Rob Havelt

+1.414.779.1302

rob {at} cobal {dot} org

Summary

Rob has devoted over 16 years to the information security industry, as a systems architect, security engineer, consultant, and director in the financial, government, automotive and telecommunications industries for such companies as SBC, Toyota, IBM and Lockheed-Martin. Although Rob has worked with clients to build complete security architectures that include policies, standards, strategies, design architectures and procedures that enable them to control security and performance on their systems, he specializes in security testing methodology, and as such continually performs testing of client systems for security concerns (Penetration Testing). As a recognized leader in this field, he strives to educate the security community about security testing and security issues through his talks and lectures and publications.

Rob has delivered multiple presentations on information security at such prestigious industry conferences as Black Hat and SANS. He has had many works published in trade periodicals in the USA, Japan, and the EU. He has been a technical editor for several security publications from the Cisco Press. His work is chronicled in various security books, and he is working own book "The Art and Science of Ethical Hacking", which is due out soon. Rob's latest speaking appearance was at ToorCon 11 in San Diego where he added to research presented at the 2009 European Black Hat Briefings speaking about frequency hopping wireless network attack techniques. One can read articles about the significance of Rob's recent Black Hat talk in Infosecurity Magazine, The Register, and other prominent technical publications.

Experience and Expertise

- **Information Security Testing -** Performed Vulnerability and Penetration Tests numbering in the hundreds for organizations in the financial, educational, manufacturing, healthcare, and other industries with an extraordinary success rate. His work with Penetration Testing and social engineering is chronicled by interviewers in popular magazines, trade publications, and books, and has been taught to peers numbering in the thousands through his own "Hacking" lecture series. This year alone, he has presented on attack techniques at ToorCon and Black Hat Briefings. He is currently writing a book with the working title "The Art and Science of Ethical Hacking" which will be a definitive reference on Penetration Testing methodology.
- **Networking** - Has designed, assessed, redesigned, and implemented large TCP/IP and even SNA based networks for multiple organizations across industries. Designed large scale and complex BGP, EIGRP, and IGP dynamically routed networks, using high availability, load balancing, and redundancy protocols. He has architected standard solutions for dynamically routed networks, Internet fail-over and load-balancing for varied organizations.
- **Firewalls** – Rob is a former Checkpoint Firewall certified instructor, as well as a certified professional. He has also been a technical editor for the Cisco Press' CCSP study guide series, and has provided technical expertise and feedback on the Cisco PIX platform; he has worked with other platforms such as Net screen, Watch guard, Raptor, IBM SNG, and others going back to the TIS toolkit.

- **Intrusion Detection** - Has designed and implemented both host and network based Intrusion Detection systems, Intrusion Prevention Systems, as well as hybrids, using such products as Source forge, Enterasys, Cisco's CSIDS and MARS, ISS, ESM, Tripwire, COPS, and nfr. He has given talks and presentations relating to Intrusion Detection methodologies for prestigious bodies such as SANS.

CAREER SUMMARY

Practice Manager, Penetration Testing - SpiderLabs, November 2005 - Present

Trustwave, Chicago, IL

I designed, built, and continue to manage the Penetration Testing practice for Trustwave's SpiderLabs. I've adjusted delivery from the largely "just me" practice to the over 24 pen testers now operating globally. I've developed service offerings across all facets of offensive security. I have and continue to streamline delivery while increasing the overall quality, value, and impact of the deliverable. I have for the past several years continuously driven the highest revenue delivery team in the consulting organization, operating at the highest gross margin.

Director of Consulting, July 2003 – November 2005

Intelligent Connections, Royal Oak, MI

I provided a lead role in multiple security consulting projects for professional services clients across a variety of sectors, including Penetration Testing, Security and Network Infrastructure design, Vulnerability Assessment, Security Policy Design, Host Auditing/Hardening/Certification, Standards and regulatory compliance. Interface with the sales team and provide pre-sales support for security and technical integration projects. Responsible for the development of Consulting Service offerings and the development of the consulting services business, while delivering services for clients. Maintain certification as a professional trainer, and both provide training for current class offerings, and help to develop new security-based training offerings.

Security Consultant, February 2002 – July 2003

Toyota Technical Center, Ann Arbor, MI

A role encompassing many security and network architecture, planning, and documentation related projects. I worked conjunction with network engineering for design and implementation of various security and network related initiatives such as TSCM specialty sweeps, network redundancy, remote engineering projects, as well as Business Continuity Planning. The scope of the project was to organize IT documentation, inventory, and procedural information to develop a full Business Continuity Plan. The main functions were to perform Business Impact and Risk Assessment, and identify critical functionality to help define metrics for continuance. Also, interact with the IT group and Engineering Administration in data gathering, document design, and development of testing methodology.

Sr. Security Consultant, July 2000 – February 2002

SBC Datacomm, Mt. Prospect, IL

Provide technical assistance to clients during all phases of security, VPN, and Internetworking projects. I managed Installation, configuration and integration of security and networking applications and hardware to support specific customer requirements. I performed customer training and knowledge transfer of security and network solutions. Provide security assessments, audits, and penetration testing in all environments.

Security Engineer, December 1999 – July 2000

Lockheed Martin/NeuStar, Chicago, IL

I was a project lead working directly under The CIO to develop full Security Policy and Procedures including Acceptable Use, Server Standards, Network Device Standards, WAN Standards, Firewall Policy, Intrusion Detection, and establish Audit Trails. My team includes technical personnel from the Networking, System Administration, Database Administration, and Applications Development departments as well as corporate legal council. I also accept the more technical responsibility of evaluation and recommendation of security products and strategies, design and systems integration into the current and any new infrastructure, Security Audit, penetration testing, technical and procedural documentation, and general security health check ups.

Security Systems Specialist, July 1997 – December 1999

IBM Global Services, Schaumburg, IL

Rob performed design, implementation, and systems integration of security systems. There I have spearheaded initiatives for large network based intrusion detection systems, host auditing, 2 factor authentication, access control, and network redundancy. I have integrated intrusion detection systems such as Netranger, Asert, and many Axent products, as well as 2 factor authentication systems (SecureID/ ACE Server) from Security Dynamics. I have worked with firewalling products from IBM, Checkpoint, and Gauntlet. Additionally, it has been my responsibility to define and enforce Security policy and Business control. I have been the point of contact for both penetration testing, and vulnerability scanning, and am adept with both commercial and freeware tools for these purposes. I am also expert in TCP/IP and SNA networking, network routing, gated, MQ, and many proxy server products, including Netscape Proxy server.

Latest Distinctions

Rob Havelt recently presented at both ToorCon 11 and Black Hat Europe in 2009, with a topic that was cause for a large amount of press coverage. See the following:

https://www.trustwave.com/pressReleases.php?n=ToorCon

http://sandiego.toorcon.org/index.php?option=com_content&task=view&id=14&Itemid=9

http://www.theregister.co.uk/2009/04/06/fhss_networks_wide_open/print.html

http://www.infosecurity-us.com/view/1264/researcher-to-blow-lid-off-secure-retail-networks/

http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=216500283

http://news.softpedia.com/news/Wireless-Networks-Belonging-to-Fortune-1000-Companies-Are-Vulnerable-108842.shtml

http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=30830&mode=thread&order=0&thold=0