

IDO DUBRAWSKY
ido@dubrawsky.org

Experience:

Microsoft, Inc.

03/06-Present

Chief Security Advisor, Communication Sector North America

Provide best practice consultation to CSO/CXO-level individuals within customers of Microsoft's Communication Sector in North America. Discuss Microsoft's security vision and roadmap under a variety of products including Windows operating system, Identity Integration and Management, ISA firewall, and general security practice. Provide feedback to product development teams on product evolution. Work with current and emerging technologies to discuss their application and integration into existing networks. In addition provide customer with subject matter expertise on a wide range of products, technologies and regulatory considerations such as identity management, PKI, HIPPA, SoX, and GLBA.

AT&T/Callisma

01/06-03/06

Acting National Practice Lead, Security Consulting

Organize security practice procedures and follow-up with business development on sales opportunities. Lead security practice and develop service delivery methodology for security services. Provide customers advanced network and network security support as an SME and trusted advisor. Continue with practice development and management.

AT&T/Callisma

11/05-03/06

Senior Network/Security Consultant, Federal Security Practice

Primary Responsibilities: Provide advanced network and network security support as a SME and trusted advisor for AT&T clients and customers. Organize, develop and manage internal training on security practices and procedures for AT&T consultants. Instruct and coordinate with AT&T sales and marketing on security consulting opportunities. Organize security practice procedures and follow-up with business development on sales opportunities. Lead security practice and develop service delivery methodology for security services.

SBC/Callisma

03/05-11/05

Senior Consultant, Federal Security Practice

Primary responsibilities: work on re-developing SBC/Callisma security practice offerings in the commercial and Federal environments. Develop internal methodologies, sales and marketing tools for InfoSec assessments. Identify and evaluate the necessary toolsets for the security practice. Project responsibilities include:

- Develop and implement InfoSec assessment methodologies utilizing the NSA's IAM methodology, OCTAVE, and ISACA's CoBIT framework.

- Consult with clients on the implementation of ITIL Governance framework, FISMA, and NIST best practices.
- Develop multi-year strategic security architecture plans for SBC/Callisma clients.
- Lead, conduct and manage InfoSec and IA security assessments including evaluation of customer readiness for HIPAA, GLBA and SOX compliance.
- Develop disaster recovery and continuity of operations plans for large government clients.

Cisco Systems, Inc.

06/04-03/05

Network Security Architect, Office of the CTO, Security Technologies Group

Primary responsibilities: Continue development of SAFE design. Provide subject matter expert support on a wide range of security technologies and Cisco security products. Project responsibilities included the following:

- Provide support for enterprise NAC deployment
- Develop best practices for Cisco Access Control Server (ACS) scalability methodologies
- Provide technical guidance on the SAFE architecture design
- Customer consultation on advanced implementations of security technologies.

Cisco Systems, Inc.

8/02-06/04

Network Security Architect, SAFE Design Architecture Group

Primary responsibilities: work in the SAFE Architecture Group in Cisco's VSEC (VPN and Security) business unit. Provide subject matter expert support to account and technical teams in security-related sales efforts. Develop and maintain training material of cutting edge Cisco technologies. Conduct research in DoS and worm mitigation methods, protocol analysis, Project responsibilities included the following:

- Research and consult on mapping policy and regulatory requirements (HIPPA, GLBA, Sarbanes-Oxley) to security technologies.
- Conduct research in Intrusion Detection Systems, firewalls, wireless, routing protocol and Layer 2 security.
- SAFE IDS and Logging project - researched and authored the SAFE: IDS and Logging in-depth white paper which focuses on in-detail considerations, design, and management of an enterprise-wide IDS deployment. Long term project was completed on-time and under budget.
- SAFE Layer 2 Security in-depth project - Project manager and lead of a team of cross-organizational individuals to research layer 2 attacks and devise attack mitigation techniques based on current switch and router technologies. Project was completed on-time and on-budget.
- Develop policy white paper focusing on the security requirements of HIPPA regulations in wireless networks
- Provide technical advice and support for Cisco Security Agent group
- Provide technical guidance on the SAFE architecture team.
- Research and design in enhancing the SAFE network architecture blueprint.

