Scott R. Shinn

Senior Technology & Security Adviser

Information Security Systems • Business Continuity & Disaster Recovery • Policy Review and Development
Risk Assessments • Project Management • Computer Crime Investigations • Expert Testimony
Forensic Data Recovery • Intrusion Detection Systems • Enterprise Network Architecture Design • Anti-Spam Guru

Security Clearance
Last held DoD Secret security clearance in April 2002.

Work Experience

Prometheus Group, Inc.
October 2002 - Present
Managing Partner
• Architect of "Atomiclean", a dedicated anti-spam/anti-virus mail gateway server product that provides anti-spam, and virus content filtering using Bayesian and P2P anti-spam mechanisms (shared signatures). Currently deployed in several major ISP's.
• Architect of "Endstate", a data mining engine for network security vulnerability data. This engine is designed to filter out false positives based on correlating data across multiple sets to establish when data is erroneous, and in addition allow the end user to assess their vulnerability state as it changes over time.
• Provide senior operational management of on site Security Posture Assessments, Forensics Analysis and Security Design Reviews.
• Lead Senior Network Security Engineer. Responsible for managing and writing security posture assessment and data analysis tools, programs, modules and new experimental distributed engines.
• Responsible for maintaining the suite of tools used by other Network Security Engineers for conducting Security Posture Assessments (SPA).
• Conducted Security Design Reviews (SDR) for clients in order to assist them in selecting and/or designing an effective security model for their enterprise.
• Responsible for conducting security posture assessments testing of customer enterprises from an operational real world approach (modeling is a separate job function) both internally and externally to the customer's enterprise.
• Created the VoIP PBX controlling all the corporate voice communications including Cisco VoIP phones, cell forwarding, and desktop access to VoIP under both windows and

linux (gnomemeeting).

Plesk, Inc.

September 1999 – June 2003
aquired by SW Soft June 2003
Chief Technology Adviser and Director
• Determine technology direction for company
• Advise and help management make strategic technology decisions for company
• Established the international communications system with the offices in Novosibirsk, Russia, using VoIP telephony, resulting in 90% reduction in the monthly communications budget.
• Develop Security policies, and practices for product development
• Perform source code and architectural reviews for security requirements

Secure Software Solutions, Inc.

April 2001 – August 2002
Senior Application Security Engineer / Co-Founder
• Assist sales force in a Sales Engineering capacity, presenting the service offering to prospective customers
• Developed business proposals, and assisted in customer qualification.
• Maintained the corporate intranet and Cisco VoIP systems
• Technical Lead for Network Vulnerability Assessment practice
• Responsible for corporate security, including establishing and monitoring the corporate electronic perimeter

Corbett Technologies

May 2001 - April 2002
aquired by BAE Systems
Project Manager
• Assist sales force in a Sales Engineering capacity, including proposal development, and customer qualification.
• Technical Lead for a large high-profile forensics data recovery project. This included extracting data from tape media that was damaged, or stored in obsolete formats. In several cases this involved researching or reverse engineering data formats, and creating tools and methods to recover data.
• Responsible for conducting security posture assessments testing of customer enterprises from an operational real world approach (modeling is a separate job function) both internally and externally to the customer's enterprise.
• Perform Vulnerability assessments on both products, and networks in order to measure the vulnerability state of that device or network.

Shadow Group

September 2000 – April 2001
Partner and Director
Aquired by Corbett Technologies, May 2001
• Perform Forensic data recovery services, including operational forensic recovery focused on the rapid reestablishment of compromised networks in a secure fashion

• Audited Juniper Networks, JUNOS on behalf on a Network Service Provider in order to establish the security profile, and capabilities of that device as it applied to the customers network security posture.
• Established a competitive analysis service to provide high level corporate intelligence to customers in information sensitive verticals

eTantrum

July 1999 - August 2000
Chief Information Officer
• Responsible for the design and upkeep of the IT infrastructure, and physical security systems by Honeywell (CCTV, proximity badges)
• Establish cost projections to support various growth scenarios.
• Assist Sales team in projecting implementation costs and technology integration needs for customers.

Cisco Systems

March 1999 - July 1999
Senior Network Security Engineer
Signature and Exploits Development Group, Active Audit, Security Internet Services Unit
• Netranger Developer
• Write new intrusion detection signatures for Ciscos premiere Network Intrusion Detection and Response System.
• Enhance the Netranger Engine and next generation Intrusion Detection Engine.
• Netsonar Developer
• Write new security vulnerability quantification tools.
• Write new exploits to find security vulnerabilities in all Oses.

May 1998 - March 1999
Advanced Network Security Research, Active Audit, Security Internet Services Unit, Cisco Systms

• Conduct research into new vulnerabilities and attack methods against all manner of Operation Systems and network devices.
• Develop new methods for defending systems and networks against attack.

March 1998 – May 1998
• Continued position from Wheelgroup performing network vulnerability assessments.

