Bibliography

The bibliography entries for RFCs are derived from Henning Schulzrinne's *bibtex* database at `http://www.cs.columbia.edu/~hgs/bib/rfc.bib`.

[Adams and Sasse, 1999] Anne Adams and Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, December 1999. Cited on: *140*.

[Adams and Farrell, 1999] C. Adams and S. Farrell. Internet X.509 public key infrastructure certificate management protocols. RFC 2510, Internet Engineering Task Force, March 1999. Cited on: *322*.
`http://www.rfc-editor.org/rfc/rfc2510.txt`

[Adams *et al.*, 1999] Carlisle Adams, Steve Lloyd, and Stephen Kent. *Understanding the Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations*. New Riders Publishing, 1999. Cited on: *345*.

[Albitz and Liu, 2001] Paul Albitz and Cricket Liu. *DNS and BIND*. O'Reilly, Fourth Edition, April 2001. Cited on: *31*.

[Anderson, 1993] Ross Anderson. Why cryptosystems fail. In *Proceedings of the First ACM Conference on Computer and Communications Security*, pages 215–227, Fairfax, VA, November 1993. Cited on: *146*.

Describes how real-world failures of cryptographic protocols don't always match the classical academic models.

[Anderson, 2002] Ross Anderson. *Security Engineering*. John Wiley & Sons, Inc., 2002. Cited on: *146*.

[Arbaugh *et al.*, 1997] William A. Arbaugh, David J. Farber, and Jonathan M. Smith. A secure and reliable bootstrap architecture. In *Proceedings of the IEEE Computer Society Symposium on Security and Privacy*, pages 65–71, May 1997. Cited on: *127*.

[Arbaugh *et al.*, 2001] William A. Arbaugh, Narendar Shankar, and Y. C. Justin Wan. Your wireless network has no clothes. `http://www.cs.umd.edu/~waa/wireless.pdf`, March 2001. Cited on: *39*.

[Asimov, 1951] Isaac Asimov. *Foundation*. Doubleday & Company, New York, 1951. Cited on: *119*.

[Atkinson, 1997] R. Atkinson. Key exchange delegation record for the DNS. RFC 2230, Internet Engineering Task Force, November 1997. Cited on: *240*.
`http://www.rfc-editor.org/rfc/rfc2230.txt`

[Avolio and Ranum, 1994] Frederick Avolio and Marcus Ranum. A network perimeter with secure external access. In *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, San Diego, CA, February 3, 1994. Cited on: *43*.
`http://www.avolio.com/papers/isoc.html`

> All the President's E-mail! A description of the firewall created for the Executive Office of the President, including mail support for *president*@WHITEHOUSE.GOV.

[Avolio and Vixie, 2001] Frederick M. Avolio and Paul Vixie. *Sendmail: Theory and Practice, Second Edition*. Butterworth-Heinemann, 2001. Cited on: *43*.

[Badger *et al.*, 1996] Lee Badger, Daniel F. Sterne, David L. Sherman, and Kenneth M. Walker. A domain and type enforcement UNIX prototype. *Computing Systems*, 9(1):47–83, 1996. Cited on: *163*.

[Bartal *et al.*, 1999] Yair Bartal, Alain Mayer, Kobbi Nissim, and Avishai Wool. Firmato: A novel firewall management toolkit. In *Proceedings of the IEEE Computer Society Symposium on Security and Privacy*, 1999. Cited on: *193*.
`http://www.eng.tau.ac.il/~yash/sp99.ps`

[Beattie *et al.*, 2002] Steve Beattie, Seth Arnold, Crispin Cowan, Perry Wagle, Chris Wright, and Adam Shostack. Timing the application of security patches for optimal uptime. In *USENIX Sixteenth Systems Administration Conference*, November 2002. Cited on: *275*.
`http://wirex.com/~crispin/time-to-patch-usenix-lisa02.ps.gz`

[Bellare *et al.*, 1996] M. Bellare, R. Canetti, and H. Krawczyk. Keying hash functions for message authentication. In *Advances in Cryptology: Proceedings of CRYPTO '96*, pages 1–15. Springer-Verlag, 1996. Cited on: *346*.
`http://www.research.ibm.com/security/keyed-md5.html`

[Bellovin, 1994] S. Bellovin. Firewall-friendly FTP. RFC 1579, Internet Engineering Task Force, February 1994. Cited on: *53, 202*.
`http://www.rfc-editor.org/rfc/rfc1579.txt`

[Bellovin, 1996] S. Bellovin. Defending against sequence number attacks. RFC 1948, Internet Engineering Task Force, May 1996. Cited on: *24*.
`http://www.rfc-editor.org/rfc/rfc1948.txt`

[Bellovin, 1989] Steven M. Bellovin. Security problems in the TCP/IP protocol suite. *Computer Communications Review*, 19(2):32–48, April 1989. Cited on: *23, 23, 179, 183*.
`http://www.research.att.com/~smb/papers/ipext.ps`

An early paper describing some security risks from the then standard protocols in TCP/IP. Not all of the attacks have happened yet...

[Bellovin, 1990] Steven M. Bellovin. Pseudo-network drivers and virtual networks. In *USENIX Conference Proceedings*, pages 229–244, Washington, D.C., January 22-26, 1990. Cited on: *234*.
`http://www.research.att.com/~smb/papers/pnet.ext.ps`

[Bellovin, 1993] Steven M. Bellovin. Packets found on an internet. *Computer Communications Review*, 23(3):26–31, July 1993. Cited on: *282*.
`http://www.research.att.com/~smb/papers/packets.ps`

[Bellovin, 1995] Steven M. Bellovin. Using the domain name system for system break-ins. In *Proceedings of the Fifth USENIX* UNIX *Security Symposium*, pages 199–208, Salt Lake City, UT, June 1995. Cited on: *32, 198*.

[Bellovin, 1996] Steven M. Bellovin. Problem areas for the IP security protocols. In *Proceedings of the Sixth USENIX* UNIX *Security Symposium*, pages 205–214, July 1996. Cited on: *313, 318*.
`http://www.research.att.com/~smb/papers/badesp.ps`

A discussion of flaws in early versions of the IPsec security protocols. The flaws were fixed in later versions.

[Bellovin, 1999] Steven M. Bellovin. Distributed firewalls. *;login:*, pages 39–47, November 1999. Cited on: *193*.

[Bellovin and Blaze, 2001] Steven M. Bellovin and Matt A. Blaze. Cryptographic modes of operation for the Internet. In *Second NIST Workshop on Modes of Operation*, August 2001. Cited on: *341*.
`http://www.research.att.com/~smb/papers/internet-modes.ps`

[Bellovin *et al.*, 2000] Steven M. Bellovin, C. Cohen, J. Havrilla, S. Herman, B. King, J. Lanza, L. Pesante, R. Pethia, S. McAllister, G. Henault, R. T. Goodden, A. P. Peterson, S. Finnegan, K. Katano, R. M. Smith, and R. A. Lowenthal. Results of the "Security in ActiveX Workshop", December 2000. Cited on: *201*.
`http://www.cert.org/reports/activeX_report.pdf`

[Bellovin and Merritt, 1991] Steven M. Bellovin and Michael Merritt. Limitations of the Kerberos authentication system. In *USENIX Conference Proceedings*, pages 253–267, Dallas, TX, Winter 1991. Cited on: *314, 316*.
`http://www.research.att.com/~smb/papers/kerblimit.usenix.ps`

[Bellovin and Merritt, 1992] Steven M. Bellovin and Michael Merritt. Encrypted key exchange: password-based protocols secure against dictionary attacks. In *Proceedings of the IEEE Computer Society Symposium on Security and Privacy*, pages 72–84, Oakland, CA, May 1992. Cited on: *317, 344*.
`http://www.research.att.com/~smb/papers/neke.ps`

[Bellovin and Merritt, 1993] Steven M. Bellovin and Michael Merritt. Augmented encrypted key exchange. In *Proceedings of the First ACM Conference on Computer and Communications Security*, pages 244–250, Fairfax, VA, November 1993. Cited on: *344*.
`http://www.research.att.com/~smb/papers/aeke.ps`

[Bellovin and Merritt, 1994] Steven M. Bellovin and Michael Merritt. An attack on the *Interlock Protocol* when used for authentication. *IEEE Transactions on Information Theory*, 40(1):273–275, January 1994. Cited on: *104, 344*.

[Berners-Lee *et al.*, 1994] T. Berners-Lee, L. Masinter, and M. McCahill. Uniform resource locators (URL). RFC 1738, Internet Engineering Task Force, December 1994. Cited on: *65, 74*.
`http://www.rfc-editor.org/rfc/rfc1738.txt`

[Biham and Shamir, 1991] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991. Cited on: *338*.

[Biham and Shamir, 1993] Eli Biham and Adi Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, Berlin, 1993. Cited on: *338*.

[Bishop, 1990] Matt Bishop. A security analysis of the NTP protocol. In *Sixth Annual Computer Security Conference Proceedings*, pages 20–29, Tucson, AZ, December 1990. Cited on: *64*.
`http://nob.cs.ucdavis.edu/~bishop/papers/Pdf/ntpsec.pdf`

[Bishop, 1992] Matt Bishop. Anatomy of a proactive password changer. In *Proceedings of the Third USENIX* UNIX *Security Symposium*, pages 171–184, Baltimore, MD, September 1992. Cited on: *96*.

