Reset Attacks", research paper and presentation, CanSecWest/Core04 Security Conference, 2004
"IPSec Interoperability", presentation, VeriSign Information Security Road show, 2001
"Using PERL for Security Applications", presentation, Usenix Security Convention, 1995
Interviewed on CBS, FOX News, CBC, TechTV regarding Infosec research
Featured in InfoSec articles by New York Times, Washington Post, San Jose Mercury, San Francisco Examiner, and many other publications

Special Awards and Achievements

Co-recipient, MIT Brunnell Award for Macro-engineering; Air Force Command Tactical Information System (CTIS)
Co-recipient, Computer Science Smithsonian Award; Iridium project

Professional Associations

ISACA - Member since November 2003
ICS2 - Member since October 2001
OSF - Open Security Foundation

Other Projects and Initiatives

Open Source Vulnerability Database (OSVDB): Founding member of project to create a comprehensive, free, unbiased, and vendor-neutral vulnerability database. Researching and documentation of security vulnerability information, testing and debugging of applications and software, community evangelist
Security News Portal: Developed web-based security and technology news aggregator providing comprehensive archive and database of security and technology related news and articles.

Skills and Abilities

- Security operations management, organization, and structure
- Security Architecture, firewall design/deployment/management, intrusion detection, investigations, forensics, secure remote access, VPN design and management, Encryption Key Management
- Extensive experience in all aspects of security operations including perimeter security, vulnerability assessment, intrusion detection, internal security, remote access, and change management
- Unix system administration and security: SunOS, Solaris, AIX, Ultrix, HP/UX, FreeBSD, NetBSD, SCO, Linux
- Extensive programming talents: Ada, C, COBOL, CGI, HTML, JAM, Pascal, PERL, PHP, Tcl/Tk, AWK/SED, SQL, Unix shell scripting
- Public Key Infrastructure deployment/management (IPSec, SSL, S/MIME) using VeriSign, Microsoft and OpenSSL CA solutions
- Microsoft Windows Active Directory administration and management
- Domain Name Service (DNS) management in large scale environments
- Cisco router, switch, PIX, and IDS configuration and deployment in high security and high availability environments
- Solid routing, switching, and network infrastructure experience
- Berkeley Sendmail installation, configuration and administration
- Experience with SS7, cellular systems, and public switched telephone network systems and architecture
- Database design, management, and programming experience

Education

- 8/96 - 5/97 Wayland Baptist University
Degree Awarded: BS in Business Administration
GPA: 3.95/4.0, Graduated with honors
- 6/93 - 8/96 Community College of the Air Force
Degree Awarded: A.A.S in Computer Science Technology
GPA: 3.9/4.0
- 1/94 - 3/96 University of Alaska
Degree Awarded: AAS
GPA: 3.9/4.0, Graduated with honors

Employment History

9/02 - Present **Rockwell Automation**
Job Title: Information Security Specialist
Responsibilities: Duties included daily operational management of global security infrastructure, ensuring availability and integrity of critical resources. Provided architecture and implementation of both innovative and traditional security solutions to meet company objectives. Responsible for development and implementation of security architecture for global financial systems. Provided team and project leadership to ensure timely delivery of projects, systems, and organizational commitments. Provided technical expertise to internal customers to ensure accurate development of requirements and work processes. Authored detailed security operations manual, covering all operational tasks, duties, and functions.

9/00 - 6/02 **VeriSign Inc.**
Job Title: Team Lead, Security Engineering Solutions
Responsibilities: Designed technical security architecture and complex engineering solutions for large Fortune 500 clients. Responsibilities included development of consulting and engineering solutions consisting of multiple components, including security, PKI, DNS, and network

architecture. Developed security policies and practices. Wrote, developed, and implemented detailed technical solution proposals. Developed new product solutions and offerings to meet market needs and provide new revenue opportunities. Provided project management and worked closely with clients to ensure successful deployment and integration of solutions. Developed and presented technical presentations at conferences and seminars. Designed, deployed, and managed Firewall, VPN, Cisco, PKI, and security research training and testing lab for field engineers.

8/99 - 9/00 **CapitalOne Financial Services**

Job Title: Senior Firewall & Security Systems Manager

Responsibilities: Managed complex computer security infrastructure to ensure 100% availability of critical financial systems in a fast paced, rapidly changing environment. Tasks included management of Firewalls, network engineering, VPN, Secure remote access, network and host based intrusion detection, virus protection, access management. Provided security consulting for internal and external organizations, training and mentoring to junior staff members, and growth and expansion strategies. Developed web-based tools to promote employee and management awareness of security issues and management and monitoring of critical systems. Developed process improvement strategies to decrease time to market for new business objectives and increase cross-departmental functionality.

5/99 - 8/99 **AppNet, Inc.**

Job Title: Senior Network & Security Engineer / Manager

Responsibilities: Design, implement, and managed secure and highly available electronic commerce data centers for commercial web hosting. Installed and managed dual OC-3 Internet connectivity while maintaining fault tolerance and high availability in internet links, routers, switches, firewalls and web hosting systems. Designed and implemented network monitoring and management, intrusion detection, secure remote access, DNS, and e-mail systems.

8/97 - 5/99 **IRIDIUM LLC**

Job Title: Senior Systems Security Manager

Responsibilities: Primary network security engineer/manager for global and corporate networks. Provided management and coordination of security related projects and efforts. Developed, documented and deployed a multi-tier global security strategy. Designed and deployed redundant, high-availability internal and external networks to support electronic commerce, electronic mail, Internet connectivity, billing systems and other critical applications. Security tasks include Firewall development, deployment and maintenance, secure remote access solutions, session and link encryption, access list development, intrusion detection, vulnerability assessments, policy development, and security training. Designed and maintained Domain name services for Internet, corporate, and global production networks, including over 40 unique domains and multiple sub-domains. Worked closely with application developers to ensure secure software solutions. Investigated and resolved suspected security incidents. Designed and maintained multiple Point-of-presence Internet connectivity and global frame relay network.

6/93 - 8/97 **United States Air Force**

Job Title: Senior Computer System Administrator / Software Engineer

Responsibilities: Senior System Administrator for NORAD Battle Management System (NBMS), Command Tactical Information System (CTIS), Battlefield Situation Display development network (BSD), Air Warfare Simulation Information Management System (AWSIMS), Rescue Coordination Center Information Management System (RMIS), Command Theatre Automated Planning System (CTAPS). Maintained Secret wide-area command and control network. Developed, implemented and ensured security and integrity of secret NBMS WAN network. Designed, developed and integrated software enhancements and fixes for NBMS systems. Performed administration and development of distributed Oracle and Sybase databases. Designed and maintained Web, DNS, and e-mail for BSD Development and RMIS offices. Frequently called upon to work with various organizations and agencies on Computer Security related tasks and projects: FBI, DOJ, OSI, AF-Warfare Information Center, and AF-CERT.

6/95 - 8/97

Anchorage Internet / Computer Security Solutions

Job Title: Owner

Description: Internet Service Provider start-up providing Internet access to individuals and businesses. Provided security assessments, consulting services, and technical expertise to business and government clients. Created and implemented custom solutions tailored to client's individual needs and concerns. Clients include Municipality of Anchorage Alaska, State of Alaska, Providence Hospital, AlaskaUSA Federal Credit Union, British Petroleum, and PetroStar Inc.

References:

Proudly presented upon request.