JONATHAN J. HART

(978) 973-0447 *http://spoofed.org jhart@spoofed.org*

Professional Summary

- Senior Systems and Security Engineer with **5+ years** of **wide-ranging professional experience**. Strong ability to quickly adapt to new environments and make an **immediate impact**. Exceptional analytical and troubleshooting skills which lead to more available, reliable and secure installations. Ultimate **team contributor** with an emphasis on success.

Experience

- **Client Confidential** — Santa Monica, CA
  Security Engineer: April 2006 - present
  -
- **Peppercoin, Inc.** — Waltham, MA
  Lead Systems and Security Engineer: February 2005 - April 2006
  - Deployed a secure and manageable network infrastructure, designed to support the next version of Peppercoin's micropayment processing software.
  - Installed, monitored and managed all corporate and production security devices, including Cisco, OpenBSD and Linux based firewalls, snort IDS, and more.
  - Used open-source software to implement an environment with a host of security features, including encryption, a secured L2 switched environment, multiple layers of firewalling and filtering, a hardened Linux installation, host and network intrusion detection as well as site-wide monitoring.
  - Designed new systems and maintained existing infrastructure while exceeding policies mandated by the Visa/Mastercard PCI/CISP regulations, thereby ensuring Peppercoin's success in becoming PCI/CISP compliant.
- **Black Dragon Software** — Lexington, MA
  Senior Security Engineer: September 2003 - December 2004
  - Aided in definition and design of a research process for data generation within a security risk modeling product, which performed simulation of security threats within a customer environment to determine security risk. United States Patent Number 20060021048
  - Lead research and development surrounding threat analysis and simulation for network software, services, protocols and policies, which included vulnerability research, documentation, and creation of attack trees to model threat relationships.
  - Designed data harvesting tools to streamline research process
  - Acted as lead liaison between R&D team and customers, partners and investors.
  - Co-authored functionality specifications and participated in design decisions for product and company development, roadmap and vision.
- **Connecterra, Inc.** — Cambridge, MA
  Systems Engineer: March 2002 - June 2003
  - Served as the primary technical lead for all company systems, including development, installation, configuration, maintenance, and security considerations.
  - Coordinated site-wide infrastructure move to new company location while eliminating downtime.
  - Acted as technical liaison for customer facing projects. Configured systems to meet project and demo requirements. Developed C, C++ and Perl code for both win32 and UNIX platforms to evaluate static and dynamic code footprint.
- **Northeastern University – College of Computer Science** — Boston, MA
  UNIX Administrator: January 2001 - June 2003
  - Deployed and manned the College's first Intrusion Detection System (IDS) using Snort running on OpenBSD sensors logging to a central MySQL database.
  - Routinely performed security assessments and penetration tests on all aspects of the the infrastructure. Audited and exploited various projects and processes, providing documentation and fixes as necessary.
  - Recommended new security policies and helped employees stay current with all pertinent security issues.
  - Developed the University's first wireless network using OpenBSD, ipf, and custom scripts to handle system functionality and security.

Knowledge

- **Tools:**

  Snort, tcpdump, Libnet, pcap, OpenBSD's pf, Linux iptables, VMware, LDAP, DNS (ISC Bind), Apache, JBoss, MySQL, Postfix, cfengine, FAI, paros, SPIKE Proxy, nikto, nmap, nessus

- **Operating Systems:**

  Linux (Debian, RedHat, Trustix, Slackware), OpenBSD, Solaris, Windows NT/XP/2000, Cisco IOS/CatOS

- **Devices:**

  Cisco PIX, Dell, SMC and Cisco IOS/CatOS based switches, Equallogic iSCSI. Ingrian, nCipher and Coyote Point hardware encryption.

- **Languages:**

  C/C++, Java, Perl, Shell, HTML, XML, Javascript

Education

- **Northeastern University** — Boston, MA
  Bachelor of Science in Computer Science (Cum Laude, 2003)
  - Associations: National Eagle Scout Association, College of Computer Science Crew, ACM

Extra-Curricular Experience

- **Published Vulnerabilities:**
  - Linksys remote memory disclosuure and DoS: CVE-2004-0580, BID-10329, OSVDB-6325
  - RealNetworks RealOne UNIX player local privilege escalation: SA9704
  - Solaris `sendfilev()` DoS POC: CVE-204-1356, BID-10202
  - Sun Solaris SMC Remote Information Disclosure: CAN-2004-1354, BID-8873