[Blaze, 1993] Matt Blaze. A cryptographic file system for UNIX. In *Proceedings of the First ACM Conference on Computer and Communications Security*, pages 9–16, Fairfax, VA, November 1993.
`http://www.crypto.com/papers/cfs.ps`

[Blaze, 1994] Matt Blaze. Key management in an encrypting file system. In *Proceedings of the Summer USENIX Conference*, pages 27–35, Boston, MA, June 1994. Cited on: *15*.
`http://www.crypto.com/papers/cfskey.ps`

Adding a smart card-based key escrow system to CFS [Blaze, 1993].

[Blaze and Bellovin, 1995] Matt Blaze and Steven M. Bellovin. Session-layer encryption. In *Proceedings of the Fifth USENIX UNIX Security Symposium*, Salt Lake City, UT, June 1995. Cited on: *59*.

[Blaze *et al.*, 1996] Matt Blaze, Whitfield Diffie, Ronald L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson, and Michael Weiner. Minimal key lengths for symmetric cyphers to provide adequate commercial security, January 1996. Cited on: *84, 142*.
`http://www.crypto.com/papers/keylength.ps`

[Bloch, 1979] Arthur Bloch. *Murphy's Law Book Two: More Reasons Why Things Go Wrong!* Price/Stern/Sloan, Los Angelos, 1979. Cited on: *227*.

The denizens of the Internet have attributed this quote to numerous people from Ptolemy on forward. This is the earliest attribution we can find for the quote.

[Bloom, 1970] B. H. Bloom. Space/time trade-offs in hash coding with allowable errors. *Communications of the ACM*, 13(7):422–426, July 1970. Cited on: *113*.

A wonderful paper describing an unjustly obscure search technique.

[Blumenthal *et al.*, 2002] U. Blumenthal, F. Maino, and K. McCloghrie. The AES cipher algorithm in the SNMP's User-based Security Model, 2002. Work in progress. Cited on: *326*.

[Blumenthal and Wijnen, 1999] U. Blumenthal and B. Wijnen. User-based security model (USM) for version 3 of the simple network management protocol (SNMPv3). RFC 2574, Internet Engineering Task Force, April 1999. Cited on: *63, 325*.
`http://www.rfc-editor.org/rfc/rfc2574.txt`

[Borisov *et al.*, 2001] Nikita Borisov, Ian Goldberg, and David A. Wagner. Intercepting mobile communications: The insecurity of 802.11. In *MOBICOM 2001*, Rome, Italy, July 2001. Cited on: *38, 38*.

[Braden *et al.*, 1998] B. Braden, D. Clark, J. Crowcroft, B. Davie, S. Deering, D. Estrin, S. Floyd, V. Jacobson, G. Minshall, C. Partridge, L. Peterson, K. Ramakrishnan, S. Shenker, J. Wroclawski, and L. Zhang. Recommendations on queue management and congestion avoidance in the Internet. RFC 2309, Internet Engineering Task Force, April 1998. Cited on: *220*.
`http://www.rfc-editor.org/rfc/rfc2309.txt`

[Braden, 1989a] R. Braden, editor. Requirements for internet hosts—application and support. RFC 1123, Internet Engineering Task Force, October 1989. Cited on: *24*.
`http://www.rfc-editor.org/rfc/rfc1123.txt`

[Braden, 1989b] R. Braden, editor. Requirements for internet hosts—communication layers. RFC 1122, Internet Engineering Task Force, October 1989. Cited on: *29*.
`http://www.rfc-editor.org/rfc/rfc1122.txt`

[Brand, 1985] Sheila L. Brand, editor. DoD trusted computer system evaluation criteria. DoD 5200.28-STD, DoD Computer Security Center, 1985. Cited on: *11, 100, 102, 260*.
`http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html`

The famous "Orange Book."

[Brand and Makey, 1985] Sheila L. Brand and Jeffrey D. Makey. Department of Defense password management guideline. DoD CSC-STD-002-85, DoD Computer Security Center, 1985. Cited on: *98*.

Part of the "Rainbow Series."

[Bryant, 1988] B. Bryant. Designing an authentication system: A dialogue in four scenes, February 8, 1988. Draft. Cited on: *11, 52, 314*.
http://web.mit.edu/kerberos/www/dialogue.html

A lighthearted derivation of the requirements Kerberos was designed to meet.

[Bunnell *et al.*, 1997] J. Bunnell, J. Podd, R. Henderson, R. Napier, and J. Kennedy-Moffat. Cognitive, associative and conventional passwords: Recall and guessing rates. *Computers and Security*, 16(7):629–641, 1997. Cited on: *140*.

[Cain *et al.*, 2002] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan. Internet group management protocol, version 3. RFC 3376, Internet Engineering Task Force, October 2002. Cited on: *67*.
http://www.rfc-editor.org/rfc/rfc3376.txt

[Callas *et al.*, 1998] J. Callas, L. Donnerhacke, H. Finney, and R. Thayer. OpenPGP message format. RFC 2440, Internet Engineering Task Force, November 1998. Cited on: *327*.
http://www.rfc-editor.org/rfc/rfc2440.txt

[Callon, 1996] R. Callon. The twelve networking truths. RFC 1925, Internet Engineering Task Force, April 1996. Cited on: *192*.
http://www.rfc-editor.org/rfc/rfc1925.txt

[Carpenter and Jung, 1999] B. Carpenter and C. Jung. Transmission of IPv6 over IPv4 domains without explicit tunnels. RFC 2529, Internet Engineering Task Force, March 1999. Cited on: *37*.
http://www.rfc-editor.org/rfc/rfc2529.txt

[Carpenter and Moore, 2001] B. Carpenter and K. Moore. Connection of IPv6 domains via IPv4 clouds. RFC 3056, Internet Engineering Task Force, February 2001. Cited on: *37*.
http://www.rfc-editor.org/rfc/rfc3056.txt

[Carroll, 1872] Lewis Carroll. *Through the Looking-Glass, and What Alice Found There*. Macmillan and Co., London, 1872. Cited on: *150*.
http://www.ibiblio.org/gutenberg/etext91/lglass18.txt

[Carson, 1993] Mark E. Carson. *Sendmail* without the superuser. In *Proceedings of the Fourth USENIX* UNIX *Security Symposium*, pages 139–144, Santa Clara, CA, October 1993. Cited on: *43*.

A good example of retrofitting an existing program to use the principle of "least privilege."

[Case *et al.*, 1990] J. D. Case, M. Fedor, M. L. Schoffstall, and C. Davin. Simple network management protocol (SNMP). RFC 1157, Internet Engineering Task Force, May 1990. Cited on: *62, 325*.
http://www.rfc-editor.org/rfc/rfc1157.txt

[CC, 1999] Common criteria for information technology security evaluation, August 1999. Version 2.1. Cited on: *11, 100*.
`http://www.commoncriteria.org`

[Chapman, 1992] D. Brent Chapman. Network (in)security through IP packet filtering. In *Proceedings of the Third USENIX* UNIX *Security Symposium*, pages 63–76, Baltimore, MD, September 1992. Cited on: *177, 188, 232*.
`http://www.greatcircle.com/pkt_filtering.html`

Shows how hard it is to set up secure rules for a packet filter.

[Chen *et al.*, 2002] Hao Chen, David A. Wagner, and Drew Dean. Setuid demystified. In *Proceedings of the of the Eleventh USENIX* UNIX *Security Symposium*, San Francisco, CA, 2002. Cited on: *125*.

A close look at setuid and setgid implementations and interactions.

[Cheswick, 1990] William R. Cheswick. The design of a secure internet gateway. In *Proceedings of the Summer USENIX Conference*, Anaheim, CA, June 1990. Cited on: *187, 195*.
`http://www.cheswick.com/ches/papers/gateway.ps`

[Cheswick, 1992] William R. Cheswick. An evening with Berferd, in which a cracker is lured, endured, and studied. In *Proceedings of the Winter USENIX Conference*, San Francisco, CA, January 1992. Cited on: *287*.
`http://www.cheswick.com/ches/papers/berferd.ps`

[Cheswick and Bellovin, 1996] William R. Cheswick and Steven M. Bellovin. A DNS filter and switch for packet-filtering gateways. In *Proceedings of the Sixth USENIX* UNIX *Security Symposium*, pages 15–19, San Jose, CA, 1996. Cited on: *198*.

[Cheswick *et al.*, 2003] William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin. *Firewalls and Internet Security; Repelling the Wily Hacker*. Addison-Wesley, Reading, MA, 2003. Cited on: *142*.
`http://www.wilyhacker.com/`

[Coene, 2002] L. Coene. Stream control transmission protocol applicability statement. RFC 3257, Internet Engineering Task Force, April 2002. Cited on: *25*.
`http://www.rfc-editor.org/rfc/rfc3257.txt`

[Comer, 2000] Douglas E. Comer. *Internetworking with TCP/IP: Principles, Protocols, and Architecture*, Volume I. Prentice-Hall, Englewood Cliffs, NJ, Fourth Edition, 2000. Cited on: *19*.

