

Abstract

Enterprise security software architect and platform-agnostic software engineer with a strong inherent inclination towards Internet-based technologies at all layers of the OSI model, as well as network and physical security strategy. Wide variety and depth of experience across operating platforms and environments involving information/data security, full life-cycle software development, scalable network communication, systems management, and technical writing. Customer advocate.

Expertise and Areas of Interest

Software Design and Development Expertise

- * Advanced programming experience with C, C++ (STL/Boost), and C#; threading and synchronization
- * Advanced programming experience with network protocols and stacks (including TCP/IP, HTTP, WCF, IPv6)
- * Advanced understanding of IT networking and security; secure software design (including Threat Modeling)
- * Advanced understanding and use of secure programming practices (including SDL)
- * Experience with multi-tier architecture design, development and deployment; grid and cloud systems
- * Experience with Windows internals, Win32 and .NET system/application/UI programming; WinForms and MFC
- * Experience with UNIX-like internals, kernel development, and application programming
- * Experience with Windows Mobile/CE and .NET Compact Framework development
- * Experience with shell-style programming in Python and PowerShell
- * Experience with regular expressions (regex)
- * Experience with SQL design on platforms including SQL Server 2008, MySQL, PostgreSQL and SQLite
- * Experience with ASP.NET, PHP, UPnP, WPF, Workflow Foundation (WF), DirectX and DirectShow SDK; MCML
- * Experience with markup including XML Schema, XSLT and XPath; Windows Presentation Framework, XAML
- * Experience with COM/COM+/DCOM and .NET interoperability

Development Tools

- * *Environments:* Visual Studio 2008; vim, cl, csc, nmake (windows); vim, gcc, g++, make (unix), razzle (MSFT)
- * *Debuggers:* Visual Studio Debugger, WinDbg
- * *Change Control:* git, svn, cvs, VSTS, SharePoint
- * *Bug Tracking:* Scarab, Bugzilla, Product Studio, Ditz

Operating Systems/Protocols/Tools/Telephony

- * *Operating Systems:* Windows Server 2008 (including Hyper-V), Linux, BSD, Solaris and OS X (not inclusive)
- * *Networking:* Ethernet, 802.11, 802.1x, TCP/IP, UDP, HTTP, WAP (not inclusive), CARP, pfsync
- * *Security:* Anti-virus, Firewalls (pf, netfilter), IDS (RealSecure, Snort), Scanners (Internet Scanner, Nessus, Nmap, Queso, Netstumbler), Crypto (PGP, PKI, SSH), Sniffers (tcpdump, windump, Ethereal, NetMon)
- * *Telephony:* Basic T-carrier, CSU/DSUs
- * *Hardware:* Cisco, Bay Networks (Wellfleet), Ascent, Adtran (not inclusive)

Methodology and Interests

- * Strong interest in user interfaces, user experience and supportability
- * Strong customer drive and passion for excellence in client relationships
- * Strong interest in object-oriented design and design patterns including enterprise architectural patterns
- * Strong interest in agile and short-iterative development, TDD, frequent check-ins, and code readings

- * Strong interest in developing new ways to protect real and intangible assets (e.g. home automation)

Experience

» Principal Software Engineer and Security Consultant, July 2008 – Present (Consultant)

Independent Consultant, Seattle, WA

- * Architect, project and resource consultant for a leading security consultancy's foray into product development
- * Successfully managed the transition of the aforementioned project to a new development team
- * Successfully managed business client expectations while working in a remote office
- * Traveled to the beta customer's site (a very well known entity) in San Jose for demos and discussion
- * Successfully delivered functional work on-time through aggressive deadlines and requirement changes
- * Designed, implemented, and unit tested a web-service (SOA) using C++, gSOAP, Boost, and other 3rd party libs
- * Research included MPICH2 for use in highly available, scalable, and robust cloud computing
- * Augmented the original build and deployment design by automating the build system using GNU Make
- * Deployed an Internet-accessible partner site to enable customer deliverable staging
- * Deployed a source control system (git) and wiki to enable developer collaboration and task management
- * Implementation of custom GUI controls (cropping and track bar) in Windows in C# / VS .NET 2008.
- * Design and implementation of an SNMP sub-agent for statistics production via the AgentX protocol

» Security Software Engineer, May 2005 – July 2008 (FTE)

Microsoft Corporation, Windows Server Division, Redmond, WA

Microsoft Forefront Codename Stirling

- * Responsible for the investigation, design, and implementation of an extensible network asset discovery feature.
- * Components included work on a core engine, SDK and custom add-ins. Technologies included C#, PowerShell, Schema, SQL and WCF; leveraged asynchronous programming model for efficient threading.

