

Donald T. Davis

148 School St., Somerville, MA 02143 (617) 629-3010
don@mit.edu <http://world.std.com/~dtd>

objective Hard problems in network security and cryptography.

skills Large-scale network security, secure protocol design, cryptography, P2P, Unix kernel internals, compiler design. C, C++, Perl, Windows, Linux, BSD, Lisp, assemblers, DBMS applications. Clear design, performance-tuning, thorough debugging; good written and oral communication. Strong mathematical skills, including Statistics, Fourier Analysis and Queuing Theory.

experience

2006-date **Unnamed Company** Greater Boston, MA
Senior technical lead (one of three) for an IPS product team. Redesigned the security administrator's GUI for improved usability; Helped design and build new content-scanning features for the IPS; Designed a new web-security protection feature.

2004-2006 **Intrusic** Burlington, MA
Security Programmer: Conceived, designed, and implemented a real-time data-mining application for network-security forensics. Designed cryptographic protocols for easy-to-use, secure installation and operation of the appliance product.

2000-2002 **Curl Corp.** Cambridge, MA
Corporate Architect Technical lead for all security decisions about a new applet language. Developed a new applet-security model for the language and runtime system (see patents, below), led the implementation, and helped implement new security features. Designed Curl's cryptographic protocol for micropayments and license-enforcement.

'99-2000 **Shym Technology** Needham, MA
Security Architect Responsible for product planning and technical decisions, for Shym's PKI middleware products. Designed cryptographic protocols for all client-server interactions in the system. Implemented low-level cryptographic code in C++. Reviewed security features in customers', partners', competitors', and Shym's own systems. Found and repaired a cryptographic flaw in several secure-email standards specifications (pub. [01a,01b], next page). Prepared and taught an in-house cryptography course for junior programmers.

'94-2004 **Network Security Consultant / Cryptographer** Boston, NYC, Chicago
Various Startups: Security reviews, designs, and advice for product features, security protocols, and system implementations. Clients included two file-encryption vendors, two wireless-networking vendors, an email-filtering vendor, and a European cryptography vendor.
Perfectway: Lead developer for a large-scale intrusion-detection system, written in Perl.
System Experts: Memory cleanup in MIT's Open-Source Kerberos distribution, on behalf of a Wall St. brokerage. Repaired the Kerberos protocol, relaxing its reliance on synchronized clocks [95a] (Kerberos is now part of Win2000 & WinXP, and is the security back-end for Microsoft's Hotmail & .Net systems). Prepared network security analyses and designs for very large corporate and financial clients. Topics included: very-large-scale security systems for ISPs, single-sign-on for PC networks, TCP/IP security, and WWW security [95b]. Designed a scalable and secure ACL-mgt system for a million-user national network.
Open Market: Designed and implemented a high-performance, cryptographic RNG as a kernel-level pseudo-device driver [94] (Linux's /dev/random RNG uses my approach). Analyzed key-management flaws in the public-key infrastructure [96a]. Prepared security analyses for electronic-commerce products, including access-control, transaction-handling, and key-management services. Analyzed the SET transaction protocol. Analyzed trading protocols and various security products. Designed a smartcard-mediated transaction protocol [96b].

'91-'94 **Geer Zolot Associates / OpenVision Technologies** Cambridge, MA
Network Security Architect Prepared network security analyses for large financial firms. Designed a Kerberos-compatible access-control system. Designed an integration of the Kerberos and SecurID authentication systems. Analyzed encryption algorithms for weaknesses.

'87-'91 **MIT / Project Athena** Cambridge, MA
Systems Programmer III Large-scale distributed systems design: Designed a novel asynchronous security protocol [90b]. Designed the peer-to-peer and *rkinit* protocol for the Kerberos authentication system [90a] (the P2P protocol is part of Globus, a distributed computing system used by various U.S. National Labs). Designed and built a cryptographically secure RNG, also for Kerberos [94]. Guided Athena's decision *not* to deploy cycle-services. Designed a video-disc scheduler for a 225-node multimedia e-mail network. Built network tools. Fixed kernel bugs. Prepared software releases. [89].

