

Blake R. Matheny

347 E Westfield Blvd
Indianapolis, IN 46220
Phone: (317) 644-6112
e-mail: blakematheny@acm.org

Professional Statement Engineer with broad experience in web application and open source software development, virtualization, cryptography, network defense, language design/creation, wireless and community applications. I have typically been responsible for building scalable, secure and highly available distributed systems for large and small customer bases including banks, wireless carriers and high traffic websites.

Professional Experience Compendium Blogware, Indianapolis, IN 09/2007 - Current
LLC

Vice President of Product

Responsible for technical strategy and application architecture, hiring and management of development resources, product support and technical business development. Report to President.

- Created SDLC based around agile methodologies including Scrum, XP and TDD
- Introduced configuration management and change management systems to the SDLC
- Segmented single tier software architecture into an n-tier architecture
- Design and implementation of multiple iterations of both hardware and software architecture
- Created a channelized support offering which was successfully integrated into the product development process.
- Utilized: PHP, MySQL 5.0, AWS (EC2, SQS, S3, SimpleDB), Java (Spring, Tomcat, Hibernate), YUI

404 Internet, LLC Seattle, WA 02/2007 - 08/2007
CTO

Provided a variety of contract services to primarily startups and small businesses. Responsibilities included software development, database engineering, system architecture and analysis, and process development.

- Designed and implemented a site and system for volatile memory analysis. Utilized Java, Groovy, Grails and MySQL 5.0.
- Wrote a distributed hash table in Java using the Chord protocol, custom HTTP Client and Server.
- Implemented load testing for a site utilizing JMeter and Java.

Mixxer.com, Inc. Seattle, WA 09/2006 - 02/2007
Chief Architect

Responsible for the design, development and deployment of high availability, fault tolerant and secure back-end systems. Coordinate deployment and installation of new systems with all engineering departments. Provide support to other engineers including documentation and tutorials. Reported to the VP of Engineering.

- Designed and deployed a distributed cache mechanism that supported multiple programming languages, centralized configuration and transparent fail-over. Used C & PHP.
- Prototyped and deployed a content acquisition application using Firefox (XUL) as the platform.
- Designed a mobile messaging and authentication system for user generated MMS.

Mixxer.com, Inc. Seattle, WA 01/2006 - 09/2006

Director of Engineering

Responsible for technical strategy as well as managing data operations, quality assurance, and development. Managed 10 engineers across 3 departments. Reported to CTO.

- Designed and implemented a system (OpenLocker) that performed automated handset recognition, on the fly transcoding and delivery of media (audio, video, images, text) to end-users. Utilized data mining and pattern recognition. Implemented using C, Java, PHP and the Bourne shell.
- Prototyped and built a system to allow mobile handsets to be utilized as an authentication mechanism. Implemented using SMS and PHP.

3GUpload.com, Inc. Indianapolis, IN 02/2004 - 01/2006

Director of Technology

Led architecture design and development of all system and software projects. Managed 7 engineers across four departments including data operations, quality assurance, development and project management. Responsible for process development and documentation. Reported to CEO.

- Completely redesigned existing software architecture and database schema. Implemented and deployed new system with a team of 3 engineers over a 4 month period of time. Used PHP, MySQL, Perl, Linux, GFS and Memcache. Deployed new hardware architecture at Savvis.
- Built a distributed mobile messaging platform utilizing information obtained by reverse engineering device handsets and carrier network protocols. Used C, Perl and Postfix.
- Wrote data mining applications used for user recommendations and fraud detection utilizing machine learning algorithms. Used PHP and Perl.

Purdue University West Lafayette, IN 10/2003 - 02/2004

Research Engineer - Research Computing Services

Research focused on high performance computing. Research areas included distributed file systems, cluster monitoring and compute grid authentication mechanisms. Mentored junior programmers.

- Implemented, tested and documented a LUSTRE system for use as cluster scratch space.
- Developed an LDAP authentication module for NFSv4.

Infotex Kokomo, IN 10/2001 - 10/2003

Application Security Engineer

Served as a subject matter expert on information security, software design and system automation. Provided code and protocol audits for numerous private businesses and government agencies. Worked on a contract basis, as needed.

- Wrote a portal site integrating IDS/IPS technologies, secure password storage and retrieval, and single sign on to multiple applications utilizing PHP, C and Perl.
- Designed a secure application for rural banks wishing to give their customers online access to their deposits using PHP.

Backwatcher, Inc. Tampa, FL 02/2002 - 02/2003

Senior Software Developer

Worked on a contract basis to provide clients with custom security solutions utilizing open source technologies. Developed internal tools for penetration testing and security audits.