- Provide customer consultation on detailed implementations of advanced firewall, IDS/IPS, and VPN deployments including management.
- Considered a subject matter expert in Layer 2 attacks and mitigation, IDS/IPS, worm mitigation, and firewalls
- Co-authored the CCIE security written exam
- Conduct customer consultations on detailed implementations of advanced firewall, intrusion detection, intrusion prevention and VPN deployments.
- Present findings at security conferences including SANS, RSA (US and Europe).

Cisco Systems, Inc.

11/00-8/02

Network Security Engineer, Cisco Secure Consulting Services

Primary responsibilities: conduct Security Posture Assessments (SPA) of customer networks including analysis and reports of assessment to customers. Additional responsibilities included:

- Research into and development of exploits under UNIX, Windows NT/2000, and Novell operating systems.
- Develop Python, PERL, shell, and C for use in customer security posture assessments.
- Provide system administration support. Assist in installation and maintenance of test network to test exploits and new versions of Cisco SPA vulnerability scanner.
- Provide security design review of customer network designs, router and firewall configurations and provide customer with feedback regarding security implications of the design and configurations.
- Develop group procedures for forensics and Incident Containment and Response (ICR) assignments.
- Co-developed SPA wireless assessment methodology and toolset. Worked on integrating wireless assessment tools into the main branch of the group's toolset.
- Conducted security audit of internal Cisco Solaris JumpStart servers, scripts, and processes.
- Taught internal training courses on wireless assessments as well as tunneling methods into a network.

Globeset, Inc.

5/00-10/00

Team Lead, Network and UNIX Systems, Infrastructure Support

Primary responsibilities: leader and manager of internal support team responsible for administering corporate network and UNIX systems as well as corporate telephony equipment. Additional responsibilities included:

- Manage team of junior and mid-level system and network administrators
- Conduct quarterly performance reviews
- Develop quarterly and yearly budget for infrastructure requirements
- Negotiate service provider contracts for data and voice services

- Provide 24x5 third tier support for corporate servers ranging from mid-range systems (Sun Enterprise 3500) to smaller systems (Sun Enterprise 450, Enterprise 220R, Enterprise 150, Ultra 5, HP-UX, DEC Alpha)
- Provide network application support
- Design, develop, and maintain corporate intrusion detection system under tight budget
- Manage corporate network connections and infrastructure
- Migrate from flat network architecture to trunked VLANs
- Develop network security policies in conjunction with corporate management

Globeset, Inc.

12/99-5/00

Sr. UNIX Systems Administrator, Application Services

Primary responsibilities: provide third tier system and network administration support for Application Services Data Center in Sterling, VA. Responsibilities included:

- System and network administration configuration and tuning
- Support high-availability cluster of Sun Enterprise 6500 Servers running Oracle database.
- Deploy supporting network security infrastructure
- Provide technical guidance and support in security audits and security analysis of data center systems.

Other Skills: Proficient in programming in Perl, Bourne Shell, C-Shell, Python, and PHP. Experience with configuration management on production systems using RCS/CVS. Fluent in English and Hebrew.

Education

Ph.D. program, Molecular Biology University of Texas at Austin 6/95-5/98
(Antibody engineering and modeling)

M.S., Aerospace Engineering University of Texas at Austin 5/92
(Orbital mechanics and mission design and analysis)
Thesis: *Design of an Unmanned Robotic Mission to Mars*

B.S., Aerospace Engineering University of Texas at Austin 12/89

Professional Affiliations:

IEEE, IEEE Computer Society, International Association for Cryptographers, USENIX, SAGE (System Administration Guild), Tau Beta Pi (National Engineering Honor Society), Sigma Gamma Tau (National Aerospace Engineering Honor Society)

Spoken Languages:

English and Hebrew.

Citizenship:

U.S. and Israeli

Publications

Books

Dubrawsky, Ido, Building DMZs for Enterprise Networks 2nd ed., Syngress Press, Boston, MA. *In progress*

Dubrawsky, Ido and Wes Noonan, Firewall Fundamentals, Cisco Press, Boston, MA. June 2006

Dubrawsky, Ido and Paul Grey, Cisco SAFE Implementation Exam Certification Guide 2nd ed., Cisco Press, Boston, MA. December 2003.

Dubrawsky, Ido and Paul Grey, Cisco SAFE Implementation Exam Certification Guide 1st ed., Cisco Press, Boston, MA. December 2003.