A well-known description of the TCP/IP protocol suite.

[Comer and Stevens, 1998] Douglas E. Comer and David L. Stevens. *Internetworking with TCP/IP: ANSI C Version: Design, Implementation, and Internals*, Volume II. Prentice-Hall, Englewood Cliffs, NJ, Third Edition, 1998. Cited on: *19*.

How to implement TCP/IP.

[Comer *et al.*, 2000] Douglas E. Comer, David L. Stevens, Marshall T. Rose, and Michael Evangelista. *Internetworking with TCP/IP: Client-Server Programming and Applications, Linux/Posix Sockets Version*, Volume III. Prentice-Hall, Englewood Cliffs, NJ, 2000. Cited on: *19*.

[Connolly and Masinter, 2000] D. Connolly and L. Masinter. The "text/html" media type. RFC 2854, Internet Engineering Task Force, June 2000. Cited on: *74*.
`http://www.rfc-editor.org/rfc/rfc2854.txt`

[Conta and Deering, 1998] A. Conta and S. Deering. Internet control message protocol (ICMPv6) for the internet protocol version 6 (IPv6) specification. RFC 2463, Internet Engineering Task Force, December 1998. Cited on: *28*.
`http://www.rfc-editor.org/rfc/rfc2463.txt`

[Costales, 1993] Bryan Costales, with Eric Allman and Neil Rickert. *sendmail*. O'Reilly, Sebastopol, CA, 1993. Cited on: *43, 43*.

[Crispin, 1996] M. Crispin. Internet message access protocol—version 4rev1. RFC 2060, Internet Engineering Task Force, December 1996. Cited on: *45*.
`http://www.rfc-editor.org/rfc/rfc2060.txt`

[Curry, 1992] David A. Curry. UNIX *System Security: A Guide for Users and System Administrators*. Addison-Wesley, Reading, MA, 1992. Cited on: *xix*.

[Daemen and Rijmen, 2002] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES–The Advanced Encryption Standard*. Springer, 2002. Cited on: *337*.

[daemon9, 1997] daemon9. Juggernaut. *Phrack Magazine*, 50, April 1997. Cited on: *130*.
`http://www.phrack.com/show.php?p=50&a=6`

[daemon9 *et al.*, 1996] daemon9, route, and infinity. Project Neptune. *Phrack Magazine*, 7(48), July 1996. Cited on: *109*.
`http://www.phrack.com/show.php?p=48&a=6`

[Davies and Price, 1989] Donald W. Davies and Wyn L. Price. *Security for Computer Networks*. John Wiley & Sons, New York, Second Edition, 1989. Cited on: *147*.

A guide to deploying cryptographic technology.

[Dean *et al.*, 1996] Drew Dean, Edward W. Felten, and Dan S. Wallach. Java security: From HotJava to Netscape and beyond. In *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, pages 190–200, Oakland, California, May 1996. Cited on: *80, 81*.

[Deering and Hinden, 1998] S. Deering and R. Hinden. Internet protocol, version 6 (IPv6) specification. RFC 2460, Internet Engineering Task Force, December 1998. Cited on: *34*.
`http://www.rfc-editor.org/rfc/rfc2460.txt`

[Denker *et al.*, 1999] J. S. Denker, S. M. Bellovin, H. Daniel, N. L. Mintz, T. Killian, and M. A. Plotnick. Moat: A virtual private network appliance and services platform. In *Proceedings of LISA XIII*, November 1999. Cited on: *244*.
`http://www.quintillion.com/moat/lisa-moat.pdf`

[Denning and Sacco, 1981] Dorothy E. Denning and Giovanni M. Sacco. Timestamps in key distribution protocols. *Communications of the ACM*, 24(8):533–536, August 1981. Cited on: *149, 314*.

Some weaknesses in [Needham and Schroeder, 1978].

[Dhamija and Perrig, 2000] R. Dhamija and A. Perrig. Deja Vu—a user study: Using images for authentication. *Proceedings of the Ninth USENIX Security Symposium*, 2000. Cited on: *142*.

[Dierks and Allen, 1999] T. Dierks and C. Allen. The TLS protocol version 1.0. RFC 2246, Internet Engineering Task Force, January 1999. Cited on: *77, 323*.
`http://www.rfc-editor.org/rfc/rfc2246.txt`

[Diffie, 1988] Whitfield Diffie. The first ten years of public key cryptography. *Proceedings of the IEEE*, 76(5):560–577, May 1988. Cited on: *145*.

An exceedingly useful retrospective.

[Diffie and Hellman, 1976] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-11:644–654, November 1976. Cited on: *48, 316, 342, 343*.

The original paper on public key cryptography. A classic.

[Diffie and Hellman, 1977] Whitfield Diffie and Martin E. Hellman. Exhaustive cryptanalysis of the NBS data encryption standard. *Computer*, 10(6):74–84, June 1977. Cited on: *338*.

The original warning about DES's key length being too short.

[Dobbertin *et al.*, 1996] H. Dobbertin, A. Bosselaers, and B. Preneel. Ripemd-160, a strengthened version of ripemd. *Fast Software Encryption, LNCS 1039*, pages 71–82, 1996. Cited on: *347*.
`http://www.esat.kuleuven.ac.be/~cosicart/ps/AB-9601/AB-9601.ps.gz`

[Droms and Arbaugh, 2001] R. Droms and W. Arbaugh, editors. Authentication for DHCP messages. RFC 3118, Internet Engineering Task Force, June 2001. Cited on: *33*.
`http://www.rfc-editor.org/rfc/rfc3118.txt`

[Eastlake, 1999] D. Eastlake. Domain name system security extensions. RFC 2535, Internet Engineering Task Force, March 1999. Cited on: *33, 33*.
`http://www.rfc-editor.org/rfc/rfc2535.txt`

[Eastlake *et al.*, 2001] D. Eastlake, 3rd, and P. Jones. US secure hash algorithm 1 (SHA1). RFC 3174, Internet Engineering Task Force, September 2001. Cited on: *326*.
`http://www.rfc-editor.org/rfc/rfc3174.txt`

[Eastlake and Kaufman, 1997] D. Eastlake and C. Kaufman. Domain name system security extensions. RFC 2065, Internet Engineering Task Force, January 1997. Cited on: *33*.
`http://www.rfc-editor.org/rfc/rfc2065.txt`

[Eichin and Rochlis, 1989] M. W. Eichin and J. A. Rochlis. With microscope and tweezers: An analysis of the Internet virus of November 1988. In *Proceedings of the IEEE Computer Society Symposium on Security and Privacy*, pages 326–345, Oakland, CA, May 1989. Cited on: *43, 100*.
`ftp://athena-dist.mit.edu/pub/virus/mit_ieee.PS`

[Eisler, 1999] M. Eisler. NFS version 2 and version 3 security issues and the NFS protocol's use of RPCSEC_GSS and Kerberos V5. RFC 2623, Internet Engineering Task Force, June 1999. Cited on: *48, 51*.
`http://www.rfc-editor.org/rfc/rfc2623.txt`

[Eisler *et al.*, 1997] M. Eisler, A. Chiu, and L. Ling. RPCSEC_GSS protocol specification. RFC 2203, Internet Engineering Task Force, September 1997. Cited on: *48*.
`http://www.rfc-editor.org/rfc/rfc2203.txt`

[Elz *et al.*, 1997] R. Elz, R. Bush, S. Bradner, and M. Patton. Selection and operation of secondary DNS servers. RFC 2182, Internet Engineering Task Force, July 1997. Cited on: *198*.
`http://www.rfc-editor.org/rfc/rfc2182.txt`

[Farmer, 1997] Dan Farmer, 1997. Cited on: *129, 259*.
`http://www.trouble.org/survey/`

[Farmer and Spafford, 1990] Dan Farmer and Eugene H. Spafford. The COPS security checker system. In *USENIX Conference Proceedings*, pages 165–170, Anaheim, CA, Summer 1990. Cited on: *125, 302*.
`http://www.cerias.purdue.edu/homes/spaf/tech-reps/993.ps`

A package to audit systems for vulnerabilities.

[Farmer and Venema, 1993] Dan Farmer and Wietse Venema. Improving the security of your site by breaking into it, 1993. Cited on: *64*.
`http://www.fish.com/security/admin-guide-to-cracking.html`

[Farrow, 1991] Rik Farrow. UNIX *System Security: How to Protect Your Data and Prevent Intruders*. Addison-Wesley, Reading, MA, 1991. Cited on: *xix*.

[Feaver, 1992] Peter Feaver. *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States*. Cornell University Press, 1992. Cited on: *3*.

[Feghhi *et al.*, 1998] Jalal Feghhi, Jalil Feghhi, and Peter Williams. *Digital Certificates: Applied Internet Security*. Addison Wesley, 1998. Cited on: *345*.