- Ported OpenVRRP and OpenH323 to OpenBSD . Worked on OpenBSD kernel drivers for T1 card.

Sprint Overland Park, KS 06/2001 - 08/2001
Security Engineer II - Firewall Implementation
Primarily responsible for tool development for the team. Also implemented Checkpoint, PIX and Raptor firewalls in HA and Cluster configurations.

- Wrote Solaris command line utility in C++ with a MySQL back-end for connecting to OOB encrypted modems.
- Built web based Solaris jumpstart system in OOPerl to allow for easier automated OS installations.
- Wrote code for several other projects including a knowledge database, VPN jumpstarts and a user import utility for Checkpoint firewalls.

Sprint Overland Park, KS 07/2000 - 06/2001
Security Engineer II - Authentication and Encryption
Responsible for training operations groups in Atlanta, DC and Kansas City as well as giving product presentations to customers on technologies including PKI, SecurID/OTP, LDAP, Radius and VPN Authentication. Rapid design, development and deployment of scalable authentication systems.

- Designed and implemented radius authentication system with LDAP back-end. Wrote tools for user administration. Wrote documentation and trained operations groups.
- Redeployed Entrust PKI for internal and external Sprint customers.
- Solaris (2.5 through 8) administration (all aspects) with dozens of enterprise class servers.

Bussert Consulting Lafayette, IN 08/1999 - 07/2000
Senior Network Engineer
Designed and implemented LAN/WAN solutions as well as new Unix and NT networks using Samba, bind, FreeBSD firewalls and sendmail. Monitored customer sites for vulnerabilities and intrusion attempts. Investigated and responded to incidents.

- Wrote custom Samba solution in C for customer needing remote office integration.

Publications "Using Hashing to Improve Volatile Memory Analysis" with A. Walters and D. White. American Society of Forensic Sciences 60th Annual Meeting. Washington, D.C., February 2008.

"Determining Mobile Forensics Timelines with Location Based Services", submitted to *Digital Forensic Research Workshop, 2007*.

"ADEPTS: Adaptive Intrusion Containment in Distributed Service Environments" with Bingrui Foo, Yu-Sung Wu, Saurabh Bagchi and Gene Spafford. CERIAS Tech Report 2005-01.

"ADEPTS: Adaptive Intrusion Containment and Response using Attack Graphs in an E-Commerce Environment" with Yu-Sung Wu, Bingrui Foo, Saurabh Bagchi, Submitted to *The International Conference on Dependable Systems and Networks, 2004*.

"Methods for Cluster-Based Incident Detection" with Brian Carrier, *Proceedings of the Second IEEE International Workshop on Information Assurance*, IEEE Press.

"ADEPTS: Adaptive Intrusion Containment and Response using Attack Graphs in an E-Commerce Environment" with Yu-Sung Wu, Bingrui Foo, Tyler Olsen, Saurabh Bagchi. CERIAS Tech Report 2003-33.

"Scope Resolution for Event Correlation", submitted to *Recent Advances in Intrusion Detection, 2003*.

Research 4tphi Research Vienna, VA 05/2007 - Present

Volatility - a framework for the extraction of digital artifacts from volatile memory (RAM) images

- Built web framework for analysis tasks
- Visualization tools for analysis results

4tphi Research

Vienna, VA

11/2002 - 05/2007

Babe - a framework for data brokering, mining and transcoding

Babe is a research framework used for providing real-time threat analysis and IDS/IPS testing.

- Designed and implemented initial system in C allowing for modular addition of protocol handlers, parsers, transcoders and detection algorithms.
- Implemented the FOL language described in "Scope Resolution for Event Correlation" in Lex/Yacc

University of Denver

Denver, CO

10/2001 - 05/2007

GNet - a framework for secure peer-to-peer networking

PI - Assistant Professor Christian Grothoff, Denver University, Department of Computer Science

Ported to OpenBSD, NetBSD, FreeBSD and Solaris. Contributed to architecture design and implementation.

Purdue University

West Lafayette, IN

07/2003 - 04/2004

ADEPTS - Adaptive Intrusion Tolerant System

PI - Assistant Professor Saurabh Bagchi, Purdue University, Department of Electrical and Computer Engineering

ADEPTS is an IPS designed to work with never before seen attacks. I designed a metric for estimating the speed of disruption propagation as well as determining the severity of the response based on the severity of the attack.

- Designed and implemented initial architecture and algorithms in C++.

Purdue University

West Lafayette, IN

08/2002 - 09/2003

October - a distributed source sharing infrastructure

PI - Associate Professor Jeff Siskind, Purdue University, Department of Electrical and Computer Engineering

October is a language independent system providing a universal source code repository, search mechanism and revisioning.

