Derek A. Atkins

435 Waterridge Ct
Sandy Springs, GA 30350
(617) 623–3745
derek@ihtfp.com

Objective

Architect, design, develop, implement, analyze, standardize, and evangelize software solutions for Computer Network Security, Secure Systems, Data Protection, Cryptography, and related fields.

Skills

Operating Systems: UNIX (Linux, BSD, Solaris, IRIX, others), OS X, Windows (7/Vista/XP/2K/NT4/95), POSIX, Android, iOS

Applications: Emacs, Firefox, OpenOffice, MS Office, MS Project, VMWare, LaTeX

Languages: C, C++, PERL, Java, Ruby, Scheme, Elisp, HTML, STL, Boost, Gnome/GTK, PThreads

Security Policies: Threat Modeling, Multi-Layer Security, Data Tagging, Cryptographic Protocol Design

Standards: Active IETF participant, Security Area Directorate, former Chair of IMPP, KINK, and OpenPGP WGs, former voting member of NomComm, author of three RFCs. Active participant in ISO JTC-1/SC-31 (WG7) and JTC-1/SC-27 (WG2).

Protocols: TCP/IP, AFS/OpenAFS, IPsec, DNSsec, VPN, 802.11, SMTP, HTTP, WebDAV, DKIM, OAUTH, SSL/TLS/DTLS, SSH

Cryptography: Kerberos, PGP, S/MIME, RSA, DSA, DH, ECC, SHA-*, AES, ECC, PKI

Chief Technology Officer, SecureRF Corporation — Atlanta, GA, and Shelton, CT
June, 2014 – Present

Plan, Architect, Design, Implement, and Deploy numerous security services to identify, protect, and manage embedded device (RFID, NFC, and IoT) security and product identification using SecureRF's cryptographic algorithms and techniques. Manage and audit the corporate security best practices, protocol designs, and product offerings. Work with development on designing secure protocols for tag identification and anti-counterfeiting. Help customers understand the technology, how it solves their problems, how to integrate into their solutions, and work with Sales to understand the customer needs to feed back into Development. Promote SecureRF technology through industry publications and standards activities.

Senior Member of Technical Staff, Mocana Corporation — Atlanta, GA, and San Francisco, CA
June, 2011 – June, 2014

Plan, Architect, Design, Implement, and Deploy numerous security services to manage embedded device security. Expand on Mocana's core technology, an embedded device security toolkit (SSL, SSH, IPsec, EAP, IKE, etc). Created an end-to-end secure firmware delivery service using C and Ruby on Rails for a distributed management solution with individualized per-device management and embedded software agent. Guided the architecture of a secure end-to-end Mobile Application Protection system, including designing the key storage and recovery subsystems. Created and provided a training class on our core cryptography toolkit and helped the customers apply it to their applications. General cross-group resource to help and guide other developers.

Senior Principal Software Engineer, PGP Corporation, now Part of Symantec
Atlanta, GA, and Mountain View, CA
April, 2005 – May, 2011

Architect, design, and implement a method to secure content between end-point applications and server storage solutions by intercepting and redirecting data flows. Created the complete PGP Whole Disk Encryption for Linux product from requirements to implementation including the design, re-xsarchitecture, refactoring of existing Windows implementations, setting up the build system, and foreseeing distribution systems. Architect, design, and implement various secure filesystem products. Worked on a proposal for security enhancements to AFS for distributed secure file storage. Worked with an international team to design and implement a cross-platform client-based filesystem security product. Designing and prototyping a Linux-specific filesystem security product to co-exist with its cross-platform cousins. General PGP historial resource. General security and programming resource.

President, IHTFP Consulting, Inc. — Atlanta, GA and Somerville, MA
January, 2002 – Present

Independent Consultant of Computer and Network Security, including analysis, architecture, design, implementation, and instruction of secure systems. Performed protocol analysis, vulnerability assessment, threat analysis, security architecture, design, and implementation for various clients.

Senior Research Scientist, Telcordia Technologies — Somerville, MA and Morristown, NJ
September 1998 – November 2001

Member of Network Security Research Group. Explored security technologies to protect telecommunications networks including Voice over IP Networks, Ethernet, and 802.11 Wireless LANs. Analyzed IPsec and DNSsec security protocols for performance, scaling, and usability. Explored multiple IP-VPN technologies, Remote Access

approaches, Certificate Authorities (PKI), Security Policy Management, Credential and other Authentication systems, Mobile-IP and Wireless Security. General Lab Security Consultant, answering security questions for other projects and guiding co-workers when security-related issues arise. Telcordia was formerly known as Bellcore.

Co-Founder, Chief Technology Officer, Arepa Inc (Into Networks) Cambridge, MA
August 1997 – July 1998

Also acting Vice-President of Engineering. Built the company from two to eighteen people. Architected and designed the company's core technology DRM solution based soley upon the co-founder's original vision for a secure real-time click-and-play software distribution system. Hired and managed the engineering team to implement that solution. Created project roadmaps and project scheduling for future development, as well as acting as lead architect for current development. Additional responsibilities included inspecting potential competitor's products and looking for viable third-party solutions to augment our core technologies. Arepa was later renamed Into Networks.

Member of Technical Staff, Sun Microsystems Mountain View, CA and Chelmsford, MA
June 1995 – August 1997

Member of the Network Security Products Group. Projects included integrating Kerberos v5 into NFSv3, integrating GSS-API into Solaris (user and kernel), PGP 3.0/5.0 (I wrote more than half of the core program), BSAFE integration, Secure Dynamic DNS Update (in Java), as well as analyzing numerous security solutions and architectures. I also acted as the group cryptographer, answering general questions about cryptographic algorithms and protocols.