'82- '86 **Intermetrics, Inc.:** Compiler Programmer Cambridge, MA

'81- '82	Iotron Corp.:	System Mother/Toolsmith	Bedford, MA
'80- '81	MITROL :	DBMS QA Toolsmith	Burlington, MA
'78- '80	Prime Computer:	Compiler Maintenance	Framingham, MA

education

'73-76, '84-86 **Massachusetts Institute of Technology** '86 Cambridge, MA
 B.Sc. in Mathematics, Linguistics minor. Most of my Math coursework was graduate-level.

publications

My research articles are cited in Schneier's *Applied Cryptography*, the *CRC Handbook of Applied Cryptography*, Internet RFCs, Internet Drafts, and other well-known articles and books about computer security. Further, various of my papers have been taught in computer-security courses in the U.S. and around the world, including NYU, U. Penn., the U.S. Naval Postgraduate School, and U. Paderborn in Germany. Abstracts and PostScript for my papers are available at: <http://world.std.com/~dtd>.

- [03] "Privacy and Security Issues in E-Commerce" Chapter 39 in: Derek C. Jones (ed.), *New Economy Handbook*, San Diego: Academic Press/ Elsevier, 2003, pp. 911-930. (With Mark S. Ackerman.)
- [01b] "Defective Sign-and-Encrypt," *Dr. Dobb's Journal*, Nov. 2001.
- [01a] "Defective Sign & Encrypt in S/MIME, PKCS#7, MOSS, PEM, PGP, and XML," *Proc. USENIX Tech. Conf. 2001* (Boston, MA, 2001), pp. 65-78.
- [96b] "Token-Mediated Certification and Electronic Commerce" (with Daniel Geer.) *USENIX Workshop on Elec. Comm.* (Oakland, CA, 1996), pp. 13-22.
- [96a] "Compliance Defects in Public-Key Cryptography" *USENIX Security Symp.* (San Jose, CA, 1996), pp. 171-178.
- [95b] "Kerberos Plus RSA for World Wide Web Security," *USENIX Workshop on Elec. Comm.* (NYC, 1995), pp. 185-188.
- [95a] "Kerberos With Clocks Adrift: History, Protocols, and Implementation," *USENIX Comp. Sys. 9:1* (Jan. 1996), (with D. Geer and T.Y. Ts'o.) Also in *USENIX UNIX Security Symp.* (Salt Lake City, 1995), pp. 35-40.
- [94] "Cryptographic Randomness from Air Turbulence in Disk Drives," In *Advances in Cryptology CRYPTO '94 Conf. Proc.*, ed. by Yvo Desmedt, pp. 114-120. Springer-Verlag Lecture Notes in Computer Science 1994. (with R. Ihaka and P.R. Fenstermacher.)
- [90b] "Network Security via Private-Key Certificates" *ACM Op. Sys. Rev.*, (Oct. '90), pp. 64-67, (with Ralph Swick). Also in *Proc 3rd USENIX Sec. Symp.*, (Baltimore, 1992) pp. 239-242.
- [90a] "Workstation Services and Kerberos Authentication at Project Athena," *MIT Lab. for Comp. Sci. Tech. Memorandum* (Feb. 1990), (with R. Swick.) Presented as LCS Seminar, 5/15/89.
- [89] "Project Athena's Release Engineering Tricks," *Proc. USENIX Software Mgt. Workshop*, (New Orleans, 1989), pp. 101-106.

patents

- 2006 U.S. Patent 6,993,588 "System and methods for securely permitting mobile code to access resources over a network" (with David Kranz and Elizabeth Martin).
- 2003 U.S. Patent Application 20030126292 "System and method for specifying access to resources in a mobile code system" (with David Kranz, Elizabeth Martin, and Matthew Hostetter).
- 2003 U.S. Patent Application 20030167350 "Safe I/O through use of opaque I/O objects" (with David Kranz)