- Developed initial C++ PLD (Programming Language Definition)
- Worked to update the Java PLD to the Java 1.5 specification

Purdue University

West Lafayette, IN

08/2002 - 02/2003

ESP - Embedded Sensors Project

PI - Professor Eugene Spafford, Purdue University, Department of Computer Science

Embedding 'sensors' into source code that are detected by the kernel, making it difficult to circumvent alerts and go undetected.

- Helped port OpenBSD kernel code to FreeBSD

Purdue University

West Lafayette, IN

08/2001 - 08/2002

CERIAS - IDS/Machine Learning

PI - Associate Professor Jeff Siskind, Purdue University, Department of Electrical and Computer Engineering

Project goal of applying ML techniques to system calls in order to detect anomalous user behavior.

- Wrote Linux kernel module in C that generated scheme code that was analyzed offline.

Purdue University

West Lafayette, IN

10/1999 - 05/2000

Computer Science Department - Cryptographic Research

PI - Professor Buster Dunsmore, Purdue University, Department of Computer Science

Worked with professors and graduate students on a research paper regarding the security of the Windows 2000 encrypting file system in a networked

environment. Resulted in the discovery of several holes in EFS.

Invited Talks

Using Hashing to Improve Volatile Memory Analysis. AAFS, Washington, DC. 02/2008.
PHP 5.1 & The SPL. PHP User Group, Indianapolis, IN. 04/2006.
A System for the end-to-end Brokering of Diverse Data Types. Rubi-con 5, Detroit, MI. 04/2003.
Natural Language Processing in IAS. CERIAS Research Symposium, West Lafayette, IN. 04/2003
Babe. CERIAS Research Symposium, West Lafayette, IN. 04/2003
The GNU Autotools. PLUG, West Lafayette, IN. 09/2002
GNUnet. Defcon 10, Las Vegas, NV. 08/2002
Enterprise Solutions for AAA. Sprint Security Initiatives, Kansas City, MO. 08/2001

Affiliations

IEEE Member, ACM Professional, EFF, CINLUG

Certifications

Sun Microsystems - SCSA Solaris 2.6 (2001)
Cisco - Cisco Pix Advanced Administration (2001)
Entrust - LiveContent (i500) Directory (2000)
Microsoft - Windows 98 (1999), Network Essentials (1999)

Computer Languages, Systems, and Applications

Programming Languages

PHP, Java, C, Perl, C++, Ruby, ASM (x86), Lua, Scheme, Python, Expect, Lisp, Prolog

Mobile Development

J2ME, WML, XHTML MP, SMS/MMS

PHP Technologies

PHP 3/4/5, PEAR, smarty, adodb, phpunit, simple test, jpgraph, Agavi, Mojavi, Vegas

Java Technologies

Spring, Hibernate, JSP, Groovy, JGroups, javacc, JavaMail, WEKA, Servlets, JMS

Operating Systems

Extensive experience including kernel level familiarity with Linux (2.2.x/2.4.x/2.6.x), FreeBSD, OpenBSD and Solaris. Familiar with HP-UX, Irix and Tru64. Cisco IOS 8-12. Working knowledge of most Windows operating systems.

Web Development

Ruby on Rails, Grails, AJAX, CSS, XUL, YUI, jQuery, Dojo, Zope, Mason

Applications

Version Control	Subversion, CVS, RCS
Build Systems	Make, Ant, Maven, Rake, GNU autotools, Visual Studio 2005
Database	MySQL 4.x, 5.0.x; SQLite; Oracle 8.x, 10.x
Network	Apache, Bind, Samba, Sendmail, Postfix, SSH
Virtualization	Xen, VMWare, EC2
Servlet	Tomcat, Resin
Containers	
Firewalls	PF, IPTables, Checkpoint, Raptor, IPF, IPFW, PIX
IDS	Snort, Dragon, RealSecure
Authentication	Entrust PKI, LDAP (OpenLDAP, Netscape/iPlanet, PeerLogic/i500), SecureID, Steel Belted Radius
Other	Trac, RT, Bugzilla, Graphviz, Latex, Spread, lex, yacc, vim, GNU development tools (bash, gdb, emacs, etc), AWS (SQS, S3, EC2)

Other

Sun Enterprise hardware up to the 3500, low end Cisco routers (up to

26xx) and switches (up to 55xx), Nortel Contivity Extranet Switch

Personal

U.S. Citizen. Native English speaker.

Interests

Electronics, Graph theory, language design, the axiom of choice, fault-tolerant protocols, cryptography, application and protocol security analysis, combinatorics, set theory, elementary quantum physics.

Recommendations Available upon request.