Wheelgroup Corporation
Senior Network Security Engineer

August 1997 - March 1998
Senior Network Security Engineer
Aquired by Cisco Systems March 1998
• Provide senior operational management of on site Security Posture Assessments, Forensics Analysis and Security Design Reviews.
• Lead Senior Network Security Engineer. Responsible for managing and writing security posture assessment and data analysis tools, programs, modules and new experimental

distributed engines.
• Responsible for maintaining the suite of tools used by other Network Security Engineers for conducting Security Posture Assessments (SPA).
• Conducted Security Design Reviews (SDR) for clients in order to assist them in selecting and/or designing an effective security model for their enterprise.
• Responsible for conducting security posture assessments testing of customer enterprises from an operational real world approach (modeling is a separate job function) both internally and externally to the customer's enterprise.
• Responsible for developing, engineering and managing security requirements development, policy creation and operational implementation for Fortune 50 companies.
• Design and testing of next generation Network Intrusion Detection and Response systems.
• Testing new software and new configurations for all commercial and open source operating systems for security vulnerabilities and other security related issues.
• Conduct ongoing research into security of Operating Systems, Networks (operational and modeling), Applications and other concepts, such as designing trusted models, secure models, exploitation tools, counter measures, re-scaling models to fit threat, etc.
• Development of automated Security Posture Assessment tools, modules, scripts and engines.

United States Securities and Exchange Commission

Contractor with User Technology Associates
August 1996 - August 1997
Systems Architect at SEC
• Senior Multi-Platform Systems Administrator for UTA personnel. Platforms range from HA Solaris platforms, BSD, Linux, HP-UX, Plan 9, SunOS, and SCO to Windows NT and OS/2 Warp Platforms.
• Senior Systems Architect for UTA personnel. As a Senior member of the IS team, was involved in evaluating, selecting, testing, recommending, modifying, creating, engineering, coding and integrating new technologies and solutions into the existing infrastructure (including methods and tools).
• Responsible for penetration testing of SEC and UTA systems and access points.
• Senior architect for implementing Public Key Infrastructures, encryption, digital signature services, Certificate Authorities, evaluating COTS products, designing customized solutions, analyzing requirements and identifying, evaluating and implementing appropriate solutions.
• Responsible for engineering and implementing Internet technologies as part of the evolving SEC EDGAR Internet project.
• Responsible for developing, engineering and managing security requirements development, policy creation and operational implementation for SEC internet/intranet/extranet systems and making recommendations to other divisions for their security needs as required by contract.
• Responsible for safe guarding all SEC EDGAR filings maintained on high visibility Internet Servers open to public anonymous ftp and Web browsing.
• Building Gauntlet, Checkpoint, TIS, Alta-Vista and Custom Firewalls.
• Developing new security tools to proactively maintain the security of SEC filings data and servers.
• Testing new software and new configurations for Solaris, BSD, Linux, Plan 9, OS/2 and NT based systems.

• Database Development and engineering
• Maintaining several high end Solaris 2.5-2.5.1 Servers and their databases
• Engineering new systems and solutions

Executive Office of the President of the United States of America

The White House
June 1995 - June 1996
Computer Analyst/Network Engineer/UNIX systems Administrator
• Designed, programmed, engineered and implemented AIX 3.2.5 and 4.1 Motif Network Management system.
• Built and integrated TFTP servers into the Network Management system for maintaining the latest operating system images for all EOP Synoptics Hubs and Switches.
• Involved in internal security monitoring, and Tiger team auditing of internal EOP systems.
• Built 100 MB/Sec CAT 5 network for Office of Management and Budget.
• Systems administrator for the EOP Network Support Groups AIX, Irix, Solaris, and Linux systems.
• Trained to trouble shoot, wire, and setup heterogeneous network containing Ethernet CAT 3 all the way to 100MB/s CAT 5 twisted pair, ATM, and FDDI networks.
• Managed BOOTP server, and DHCP server for 1500 machine network.
• Developed Automatic, paging and desktop notification system for heterogeneous Netware (IPX/SPX), and TCP/IP device failures, server errors and failures, and other network problems.
• Developed, implemented and administered NetView 6000 machine to manage entire network at the White House. Wrote applications and GUIs to interact with Netview 6000, Optivity and Cisco Works.

Programming Languages

PERL - 10 Years
PHP - 5 Years
C - 6 Years
C++ - 6 Years
Python - 6 Years
Tcl/TK - 10 Years
Expect – 10 Years
UNIX Shell Programming - 12 Years
Operating Systems
10 Years of expert experience with UNIX. Including Linux, SunOS, Solaris, HP/UX, IRIX, Digital Uinx, Tru64, OSF/1, VOS, and the various BSD derivatives
5 Years of expert experience with IOS
10 Years expert experience with Microsoft OS's, including NT, 2000 and XP as well as the older derivatives, 95, 98, and ME.

Other Skills

Database Systems
Mysql - 6 Years

Sybase - 7 Years
Oracle - 7 Years
Postgres – 3 Years
Recovering data from damaged media, or unsupported data formats, including hard disks, tape drives, floppies, and CD-ROM/DVD.
Anti-Spam guru – Currently maintaining an open source Anti-Spam project called "Atomiclean" protecting over 400,000 users world-wide, and processing millions of messages per day.