

Michael Davis

Web: <http://www.datanerds.net/~mike>

E-Mail: mike@datanerds.net

Highlights

- Strong background in software development and engineering;
- Skilled at software design and analysis, focused on performance and tuning;
- Proven proficiency with most major programming languages;
- Well-versed with administration and development practices of several widely used databases;
- Comprehensive knowledge of UNIX system administration and security;
- Experienced developing software while working alone, with a team, or managing a team.

Professional

Software Engineer, 3Com Corporation, Mt. Prospect, IL Nov 2000 – Present

Languages: PERL, C++, C, Bash, SQL, T-SQL, SGML

Software: SSH, MSSQL, PostgreSQL, Clearcase, Lotus Notes

OS: Win*/x86, Linux/x86, Solaris/SPARC, FreeBSD/x86

Responsibilities:

- Manage and support a suite of PERL modules used for functionality testing.
- Manage documentation for all new Automation projects.
- Team lead for 3 other software engineers.
- Support internal Bulk VoIP Call Generation tool.
- Manage and support internal RedHat based Linux Distribution.
- Development, Code-Review, and Acceptance Testing of all software written by the Automation group.

Accomplishments:

- Created a documentation standard based on SGML for us throughout all of the Software Test Group.
- Developed Bulk VoIP Call Generator for stress testing of VoIP systems.
- Developed a suite of PERL Modules to perform functionality testing. This software was later standardized and used through out the company globally.

VP of Application Development, College Companies, Inc., Chicago, IL June 2001 – Present

Languages: C++, SQL, T-SQL, VBScript, ASP

Software: SSH, CVS/SourceSafe, MSSQL, IIS 5, Visual Interdev, QMail

OS: Win*/x86, Linux, FreeBSD/x86

Responsibilities:

- Architecture and development of the backend server systems.
- Architecture and development of the clustered load-balancing subsystems.
- Deployment, security, and ongoing maintenance of production server systems and networks.
- Management of MSSQL DB systems.
- Security and ongoing maintenance of corporate network.
- All release management pertaining to server development, including managing the source repository and developing a secure distribution system using CVS versioning.

Accomplishments:

- Chief Architect and primary developer for all major releases.
- Designed clustered and fault tolerant server environment.
- Wrote external management modules in C++ to perform external functionality of the backend systems.
- Implemented usage reports.

Chief Technical Officer, Urban Communications, Inc., Oak Forest, IL Jan 2000 – Feb 2002

Languages: C, C++, PERL, Shell, ASP, PHP

Software: MySQL, MSSQL, Visual InterDev, SSH, GNU compilers + tools, QMail, Apache, OpenLDAP, RADIUS, SGML/DocBook Cisco IOS.

OS: Win*/x86, Linux/x86, FreeBSD/x86, OpenBSD/x86

Responsibilities:

- Management of all Cisco routers using OSPF for routing.
- Management of 20+ FreeBSD servers serving 1000+ wireless and dialup customers.
- Security auditing of all servers and routers using custom written scripts and commercial scanners.
- Configuration and maintenance of Apache Web Server for 200+ domains.
- Configuration and maintenance of hub based mail cluster configured for SMTP, POP3, IMAP using MySQL based authentication.
- Network Design and development of a wireless network spanning 10+ cities.
- Manage and Coordinate activities of other programmers and network engineers including Tech Support and Billing department.
- Billing system backend management.

Accomplishments:

- Redundant Wireless Network by utilizing wireless backbones with wired backbones in a star topology with OSPF.
- Implementation and configuration of SMTP virus scanner including automatic virus definition updates.
- 99.9% uptime for Core services (SMTP, POP3, WWW)
- Development of custom Intranet for use by Tech Support.
- Installation and customization of MSSQL based billing system.
- Creating a documentation standard using SGML/DocBook to use when configuring new servers.

Senior UNIX Administrator, Omni Internet, LLC, Kerrville TX Oct 1999 – Jan 2000

Languages: PERL, Shell

Software: SSH, CVS, PostgreSQL, Apache, QMail

OS: FreeBSD/x86

Responsibilities:

- Manage FreeBSD mail hub and Apache web servers.
- Security auditing of FreeBSD servers.

Accomplishments:

- Created an administration interface for managing domains on Apache Web server.
- Implementation and configuration of SMTP virus scanner including automatic virus definition updates.

Level 3 Technician, CoreComm Internet., Chicago IL Jan 1999 – Oct 1999

Software: Emerald CRM, Cisco IOS

OS: Win*/x86, Solaris/SPARC

Responsibilities:

- Tech support for 10,000+ T1, ISDN and Dial up customers.
- Dealt exclusively with Dedicated/business customers.

Accomplishments:

- Helped fix several DoS attacks by reconfiguring Cisco border routers.

Network Security Specialist, eEye Digital Security Team, Corona del Mar CA June 1998 – Jan 1999

Languages: C, PERL

Software: MS Visual C++

OS: Win*/x86, Various UNIX OSes

Responsibilities:

- Network Penetration Testing.
- Research Security Vulnerabilities.
- Publish vulnerabilities.
- Development of Security Scanner, Retina.

Accomplishments:

- Publish various security vulnerabilities.
- Decryption of WinGate password encryption.

Personal Experience

Published Software:

snort-win32 (Software Intrusion Detection System)

Snort is an open source lightweight intrusion detection system. I ported snort from UNIX to the win32 platform. Snort-win32 is currently being used by thousands of people including Government and military organizations. Featured recently in Hacking Exposed, 2nd Edition.

Released Software:

ngrep-win32 (Network GREP)

ngrep is a network sniffer designed to facilitate network traffic analysis by providing regular expression matching capabilities, applied at the network layer. Released into the public domain and is packaged in several major UNIX operating systems, including NetBSD and various distributions of Linux. I wrote the initial port to win32 which is now maintained by the original author. Written in C.

dsniff-win32

Dsniff is a password sniffer that understand multiple protocols. Originally written for UNIX platform I ported it to win32. Written in C.

Works in Progress:

OpenBSD TCP/IP stack port to Win32

A port of OpenBSD's TCP/IP stack to the win32 platform. This work is in progress. Overview and general discussion is available upon request.

Reverse Engineering

I have reverse engineered various protocols, including MediaShares's login and chat communication protocol, IMail's encryption protocol, and others. Resulting protocol specifications have enabled myself and others to develop open-source applications that interoperate with these systems. Available by request.