[Feldmann *et al.*, 1998] Anja Feldmann, Jennifer Rexford, and Ramon Caceres. Efficient policies for carrying web traffic over flow-switched networks. *IEEE/ACM Transactions on Networking*, pages 673–685, December 1998. Cited on: *192*.
`http://www.research.att.com/~jrex/papers/ton98.ps`

> This paper computes the average TCP flow size as 12 packets. The authors report that newer data has increased this size to 20.

[Feldmeier and Karn, 1990] David C. Feldmeier and Philip R. Karn. UNIX password security—ten years later. In *Advances in Cryptology: Proceedings of CRYPTO '89*, pages 44–63. Springer-Verlag, 1990. Cited on: *96*.

[Felten *et al.*, 1997] Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan Wallach. Web spoofing: An internet con game. *Twentieth National Information Systems Security Conference*, 1997. Cited on: *82, 84*.

[Ferguson and Senie, 2000] P. Ferguson and D. Senie. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. RFC 2827, Internet Engineering Task Force, May 2000. Cited on: *20, 177*.
`http://www.rfc-editor.org/rfc/rfc2827.txt`

[Fielding *et al.*, 1999] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee. Hypertext transfer protocol – HTTP/1.1. RFC 2616, Internet Engineering Task Force, June 1999. Cited on: *74*.
`http://www.rfc-editor.org/rfc/rfc2616.txt`

[Fluhrer *et al.*, 2001] Scott Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the key scheduling algorithm of RC4. In *Eighth Annual Workshop on Selected Areas in Cryptography*, Toronto, Canada, August 2001. Cited on: *39*.

[Forrest *et al.*, 1996] S. Forrest, S.A Hofmeyr, A. Somayaji, and T. A. Longstaff. A sense of self for unix processes. In *Proceedings of the IEEE Computer Society Symposium on Security and Privacy*, 1996. Cited on: *281*.
`http://cs.unm.edu/~forrest/publications/ieee-sp-96-unix.ps`

[Freed and Borenstein, 1996a] N. Freed and N. Borenstein. Multipurpose internet mail extensions (MIME) part one: Format of internet message bodies. RFC 2045, Internet Engineering Task Force, November 1996. Cited on: *43, 75*.
`http://www.rfc-editor.org/rfc/rfc2045.txt`

[Freed and Borenstein, 1996b] N. Freed and N. Borenstein. Multipurpose internet mail extensions (MIME) part two: Media types. RFC 2046, Internet Engineering Task Force, November 1996. Cited on: *44*.
`http://www.rfc-editor.org/rfc/rfc2046.txt`

[Fu *et al.*, 2001] Kevin Fu, Emil Sit, Kendra Smith, and Nick Feamster. Dos and don'ts of client authentication on the web. *In Proceedings of the Eighth USENIX Security Symposium*, pages 251–270, 2001. Cited on: *76*.

[Fuller *et al.*, 1993] V. Fuller, T. Li, J. Yu, and K. Varadhan. Classless inter-domain routing (CIDR): an address assignment and aggregation strategy. RFC 1519, Internet Engineering Task Force, September 1993. Cited on: *191*.
`http://www.rfc-editor.org/rfc/rfc1519.txt`

[Garfinkel and Spafford, 1996] Simson Garfinkel and Eugene Spafford. *Practical Unix and Internet Security*. O'Reilly, Sebastopol, CA, Second Edition, 1996. Cited on: *xix*.

[Garon and Outerbridge, 1991] Gilles Garon and Richard Outerbridge. DES Watch: An examination of the sufficiency of the data encryption standard for financial institution information security in the 1990s. *Cryptologia*, XV(3):177–193, July 1991. Cited on: *342*.

Gives the economics—and the economic impact—of cracking DES.

[Gavron, 1993] E. Gavron. A security problem and proposed correction with widely deployed DNS software. RFC 1535, Internet Engineering Task Force, October 1993. Cited on: *32*.
`http://www.rfc-editor.org/rfc/rfc1535.txt`

[Gaynor and Bradner, 2001] M. Gaynor and S. Bradner. Firewall enhancement protocol (FEP). RFC 3093, Internet Engineering Task Force, April 2001. Cited on: *228*.
`http://www.rfc-editor.org/rfc/rfc3093.txt`

[Gifford, 1982] David K. Gifford. Cryptographic sealing for information secrecy and authentication. *Communications of the ACM*, 25(4):274–286, 1982. Cited on: *15*.

[Gilbert and Sullivan, 1879] W. S. Gilbert and A. S. Sullivan. The pirates of penzance, or the slave of duty, 1879. Cited on: *128*.

[Gilmore *et al.*, 1999] Christian Gilmore, David Kormann, and Aviel D. Rubin. Secure remote access to an internal web server. *IEEE Network*, 13(6):31–37, 1999. Cited on: *228*.

[Gilmore, 1998] John Gilmore, editor. *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design*. O'Reilly, July 1998. Cited on: *338*.
`http://www.eff.org/descracker.html`

[Goldberg *et al.*, 1996] Ian Goldberg, David A. Wagner, Randi Thomas, and Eric A. Brewer. A secure environment for untrusted helper applications. In *Proceedings of the Sixth USENIX Security Symposium*, San Jose, CA, USA, 1996. Cited on: *163*.
`http://HTTP.CS.Berkeley.EDU/~daw/janus/`

[Goldman, 1998] William Goldman. *The Princess Bride: S. Morgenstern's Classic Tale of True Love and High Adventure: The "Good Parts" Version: Abridged*. Ballantine Books, 1998. Cited on: *xix*.

[Goldsmith and Schiffman, 1998] David Goldsmith and Michael Schiffman. Firewalking: A traceroute-like analysis of IP packet responses to determine gateway access control lists, 1998. Cited on: *229*.
`http://www.packetfactory.net/firewalk/firewalk-final.html`

[Gong, 1997] Li Gong. Java security: Present and near future. *IEEE Micro*, pages 14–19, May/June 1997. Cited on: *82*.

[Goodell *et al.*, 2003] Geoffrey Goodell, William Aiello, Timothy Griffin, John Ioannidis, Patrick McDaniel, and Aviel Rubin. Working around bgp: An incremental approach to improving security and accuracy of interdomain routing. In *Proceedings of the IEEE Network and Distributed System Security Symposium*, February 2003. Cited on: *30*.

[Grampp and Morris, 1984] Fred T. Grampp and Robert H. Morris. UNIX operating system security. *AT&T Bell Laboratories Technical Journal*, 63(8, Part 2):1649–1672, October 1984. Cited on: *xvii, 96*.

[Grimm and Bershad, 2001] Robert Grimm and Brian N. Bershad. Separating access control policy, enforcement and functionality in extensible systems. *ACM Transactions on Computer Systems*, 16(1):36–70, February 2001. Cited on: *163*.
`http://www.cs.washington.edu/homes/rgrimm/papers/tocs01.pdf`

[Haber and Stornetta, 1991a] S. Haber and W. S. Stornetta. How to time-stamp a digital document. In *Advances in Cryptology: Proceedings of CRYPTO '90*, pages 437–455. Springer-Verlag, 1991. Cited on: *347*.

[Haber and Stornetta, 1991b] S. Haber and W. S. Stornetta. How to time-stamp a digital document. *Journal of Cryptology*, 3(2):99–112, 1991. Cited on: *347*.

[Hafner and Markoff, 1991] Katie Hafner and John Markoff. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. Simon & Schuster, New York, 1991. Cited on: *14*.

Background and personal information on three famous hacking episodes.

[Hagino and Yamamoto, 2001] J. Hagino and K. Yamamoto. An IPv6-to-IPv4 transport relay translator. RFC 3142, Internet Engineering Task Force, June 2001. Cited on: *37*.
`http://www.rfc-editor.org/rfc/rfc3142.txt`

[Hain, 2000] T. Hain. Architectural implications of NAT. RFC 2993, Internet Engineering Task Force, November 2000. Cited on: *38*.
`http://www.rfc-editor.org/rfc/rfc2993.txt`

[Haller, 1994] N. Haller. The S/Key one-time password system. In *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, San Diego, CA, February 3, 1994. Cited on: *98, 146*.

An implementation of the scheme described in [Lamport, 1981].

[Haller and Metz, 1996] N. Haller and C. Metz. A one-time password system. RFC 1938, Internet Engineering Task Force, May 1996. Cited on: *98, 146*.
`http://www.rfc-editor.org/rfc/rfc1938.txt`

[Haller *et al.*, 1998] N. Haller, C. Metz, P. Nesser, and M. Straw. A one-time password system. RFC 2289, Internet Engineering Task Force, February 1998. Cited on: *104*.
`http://www.rfc-editor.org/rfc/rfc2289.txt`

[Hambridge and Lunde, 1999] S. Hambridge and A. Lunde. DON'T SPEW a set of guidelines for mass unsolicited mailings and postings (spam*). RFC 2635, Internet Engineering Task Force, June 1999. Cited on: *43*.
`http://www.rfc-editor.org/rfc/rfc2635.txt`

[Handley *et al.*, 2001] M. Handley, C. Kreibich, and V. Paxson. Network intrusion detection: Evasion, traffic normalization, and end-to-end protocol semantics. *Proceedings of the USENIX Security Symposium*, pages 115–131, 2001. Cited on: *279, 280*.