Microsoft Forefront Client Security

- * Responsible for the design and implementation of a threat data import service. Data was stored in a SQL database via the OLEDB API. The service was implemented in C++ using the Win32 API.
- * Implemented an API to retrieve malware signature metadata on behalf of the UI in C#.
- * Implemented a Windows service to schedule security state assessment invocations in C++/COM+.
- * Participated in SQL schema design and implementation.
- * Performed reviews of functional design, code and threat models product-wide.
- * Contributions to patentable intellectual property

» Software Engineer and System Administrator, October 2002 – April 2005 (Consultant)

Syracuse University, Syracuse, NY

- * Leveraged Python, SQL and C development skills to develop and maintain web applications.
- * Managed customer-facing servers running BSD, Linux, MacOS X, and Windows.
- * Actively monitored network resources using Snort, tcpdump, Python and shell scripts.
- * Programmed system maintenance scripts in Python, shell and batch.
- * Attended university computing staff meetings to emphasize the importance of web application security.
- * Worked with campus secure-computing staff to help strategize their computing policy.

» Software Engineer, October 2002 – October 2004 (FTE)

Tickets.com, Syracuse, NY

- * Key developer on the ProVenueMAX (PVM) ticketing solution.
- * Developed ticket accounting system using C++, TCP/IP, SQL, XML and smart cards.
- * Developed UI controls for PVM using MFC (and GDI).

- * Established the first continuous build system for the PVM product using Python.
- * Implemented database benchmark and reporting tools for the PVM ISAM database using C++.
- * Created the engineering intranet and associated discussion lists.

» **Software Engineer, 2001-2002 (Consultant)**

SPI Dynamics, Inc., Atlanta, GA

- * Drove the company's initial investigation into web-application firewalls
- * Developed web-application firewall (WAF) prototype in C++, using Apache 1 and 2; BSD, Solaris and Windows

» **Software Engineer, March 1997 – May 2000 (FTE)**

Internet Security Systems, Inc., Atlanta, GA

- * Implemented a kernel module to thwart IP stack fingerprinting (OpenBSD, prior to the availability of pf).
- * Software developer and threat analyst for network (Internet Scanner) and host (System Scanner) vulnerability analysis engines; and network intrusion detection (RealSecure IDS) engine (Win32, C/C++, COM, TCL).
- * Implemented an online vulnerability database for the customer-facing corporate web site.
- * Network-security visualization research and prototype (Win32, MFC, GDI, DirectX)
- * Maintained portions of the corporate web site and download areas.
- * Performed vulnerability assessments and penetration testing as needed.
- * Worked on platforms including AIX, BSD, HPUX, IRIX, Linux, Netware, Solaris and Windows.
- * Evaluation of the IBM Tivoli and HP OpenView network management products

» **System Administrator, June 1996 – March 1997 (FTE)**

Dreamscape Online, Northland Communications Corporation, Syracuse, NY

- * Managed Internet connectivity, provisioning, and hardware.
- * Developed customer web applications using Perl and SQL.
- * Implemented Microsoft's ISP package, enabling Windows users to sign-up for Internet service.
- * Performed installation and maintenance of the BSD and Solaris operating environments.
- * Developed network resource monitoring system in C and Perl.
- * Collaborated on network architecture with other administrators.
- * Performed on-site service and support for corporate clients as necessary.

Professional Development/Training/Conferences

- * Threat Mitigation (Microsoft)
- * Threat Modeling and the SDL (Microsoft)
- * Software Design: Advanced (NetObjectives)
- * Developing with Design Patterns (NetObjectives)
- * Threading in C#: Building Responsive, Reliable, and Scalable Code (Wintellect)
- * Debugging Microsoft Windows Applications (Wintellect)
- * BlackHat Briefings: 2000, 2006 (Conference)
- * Hackers on Planet Earth (HOPE): 1994, 1997, 2000, 2002, 2004, 2006 (Conference)

Personal Development

- * Packet visualization and construction tool for Windows using C#/Forms (later converted to WPF)
- * SSH file manager for Windows using C++
- * Image manipulator in Windows using C++, DirectX and GDI
- * Digital audio extraction application w/ CDDDB support for BSD using C
- * SAX XML parser class for BSD and Windows using C++

- * ftp-proxy patch included in OpenBSD 3.2
- * identd user-specified token option included in OpenBSD 2.8
- * High-port DCC send for BitchX IRC client 1.0c18
- * Various ASP.NET, PHP, Python and Perl web applications
- * Various iterations of network discovery tools
- * Contacts retrieval tool for Windows Mobile
- * Password brute-force utility using Ruby

Education

University of Massachusetts at Amherst

Bachelor of Science - Computer Systems Engineering
1995-1996 (Left to pursue start-up opportunity)

State University of New York – ESC Syracuse

Bachelor of Science – Computer Science
2003-2005 (Left to join Microsoft)