White Papers

Dubrawsky, Ido, "SAFE L2 Security In-Depth, version 2", Cisco White Paper, <http://www.cisco.com/go/safe> , February 2004

Dubrawsky, Ido "SAFE Worm Mitigation", Cisco White Paper, <http://www.cisco.com/go/safe> , November 2003

Dubrawsky, Ido and Roland Seville, "SAFE: IDS and Logging in-depth", Cisco White Paper, <http://www.cisco.com/go/safe>, July 2003

Dubrawsky, Ido and Lance Hayden, "Wireless Networking: Addressing the Health Insurance Portability and Accountability Act Requirements", Cisco White Paper, http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/hipaa_wp.pdf,

Articles

"Firewall Evolution - Deep Packet Inspection" - SecurityFocus.com, August 2004

"Effects of Worms on Internet Routing Stability" - SecurityFocus.com, June 2003

"Cryptographic Filesystems - Part 2" - SecurityFocus.com, April 2003

"Cryptographic Filesystems - Part 1" - SecurityFocus.com, March 2003

"SunScreen - Part 2" - SecurityFocus.com, January 2003

"SunScreen - Part 1" - SecurityFocus.com, January 2003

"Configuring IPsec/IKE on Solaris - Part 3" - SecurityFocus.com, September 2002

"Configuring IPsec/IKE on Solaris - Part 2" - SecurityFocus.com, August 2002

"Configuring IPsec/IKE on Solaris - Part 1" - SecurityFocus.com, August 2002

Contributing Author:

Ch. 5 - *Configuring the Appliance Sensor* - Cisco Security Professional's Guide to Secure Intrusion Detection Systems, Michael Sweeney - Technical Editor, Syngress Publishing, July 2003

Ch. 10 - *Cisco Enterprise IDS Management* - Cisco Security Professional's Guide to Secure Intrusion Detection Systems, Michael Sweeney - Technical Editor, Syngress Publishing, July 2003

Ch. 10 - *DMZ Based VPN Services* - Building DMZs for Enterprise Networks, Robert Shimonski - Technical Editor, Syngress Publishing, May 2003

Ch. 1 - *Hide and Sneak* - Stealing the Network: How to Own the Box, Ryan Russell - Technical Editor, Syngress Publishing, April 2003

Ch. 4 - *Wireless* - Security+ Study Guide and DVD Training System, Robert J. Shimonski and Debra Littlejohn Shinder - Technical Editors, Syngress Publishing, December 2002

Appendix A - *Tunneling* - Hack Proofing Your Network (Electronic Edition), Ryan Russell - Technical Editor, Syngress Publishing, February 2002

Ch. 10 - *Dissecting Hacks* - Hack Proofing Sun Solaris 8, Randy Cook - Technical Editor, Syngress Publishing, November 2001

Ch. 12 - *Media Selection and Storage* - Red Hat Linux System Administration Unleashed, Caldera OpenLinux System Administration Unleashed, Tom Schenk, MacMillan Publishing, June 2000

Ch. 26 - *Firewall Strategies* - Red Hat Linux System Administration Unleashed, Caldera OpenLinux System Administration Unleashed, Tom Schenk, MacMillan Publishing, June 2000

Papers and Conferences:

"Layer 2 Security", Cisco Networkers, Cannes, France, December 2004

"Layer 2 Attacks and Defense", CSI, Washington, D.C., November 2004

"Advanced Enterprise Intrusion Detection Systems Deployment", NetSec, San Francisco, CA. June 2004

"Global Routing Instability due to Internet Worms", RSA San Francisco, San Francisco, CA., February 2004

"Realizing the Promise of Intrusion Detection Systems", Cisco Networkers, Los Angeles, CA. July 2003

"Layer 2 Security", Cisco Networkers, Orlando, FL. June 2003

"Realizing the Promise of Intrusion Detection Systems", Cisco Networkers, Orlando, FL. June 2003

"Routing Protocol Security," RSA Security Conference, San Francisco, CA., April 2003

Certifications:

Sun Certified System Administrator for Solaris 7

Cisco Certified Network Associate (CCNA)

Cisco Certified Design Associate (CCDA)

Certified Information Systems Security Professional (CISSP)

Security+

Currently working on Cisco Certified Internet Expert (CCIE) in Security

REFERENCES AVAILABLE UPON REQUEST