[Harkins and Carrel, 1998] D. Harkins and D. Carrel. The internet key exchange (IKE). RFC 2409, Internet Engineering Task Force, November 1998. Cited on: *318, 320*.
`http://www.rfc-editor.org/rfc/rfc2409.txt`

[Harrenstien, 1977] K. Harrenstien. NAME/FINGER protocol. RFC 742, Internet Engineering Task Force, December 1977. Cited on: *64*.
`http://www.rfc-editor.org/rfc/rfc742.txt`

[Harrenstien *et al.*, 1985] K. Harrenstien, M. K. Stahl, and E. J. Feinler. NICNAME/WHOIS. RFC 954, Internet Engineering Task Force, October 1985. Cited on: *64*.
`http://www.rfc-editor.org/rfc/rfc954.txt`

[Haskett, 1984] J. A. Haskett. Pass-algorithms: A user validation scheme based on knowledge of secret algorithms. *Communications of the ACM*, 27(8):777–781, 1984. Cited on: *142*.

[Heffernan, 1998] A. Heffernan. Protection of BGP sessions via the TCP MD5 signature option. RFC 2385, Internet Engineering Task Force, August 1998. Cited on: *30*.
`http://www.rfc-editor.org/rfc/rfc2385.txt`

[Heinlein, 1967] Robert A. Heinlein. *The Past Through Tomorrow*. Putnam, New York, 1967. Cited on: *227*.

Originally appeared in "Logic of Empire," published in Astounding SF, 1941.

[Heinlein, 1996] Robert A. Heinlein. *Glory Road*. Baen Books, 1996. Cited on: *80*.

[Hill, 2000] Paul B. Hill. Kerberos interoperability issues. In *Third Large Installation System Administration of Windows NT Conference*, pages 35–42, 2000. Cited on: *317*.

[Hinden and Deering, 1998] R. Hinden and S. Deering. IP version 6 addressing architecture. RFC 2373, Internet Engineering Task Force, July 1998. Cited on: *35*.
`http://www.rfc-editor.org/rfc/rfc2373.txt`

[Hobbs, 1853] Alfred Charles Hobbs. *Rudimentary Treatise on the Construction of Locks*. Edited by Charles Tomlinson. J. Weale, London, 1853. Cited on: *119*.

[Hoffman, 2002] P. Hoffman. SMTP service extension for secure SMTP over transport layer security. RFC 3207, Internet Engineering Task Force, February 2002. Cited on: *43, 171*.
`http://www.rfc-editor.org/rfc/rfc3207.txt`

[Holdrege and Srisuresh, 2001] M. Holdrege and P. Srisuresh. Protocol complications with the IP network address translator. RFC 3027, Internet Engineering Task Force, January 2001. Cited on: *38*.
`http://www.rfc-editor.org/rfc/rfc3027.txt`

[Honeyman *et al.*, 1992] P. Honeyman, L. B. Huston, and M. T. Stolarchuk. Hijacking AFS. In *USENIX Conference Proceedings*, pages 175–182, San Francisco, CA, Winter 1992. Cited on: *52*.

A description of some security holes—now fixed—in AFS.

[Howard, 1988] John H. Howard. An overview of the Andrew File System. In *USENIX Conference Proceedings*, pages 23–26, Dallas, TX, Winter 1988. Cited on: *52*.

[Ioannidis and Bellovin, 2002] John Ioannidis and Steven M. Bellovin. Implementing pushback: Router-based defense aganist DDoS attacks. In *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, 2002. Cited on: *115*.

[Jermyn *et al.*, 1999] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin. The design and analysis of graphical passwords. *In Proceedings of the Eighth USENIX Security Symposium*, pages 1–14, 1999. Cited on: *142*.

[Joncheray, 1995] Laurent Joncheray. A simple active attack against TCP. In *Proceedings of the Fifth USENIX* UNIX *Security Symposium*, Salt Lake City, UT, 1995. Cited on: *118, 130*.

[Kahn, 1996] David Kahn. *The Code-Breakers: The Story of Secret Writing*. Macmillan, New York, Second Edition, 1996. Cited on: *335*.

The definitive work on the history of cryptography, and an introduction to classical cryptography. A must-read, but it does not discuss modern cryptographic techniques.

[Kantor and Lapsley, 1986] B. Kantor and P. Lapsley. Network news transfer protocol. RFC 977, Internet Engineering Task Force, February 1986. Cited on: *66*.
`http://www.rfc-editor.org/rfc/rfc977.txt`

[Karger and Schell, 2002] Paul A. Karger and Roger R. Schell. Thirty years later: Lessons from the Multics security evaluation. *Annual Computer Security Applications Conference*, 2002. Cited on: *332*.

[Kaufman, 1993] C. Kaufman. DASS—distributed authentication security service. RFC 1507, Internet Engineering Task Force, September 1993. Cited on: *327*.
http://www.rfc-editor.org/rfc/rfc1507.txt

[Kaufman *et al.*, 2002] Charlie Kaufman, Radia Perlman, and Mike Speciner. *Network Security: Private Communication in a Public World*. Prentice Hall, Second Edition, 2002. Cited on: *313*.

[Kazar, 1988] Michael Leon Kazar. Synchronization and caching issues in the Andrew file system. In *USENIX Conference Proceedings*, pages 27–36, Dallas, TX, Winter 1988. Cited on: *52*.

[Kent and Atkinson, 1998a] S. Kent and R. Atkinson. IP authentication header. RFC 2402, Internet Engineering Task Force, November 1998. Cited on: *318*.
http://www.rfc-editor.org/rfc/rfc2402.txt

[Kent and Atkinson, 1998b] S. Kent and R. Atkinson. IP encapsulating security payload (ESP). RFC 2406, Internet Engineering Task Force, November 1998. Cited on: *318*.
http://www.rfc-editor.org/rfc/rfc2406.txt

[Kent and Atkinson, 1998c] S. Kent and R. Atkinson. Security architecture for the internet protocol. RFC 2401, Internet Engineering Task Force, November 1998. Cited on: *318*.
http://www.rfc-editor.org/rfc/rfc2401.txt

[Kent *et al.*, 2000a] Stephen Kent, Charles Lynn, Joanne Mikkelson, and Karen Seo. Secure border gateway protocol (S-BGP)—real world performance and deployment issues. In *Proceedings of the IEEE Network and Distributed System Security Symposium*, February 2000. Cited on: *30*.

[Kent *et al.*, 2000b] Stephen Kent, Charles Lynn, and Karen Seo. Secure border gateway protocol (Secure-BGP). *IEEE Journal on Selected Areas in Communications*, 18(4):582–592, April 2000. Cited on: *30*.

[Klein, 1990] Daniel V. Klein. "Foiling the cracker": A survey of, and improvements to, password security. In *Proceedings of the USENIX* UNIX *Security Workshop*, pages 5–14, Portland, OR, August 1990. Cited on: *96, 96, 98*.

> Describes the author's experiments cracking password files from many different machines.

[Klensin, 2001] J. Klensin, editor. Simple mail transfer protocol. RFC 2821, Internet Engineering Task Force, April 2001. Cited on: *41*.
http://www.rfc-editor.org/rfc/rfc2821.txt

[Klensin *et al.*, 1997] J. Klensin, R. Catoe, and P. Krumviede. IMAP/POP AUTHorize extension for simple challenge/response. RFC 2195, Internet Engineering Task Force, September 1997. Cited on: *45*.
http://www.rfc-editor.org/rfc/rfc2195.txt

[Knuth, 2001] D. E. Knuth. *Literate Programming (Center for the Study of Language and Information—Lecture Notes, No 27*. C S L I Publications, January 2001. Cited on: *154*.

[Ko *et al.*, 2000] C. Ko, T. Fraser, L. Badger, and D. Kilpatrick. Detecting and countering system intrusions using software wrappers. *Proceedings of the USENIX Security Conference*, pages 145–156, 2000. Cited on: *281*.

[Koblas and Koblas, 1992] David Koblas and Michelle R. Koblas. SOCKS. In UNIX *Security III Symposium*, pages 77–83, Baltimore, MD, September 14-17, 1992. USENIX. Cited on: *187*.

A description of the most common circuit-level gateway package.

[Kohl and Neuman, 1993] J. Kohl and C. Neuman. The kerberos network authentication service (V5). RFC 1510, Internet Engineering Task Force, September 1993. Cited on: *11, 52, 314*.
`http://www.rfc-editor.org/rfc/rfc1510.txt`

[Krawczyk *et al.*, 1997] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: keyed-hashing for message authentication. RFC 2104, Internet Engineering Task Force, February 1997. Cited on: *326*.
`http://www.rfc-editor.org/rfc/rfc2104.txt`

[Krishnamurthy and Rexford, 2001] Balachander Krishnamurthy and Jennifer Rexford. *Web Protocols and Practice: HTTP/1.1, Networking Protocols, Caching, and Traffic Measurement*. Addison-Wesley, Reading, MA, 2001. Cited on: *74*.