Programmer, MIT Information Systems Cambridge, MA
Summer 1994

Ported AFS, the Andrew File System, to Linux. Integrated the required changes into the Linux VFS and Networking layers to support the AFS kernel module.

Programmer, OpenVision, Security Unit Cambridge, MA
Summer 1993

Researched a Kerberos-based authorization system. Started an implementation of GSSAPI.

Undergraduate Research Assistant, MIT Media Laboratory Cambridge, MA
1989 – 1993

Hardware and software developer for the Speech Research Group. Designed and implemented the power and communication network for an Olivetti Active Badge IR sensor network. Wrote C code to monitor and react to the active badge network. Designed and implemented an analog voice computer interface with a Sun/SPARC and MC6811 Microcontroller.

Intern, Bell Communications Research Morristown, NJ
Summer 1992

Designed a Privacy-Enhanced Mail system on top of RSA TIPEM library. Installed Athena system components for lab usage. Contributed to the lab's network security systems.

Intern, Sun Microsystems Mountain View, CA
Summer 1991

Designed hardware and software to help debug a new board and two first-run Silicon chips for the new Sun Workstations for ISDN and high quality audio. Worked with AT&T Concentration Highway (CHI) and Sun SBus interfaces. Contributed to group discussions and meetings of the project group.

Achievements

Internet Engineering Task Force (IETF), 1992 – Present
Member of the Security Area Directorate. Chair of the OAUTH Working Group. Former Chairman of the OpenPGP, Kerberized Internet Negotiation of Keys, and the Instant Messaging and Presence Protocol working groups. Member of the IETF Nominations Committee, 2007. Former member of the DNS Directorate. Author of RFC 1991, the PGP 2.x format, RFC 3862, Common Presence and Instant Messaging (CPIM): Message Format, and RFC 3833, Threat Analysis of the Domain Name System.

PacketCable Security Focus Group, 1998 – 2005
Member in the PacketCable Voice over IP (VoIP) Security Focus group, standardizing on VoIP security for Telephony over CATV. PacketCable is a project sponsored by CableLabs of Englewood, CO.

Pretty Good Privacy (PGP), 1992 – 1997
Programmer, bug tracker, release engineer, and first-round technical support for PGP release 2.2 through PGP 5. In the later years, while at Sun Microsystems, also project lead for PGP 3.0 (later renamed PGP 5.0) and wrote more than half the core program (which is now the core technology of PGP Corporation).

PGP Keysigner, 1994 – 1995
Wrote a Kerberized PGP Keysigner, an automated PGP Certification Authority, and presented the paper, *PGPSign: Kerberized PGP Key Signer*, at the 1995 Usenix conference.

RSA-129 Factoring Project, 1993 – 1994
One of four coordinators of the RSA-129 factoring project. Co-author of resulting paper, *The Magic Words are Squeamish Ossifrage*, which was published and presented at AsiaCrypt '94.

OpenSource Projects, 1993 – Present
Member of numerous open-source development projects. Currently am an active member in the following projects: OpenAFS, Gnucash, Zephyr, GPhoto, others. Wrote the BayStack 802.11 FH driver for Linux. Lead developer of the GnuCash project from 2004-2008. Provide active tech support for the application. Manage the GnuCash Subversion, Email, Wiki, etc. server from 2004 to present.

MIT Athena
Member of Student Information Processing Board. Project Athena Volunteer Consultant. Well versed in much of Project Athena, including intricate knowledge of Kerberos network security, the Zephyr messaging system, and the Andrew File System. Helped port Athena to Linux. Wrote (or assisted in writing) all of the SIPB Linux-Athena installer suites.

Education

Massachusetts Institute of Technology Cambridge, MA
1993 – 1995
S.M. in Media Arts and Sciences (1995)
Topics included Cryptography, Digital Signal Processing, and Digital Image Processing. Researched, designed and implemented a digital voucher ("digital movie ticket") system based upon the theories of digital cash.

Massachusetts Institute of Technology Cambridge, MA
1989 – 1993
S.B. in Electrical Engineering and Computer Science (1993)
Classes include Software Engineering, Communication Systems, Data Communications, Digital Systems Laboratory, and Telephony.

Publications

US Patent #7,707,641 USPTO
Method and apparatus for secure content delivery over broadband access networks

US Patent #7,690,039 USPTO
Method and apparatus for content protection in a secure content delivery system

US Patent #7,017,188 USPTO
Method and apparatus for secure content deliver over broadband access networks

US Patent #6,763,370 USPTO
Method and apparatus for content protection in a secure content delivery system

US Patent #6,374,402 USPTO
Method and apparatus for installation abstraction in a secure content delivery system

The Magic Words are Squeamish Ossifrage AsiaCrypt '94

Personal

Memberships
US Citizen. Usenix Association, Internet Society, International Association of Cryptologic Research, International Financial Cryptography Association

In my spare time I enjoy flying my airplane, sometimes just for the sheer joy of flight. When actually trying to get somewhere, frequently Ohio or Florida, I use my Instrument rating to fly longer distances safely. I am slowly working towards my Commercial rating, the next step in my flight training.

During the winter I ski (Jay Peak is my favorite resort in New England) and during the summer I like to scuba dive, waterski and can almost run a full slalom course. At home I like to relax by learning new songs to play on my guitar.