

Derek A. Atkins

4 Farragut Ave.
Somerville, MA 02144
(617) 623-3745
derek@ihtfp.com

- Objective** Architect, design, develop, implement, analyze, 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), Windows (XP/2K/NT4/95), POSIX
 - Applications:** Emacs, Firefox, MS Office, MS Project, VMWare, OpenOffice, L^AT_EX
 - Languages:** C, C++, PERL, Java, Scheme, Elisp, HTML, PThreads
 - Protocols:** TCP/IP, AFS/OpenAFS, IPsec, DNSsec, VPN, 802.11, ONC-RPC, XDR
 - Cryptography:** Kerberos, PGP, S/MIME, RSA, IDEA, DH, DSS, DES, 3DES, AES, BSAFE, PKI
- Experience**
- Principal Software Engineer**, PGP CORPORATION Somerville, MA and Palo Alto, CA
April, 2005 – Present
Architect, design, and implement various secure filesystem products. Worked on a proposal for security enhancements to AFS. 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 historical resource. General security and programming resource.
- President**, IHTFP CONSULTING, INC. 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 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 solely 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
1989 – 1993

Cambridge, MA

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
Summer 1992

Morristown, NJ

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
Summer 1991

Mountain View, CA

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

Chairman of the OpenPGP working group. Former Chairman of the 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.

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**
1993 – 1995

Cambridge, MA

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
1989 – 1993

Cambridge, MA

S.B. in Electrical Engineering and Computer Science (1993)

Classes include Software Engineering, Communication Systems, Data Communications, Digital Systems Laboratory, and Telephony.

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.