[Kurose and Ross, 2002] James F. Kurose and Keith W. Ross. *Computer Networking: A Top-Down Approach Featuring the Internet*. Addison-Wesley, Reading, MA, Second Edition, 2002. Cited on: *19*.

[LaMacchia *et al.*, 2002] Brian A. LaMacchia, Sebastian Lange, Matthew Lyons, Rudi Martin, and Kevin T. Price. *.NET Framework Security*. Addison-Wesley, Reading, MA, 2002. Cited on: *264*.

[LaMacchia and Odlyzko, 1991] Brian A. LaMacchia and Andrew M. Odlyzko. Computation of discrete logarithms in prime fields. *Designs, Codes, and Cryptography*, 1:46–62, 1991. Cited on: *48*.

Describes how the authors cryptanalyzed Secure RPC.

[Lamport, 1981] Leslie Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772, November 1981. Cited on: *146, 367*.

The basis for the Bellcore S/Key system.

[Leech, 2002] M. Leech. Chinese Lottery cryptanalysis revisited: The Internet as codebreaking tool, 2002. Work in progress. Cited on: *117*.

[LeFebvre, 1992] William LeFebvre. Restricting network access to system daemons under SunOS. In UNIX *Security III Symposium*, pages 93–103, Baltimore, MD, September 14-17, 1992. USENIX. Cited on: *163*.

Using shared libraries to provide access control for standing servers.

[Lehrer, 1959] Tom Lehrer. *An Evening (Wasted) with Tom Lehrer*. Reprise Records, 1959. Cited on: *351*.

[Leong and Tham, 1991] Philip Leong and Chris Tham. UNIX password encryption considered insecure. In *Proceedings of the Winter USENIX Conference*, Dallas, TX, 1991. Cited on: *96*.

How to build a hardware password-cracker.

[Limoncelli and Hogan, 2001] Thomas A. Limoncelli and Christine Hogan. *The Practice of System and Network Administration*. Addison-Wesley, Reading, MA, 2001. Cited on: *123*.

[Linn, 2000] J. Linn. Generic security service application program interface version 2, update 1. RFC 2743, Internet Engineering Task Force, January 2000. Cited on: *327*.
`http://www.rfc-editor.org/rfc/rfc2743.txt`

[Lomas *et al.*, 1989] T. Mark A. Lomas, Li Gong, Jerome H. Saltzer, and Roger M. Needham. Reducing risks from poorly chosen keys. In *Proceedings of the Twelfth ACM Symposium on Operating Systems Principles*, pages 14–18. SIGOPS, December 1989. Cited on: *317*.

[Lottor, 1987] M. Lottor. Domain administrators operations guide. RFC 1033, Internet Engineering Task Force, November 1987. Cited on: *31*.
`http://www.rfc-editor.org/rfc/rfc1033.txt`

[MacAvoy, 1983] R. A. MacAvoy. *Tea with the Black Dragon*. Bantam Books, New York, 1983. Cited on: *98*.

A science fiction story of a rather different flavor.

[Mahajan *et al.*, 2002] R. Mahajan, Steven M. Bellovin, Sally Floyd, John Ioannidis, Vern Paxson, and Scott Shenker. Controlling high bandwidth aggregates in the network. *Computer Communications Review*, 32(3):62–73, July 2002. Cited on: *115*.
`http://www.icir.org/floyd/papers/pushback-CCR.ps`

[Malkin, 1994] G. Malkin. RIP version 2—carrying additional information. RFC 1723, Internet Engineering Task Force, November 1994. Cited on: *29, 29*.
`http://www.rfc-editor.org/rfc/rfc1723.txt`

[Markoff, 1989] John Markoff. Computer invasion: “back door” ajar. In *The New York Times*, Volume CXXXVIII, page B10, November 7, 1989. Cited on: *43*.

[Markoff, 1993] John Markoff. Keeping things safe and orderly in the neighborhood of cyberspace. In *The New York Times*, Volume CXLIII, page E7, October 24, 1993. Cited on: *16*.

[Martin *et al.*, 1997] David Martin, S. Rajagopalan, and Aviel D. Rubin. Blocking Java applets at the firewall. *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, pages 16–26, 1997. Cited on: *54, 90, 201, 202, 228*.

[Mayer *et al.*, 2000] A. Mayer, A. Wool, and E. Ziskind. Fang: A firewall analysis engine. In *Proceedings of the IEEE Computer Society Symposium on Security and Privacy*, pages 177–187, May 2000. Cited on: *212, 232*.

[McClure *et al.*, 2001] Stuart McClure, Joel Scambray, and George Kurtz. *Hacking Exposed: Network Security Secrets & Solutions, Third Edition*. McGraw-Hill, September 2001. Cited on: *131*.
`http://www.hackingexposed.com/`

[McGraw and Felten, 1999] Gary McGraw and Edward W. Felten. *Securing Java: Getting Down to Business with Mobile Code*. John Wiley & Sons, New York, 1999. Cited on: *81, 81*.
`http://www.securingjava.com`

[Menezes *et al.*, 1997] A. J. Menezes, P. V. Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997. Cited on: *335*.

[Merkle, 1990] Ralph C. Merkle. One way hash functions and DES. In *Advances in Cryptology: Proceedings of CRYPTO '89*, pages 428–446. Springer-Verlag, 1990. Cited on: *347*.

[Meyer, 1998] D. Meyer. Administratively scoped IP multicast. RFC 2365, Internet Engineering Task Force, July 1998. Cited on: *68*.
`http://www.rfc-editor.org/rfc/rfc2365.txt`

[Microsoft, 2002] Microsoft. Microsoft security bulletin 02-015, March 2002. Cited on: *79*.

[Miller, 2002] Jeremie Miller, 2002. Cited on: *46*.
`http://www.jabber.org`

Several Internet Drafts and revisions have been submitted to the IETF concerning *jabber*.

[Miller *et al.*, 1987] S. P. Miller, B. C. Neuman, J. I. Schiller, and J. H. Saltzer. Kerberos authentication and authorization system. In *Project Athena Technical Plan*. MIT, December 1987. Section E.2.1. Cited on: *11, 52, 314*.

[Mills, 1992] D. Mills. Network time protocol (version 3) specification, implementation. RFC 1305, Internet Engineering Task Force, March 1992. Cited on: *63*.
`http://www.rfc-editor.org/rfc/rfc1305.txt`

[Mitchell and Walker, 1988] Chris Mitchell and Michael Walker. Solutions to the multidestination secure electronic mail problem. *Computers & Security*, 7(5):483–488, 1988. Cited on: *347*.

[Mitnick *et al.*, 2002] Kevin D. Mitnick, William L. Simon, and Steve Wozniak. *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons, New York, 2002. Cited on: *100, 231*.

[Mockapetris, 1987a] P. V. Mockapetris. Domain names—concepts and facilities. RFC 1034, Internet Engineering Task Force, November 1987. Cited on: *31*.
`http://www.rfc-editor.org/rfc/rfc1034.txt`

[Mockapetris, 1987b] P. V. Mockapetris. Domain names—implementation and specification. RFC 1035, Internet Engineering Task Force, November 1987. Cited on: *31*.
`http://www.rfc-editor.org/rfc/rfc1035.txt`

[Mogul, 1989] J. C. Mogul. Simple and flexible datagram access controls for UNIX-based gateways. In *USENIX Conference Proceedings*, pages 203–221, Baltimore, MD, Summer 1989. Cited on: *229*.
`http://www.hpl.hp.com/techreports/Compaq-DEC/WRL-89-4.html`

A description of one of the first packet filters. Also see [Mogul, 1991].

[Mogul, 1991] J. C. Mogul. Using *screend* to implement IP/TCP security policies. Network Note NSL Technical Note TN-2, Digital Equipment Corp. Network Systems Laboratory, July 1991. Cited on: *374*.
`http://gatekeeper.dec.com/pub/DEC/WRL/technical-notes/nsltn2.pdf`

A longer version of [Mogul, 1989], with some worked examples.

[Mogul and Deering, 1990] J. C. Mogul and S. E. Deering. Path MTU discovery. RFC 1191, Internet Engineering Task Force, November 1990. Cited on: *27*.
`http://www.rfc-editor.org/rfc/rfc1191.txt`

[Monrose *et al.*, 2001] Fabian Monrose, Michael K. Reiter, Q. Peter Li, and Susanne Wetzel. Cryptographic key genereation from voice. In *Proceedings of the IEEE Computer Society Symposium on Security and Privacy*, May 2001. Cited on: *148*.

[Monrose and Rubin, 2000] Fabian Monrose and Aviel D. Rubin. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*, March 2000. Cited on: *148*.

[Moore *et al.*, 2001] D. Moore, G. M. Voelker, and S. Savage. Inferring internet Denial-of-Service activity. In *Proceedings of the 10th USENIX Security Symposium*, pages 9–22, Washington, D.C., USA, 2001. Cited on: *116*.
`http://www.caida.org/outreach/papers/2001/BackScatter/`

[Moore, 1988] J. H. Moore. Protocol failures in cryptosystems. *Proceedings of the IEEE*, 76(5):594–602, May 1988. Cited on: *313*.

[Morris and Thompson, 1979] R. H. Morris and K. Thompson. UNIX password security. *Communications of the ACM*, 22(11):594, November 1979. Cited on: *96, 96, 316*.

Gives the rationale for the design of the current UNIX password hashing algorithm.

[Morris, 1985] R. T. Morris. A weakness in the 4.2BSD UNIX TCP/IP software. Computing Science Technical Report 117, AT&T Bell Laboratories, Murray Hill, NJ, February 1985. Cited on: *23, 117*.
`http://netlib.bell-labs.com/cm/cs/cstr/117.ps.gz`

The original paper describing sequence number attacks.

[Moy, 1998] J. Moy. OSPF version 2. RFC 2328, Internet Engineering Task Force, April 1998. Cited on: *29*.
`http://www.rfc-editor.org/rfc/rfc2328.txt`

[Muffett, 1992] Alec D. E. Muffett. A sensible password checker for UNIX, 1992. Cited on: *96, 129*.

Available with the *Crack* package; see `http://www.users.dircon.co.uk/~crypto/download/c50-faq.html`.

[Myers, 1997] J. Myers. Simple authentication and security layer (SASL). RFC 2222, Internet Engineering Task Force, October 1997. Cited on: *148, 149*.
`http://www.rfc-editor.org/rfc/rfc2222.txt`

[Myers, 1999] J. Myers. SMTP service extension for authentication. RFC 2554, Internet Engineering Task Force, March 1999. Cited on: *43*.
`http://www.rfc-editor.org/rfc/rfc2554.txt`

[Myers and Rose, 1996] J. Myers and M. Rose. Post office protocol—version 3. RFC 1939, Internet Engineering Task Force, May 1996. Cited on: *44*.
`http://www.rfc-editor.org/rfc/rfc1939.txt`

[Myers *et al.*, 1999] M. Myers, C. Adams, D. Solo, and D. Kemp. Internet X.509 certificate request message format. RFC 2511, Internet Engineering Task Force, March 1999. Cited on: *322*.
`http://www.rfc-editor.org/rfc/rfc2511.txt`

[Narten and Draves, 2001] T. Narten and R. Draves. Privacy extensions for stateless address autoconfiguration in IPv6. RFC 3041, Internet Engineering Task Force, January 2001. Cited on: *35*.
`http://www.rfc-editor.org/rfc/rfc3041.txt`

[Narten *et al.*, 1998] T. Narten, E. Nordmark, and W. Simpson. Neighbor discovery for IP version 6 (IPv6). RFC 2461, Internet Engineering Task Force, December 1998. Cited on: *36*.
`http://www.rfc-editor.org/rfc/rfc2461.txt`

[NBS, 1977] NBS. Data encryption standard, January 1977. Federal Information Processing Standards Publication 46. Cited on: *48, 96, 337*.

The original DES standard. It's a bit hard to get, and most recent books on cryptography explain DES much more clearly. See, for example, [Schneier, 1996].

[NBS, 1980] NBS. DES modes of operation, December 1980. Federal Information Processing Standards Publication 81. Cited on: *337*.

The four officially approved ways in which DES can be used. Clearer explanations are available in most recent books on cryptography.

[Nechvatal, 1992] James Nechvatal. Public key cryptography. In Gustavus J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, pages 177–288. IEEE Press, Piscataway, NJ, 1992. Cited on: *347*.

[Needham and Schroeder, 1978] R. M. Needham and M. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, December 1978. Cited on: *149, 314, 363*.

The first description of a cryptographic authentication protocol. Also see [Denning and Sacco, 1981] and [Needham and Schroeder, 1987].

[Needham and Schroeder, 1987] R. M. Needham and M. Schroeder. Authentication revisited. *Operating Systems Review*, 21(1):7, January 1987. Cited on: *149, 314, 376*.

[Nemeth *et al.*, 2000] Evi Nemeth, Garth Snyder, Scott Seebass, and Trent R. Hein. *UNIX System Administration Handbook*. Prentice-Hall, Englewood Cliffs, NJ, Third Edition, 2000. Cited on: *123*.

[NetBIOS Working Group in the Defense Advanced Research Projects Agency *et al.*, 1987a] NetBIOS Working Group in the Defense Advanced Research Projects Agency, Internet Activities Board, and End-to-End Services Task Force. Protocol standard for a NetBIOS service on a TCP/UDP transport: Concepts and methods. RFC 1001, Internet Engineering Task Force, March 1987. Cited on: *57*.
`http://www.rfc-editor.org/rfc/rfc1001.txt`

[NetBIOS Working Group in the Defense Advanced Research Projects Agency *et al.*, 1987b] NetBIOS Working Group in the Defense Advanced Research Projects Agency, Internet Activities Board, and End-to-End Services Task Force. Protocol standard for a NetBIOS service on a TCP/UDP transport: Detailed specifications. RFC 1002, Internet Engineering Task Force, March 1987. Cited on: *57*.
`http://www.rfc-editor.org/rfc/rfc1002.txt`

[Neugent and Olson, 1985] H. William Neugent and Ingrid M. Olson. Technical rationale behind CSC-STD-003-83: Computer security requirements. DoD CSC-STD-004-85, DoD Computer Security Center, 1985. Cited on: *11*.

A lesser-known companion to the Orange Book [Brand, 1985]. It describes how to select a security assurance level based on the data on the system and the risks to which it is exposed.

[New and Rose, 2001] D. New and M. Rose. Reliable delivery for syslog. RFC 3195, Internet Engineering Task Force, November 2001. Cited on: *158*.
`http://www.rfc-editor.org/rfc/rfc3195.txt`

[Newman, 1997] C. Newman. Anonymous SASL mechanism. RFC 2245, Internet Engineering Task Force, November 1997. Cited on: *148*.
`http://www.rfc-editor.org/rfc/rfc2245.txt`

[Newman, 1998] C. Newman. The one-time-password SASL mechanism. RFC 2444, Internet Engineering Task Force, October 1998. Cited on: *148*.
`http://www.rfc-editor.org/rfc/rfc2444.txt`

[Newman, 1999] C. Newman. Using TLS with IMAP, POP3 and ACAP. RFC 2595, Internet Engineering Task Force, June 1999. Cited on: *171, 325*.
`http://www.rfc-editor.org/rfc/rfc2595.txt`

[NIST, 1993] NIST. Secure hash standard (SHS), May 1993. Federal Information Processing Standards Publication 180. Cited on: *326, 347*.

The algorithm is also described in [Schneier, 1996]. The original version was recalled by NSA; a new version incorporates a one-line fix.

[NIST, 1994] NIST. Digital signature standard (DSS), May 1994. Federal Information Processing Standards Publication 186. Cited on: *345*.

The algorithm is also described in [Schneier, 1996].

[NIST, 2001] NIST. Recommendation for block cipher modes of operation, 2001. NIST Special Publication 800-38A. Cited on: *337*.
`http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf`

[NIST, 2002] NIST. DRAFT recommendation for block cipher modes of operation: The RMAC authentication mode, 2002. NIST Special Publication 800-38B. Cited on: *346*.
`http://csrc.nist.gov/publications/drafts/draft800-38B-110402.pdf`

[Niven, 1968] Larry Niven. "Flatlander". In *Neutron Star*, pages 129–171. Ballantine Books, New York, NY, 1968. Cited on: *8*.

[Niven and Pournelle, 1994] Larry Niven and Jerry Pournelle. *The Mote in God's Eye*. Simon and Schuster, 1994. Cited on: *233*.

[Northcutt and Novak, 2000] Stephen Northcutt and Judy Novak. *Network Intrusion Detection: An Analyst's Handbook*. New Riders, Second Edition, 2000. Cited on: *108*.

[Ong and Yoakum, 2002] L. Ong and J. Yoakum. An introduction to the stream control transmission protocol (SCTP). RFC 3286, Internet Engineering Task Force, May 2002. Cited on: *25*.
`http://www.rfc-editor.org/rfc/rfc3286.txt`

[Orwell, 1949] George Orwell. *1984*. Harcourt, Brace, 1949. Cited on: *91*.

[Paxson, 1997] Vern Paxson. End-to-end routing behavior in the Internet. *IEEE/ACM Transactions on Networking*, 5(5):601–615, 1997. Cited on: *160*.
`ftp://ftp.ee.lbl.gov/papers/vp-routing-TON.ps.gz`

[Paxson, 1998] Vern Paxson. Bro: A system for detecting network intruders in real-time. *Proceedings of the Seventh USENIX Security Symposium*, pages 31–51, 1998. Cited on: *21, 279, 282*.

[Pike *et al.*, 1995] Rob Pike, David L. Presotto, Sean Dorward, Bob Flandrena, Ken Thompson, Howard Trickey, and Phil Winterbottom. Plan 9 from Bell Labs. *Computing Systems*, 8(3):221–254, Summer 1995. Cited on: *310*.
`http://www.cs.bell-labs.com/sys/doc/9.ps`

[Piscitello and Chapin, 1994] David M. Piscitello and A. Lyman Chapin. *Open Systems Networking: TCP/IP and OSI*. Addison-Wesley, Reading, MA, 1994. Cited on: *28*.

[Plummer, 1982] D. C. Plummer. An Ethernet address resolution protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware. RFC 826, Internet Engineering Task Force, November 1982. Cited on: *21*.
`http://www.rfc-editor.org/rfc/rfc826.txt`

[Postel, 1980] J. Postel. User datagram protocol. RFC 768, Internet Engineering Task Force, August 1980. Cited on: *27*.
`http://www.rfc-editor.org/rfc/rfc768.txt`

[Postel, 1981a] J. Postel. Internet control message protocol. RFC 792, Internet Engineering Task Force, September 1981. Cited on: *27*.
`http://www.rfc-editor.org/rfc/rfc792.txt`

[Postel, 1981b] J. Postel. Internet protocol. RFC 791, Internet Engineering Task Force, September 1981. Cited on: *19*.
`http://www.rfc-editor.org/rfc/rfc791.txt`

[Postel, 1981c] J. Postel. Transmission control protocol. RFC 793, Internet Engineering Task Force, September 1981. Cited on: *22*.
`http://www.rfc-editor.org/rfc/rfc793.txt`

[Postel and Reynolds, 1985] J. Postel and J. K. Reynolds. File transfer protocol. RFC 959, Internet Engineering Task Force, October 1985. Cited on: *53*.
`http://www.rfc-editor.org/rfc/rfc959.txt`

[Presotto, 1985] David L. Presotto. *Upas*—a simpler approach to network mail. In *USENIX Conference Proceedings*, pages 533–538, Portland, OR, Summer 1985. Cited on: *262*.

[Provos and Honeyman, 2001] Niels Provos and Peter Honeyman. Scanssh—scanning the internet for ssh servers. In *Sixteenth USENIX Systems Administration Conference (LISA)*, San Diego, 2001. Cited on: *275*.

[Ptacek and Newsham, 1998] Thomas H. Ptacek and Timothy N. Newsham. Insertion, evasion, and denial of service: Eluding network intrusion detection. Technical Report, Suite 330, 1201 5th Street S.W, Calgary, Alberta, Canada, T2R-0Y6, 1998. Cited on: *279*.

[Quisquater and Desmedt, 1991] J. Quisquater and Y. Desmedt. Chinese lotto as an exhaustive code-breaking machine. *Computer*, 24(11):14–22, November 1991. Cited on: *117*.

[Quittner and Slatalla, 1995] Joshua Quittner and Michele Slatalla. *Masters of Deception: The Gang That Ruled Cyberspace*. Harper-Collins, 1995. Cited on: *301*.

[Reiter, 1994] M. K. Reiter. Secure agreement protocols: Reliable and atomic group multicast in Rampart. In *Proceedings of the Second ACM Conference on Computer and Communications Security*, pages 68–80, November 1994. Cited on: *192*.

[Reiter, 1995] M. K. Reiter. The Rampart toolkit for building high-integrity services. In K. P. Birman, F. Mattern, and A. Schiper, editors, *Theory and Practice in Distributed Systems (Lecture Notes in Computer Science 938)*, pages 99–110. Springer-Verlag, 1995. Cited on: *192*.

[Rekhter *et al.*, 1996] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. Address allocation for private internets. RFC 1918, Internet Engineering Task Force, February 1996. Cited on: *37, 182, 183*.
`http://www.rfc-editor.org/rfc/rfc1918.txt`

[Rekhter *et al.*, 1997] Yakov Rekhter, Paul Resnick, and Steven M. Bellovin. Financial incentives for route aggregation and efficient address utilization in the internet. In *Proceedings of Telecommunications Policy Research Conference*, Solomons, MD, 1997. Cited on: *330*.
`http://www.research.att.com/~smb/papers/piara/index.html`

[Rescorla, 2000a] E. Rescorla. HTTP over TLS. RFC 2818, Internet Engineering Task Force, May 2000. Cited on: *324*.
`http://www.rfc-editor.org/rfc/rfc2818.txt`

[Rescorla, 2000b] Eric Rescorla. *SSL and TLS: Designing and Building Secure Systems*. Addison-Wesley, 2000. Cited on: *45, 77, 83, 323*.

[Resnick, 2001] P. Resnick, editor. Internet message format. RFC 2822, Internet Engineering Task Force, April 2001. Cited on: *43*.
`http://www.rfc-editor.org/rfc/rfc2822.txt`

[Reynolds, 1989] J. K. Reynolds. Helminthiasis of the internet. RFC 1135, Internet Engineering Task Force, December 1989. Cited on: *206*.
`http://www.rfc-editor.org/rfc/rfc1135.txt`

[Rigney *et al.*, 1997] C. Rigney, A. Rubens, W. Simpson, and S. Willens. Remote authentication dial in user service (RADIUS). RFC 2138, Internet Engineering Task Force, April 1997. Cited on: *148*.
`http://www.rfc-editor.org/rfc/rfc2138.txt`

[Rivest, 1992a] R. Rivest. The MD4 message-digest algorithm. RFC 1320, Internet Engineering Task Force, April 1992. Cited on: *149*.
`http://www.rfc-editor.org/rfc/rfc1320.txt`

[Rivest, 1992b] R. Rivest. The MD5 message-digest algorithm. RFC 1321, Internet Engineering Task Force, April 1992. Cited on: *326, 347*.
`http://www.rfc-editor.org/rfc/rfc1321.txt`

[Rivest and Shamir, 1984] Ronald L. Rivest and Adi Shamir. How to expose an eavesdropper. *Communications of the ACM*, 27(4):393–395, 1984. Cited on: *344*.

[Rivest *et al.*, 1978] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A method of obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978. Cited on: *342*.

The original RSA paper.

[Rochlis and Eichin, 1989] J. A. Rochlis and M. W. Eichin. With microscope and tweezers: the worm from MIT's perspective. *Communications of the ACM*, 32(6):689–703, June 1989. Cited on: *43, 100*.
`ftp://athena-dist.mit.edu/pub/virus/mit.PS`

There are several other stories on the Worm in this issue of CACM.

[Roesch, 1999] Martin Roesch. Writing snort rules, 1999. Cited on: *282*.
`http://www.snort.org/docs/writing_rules/`

[Rosenberg *et al.*, 2002] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: session initiation protocol. RFC 3261, Internet Engineering Task Force, June 2002. Cited on: *46*.
`http://www.rfc-editor.org/rfc/rfc3261.txt`

[Rosenberry *et al.*, 1992] Ward Rosenberry, David Kenney, and Gerry Fisher. *Understanding DCE*. O'Reilly, Sebastopol, CA, 1992. Cited on: *48*.

[Rosenblatt, 1995] Kenneth Rosenblatt. *High-Technology Crime: Investigating Cases Involving Computers*. KSK Publications, 1995. Cited on: *311*.

[RSA Laboratories, 2002] RSA Laboratories. PKCS #1—RSA cryptography standard, 2002. Version 2.1. Cited on: *343*.
`http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html`

[Rubin, 1995] Aviel D. Rubin. Trusted distribution of software over the Internet. In *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, pages 47–53, 1995. Cited on: *270*.

[Rubin, 2001] Aviel D. Rubin. *White-Hat Security Arsenal: Tackling the Threats*. Addison-Wesley, Reading, MA, 2001. Cited on: *106*.

[Rubin *et al.*, 1997] Aviel D. Rubin, Daniel Geer, and Marcus J. Ranum. *Web Security Sourcebook*. John Wiley & Sons, Inc., 1997. Cited on: *91*.

[Safford *et al.*, 1993] David R. Safford, Douglas Lee Schales, and David K. Hess. The TAMU security package: An ongoing response to Internet intruders in an academic environment. In *Proceedings of the Fourth USENIX* UNIX *Security Symposium*, pages 91–118, Santa Clara, CA, October 1993. Cited on: *289*.

A detailed look at a hacker's activities in a university environment—and what they did to stop them. The paper is available for *ftp* as part of the TAMU security package.

[Savage *et al.*, 2000] Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson. Practical network support for IP traceback. *ACM SIGCOMM '00*, pages 295–306, 2000. Cited on: *114*.

[Scheifler and Gettys, 1992] Robert W. Scheifler and James Gettys. *X Window System*. Digital Press, Burlington, MA, Third Edition, 1992. Cited on: *70*.

[Schneider, 1999] Fred B. Schneider, editor. *Trust in Cyberspace*. National Academy Press, 1999. Cited on: *331*.

[Schneier, 1996] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, New York, Second Edition, 1996. Cited on: *335, 375, 377, 377*.

A comprehensive collection of cryptographic algorithms, protocols, and so on. Source code is included for many of the most important algorithms.

[Schneier, 2000] Bruce Schneier. *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons, Inc., 2000. Cited on: *7, 228*.

[Schneier and Mudge, 1998] Bruce Schneier and Mudge. Cryptanalysis of Microsoft's point-to-point tunneling protocol (PPTP). In *Proceedings of the Fifth ACM Conference on Computer and Communications Security*, pages 132–141, November 1998. Cited on: *241*.

[Schulzrinne *et al.*, 1996] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RTP: a transport protocol for real-time applications. RFC 1889, Internet Engineering Task Force, January 1996. Cited on: *215*.
`http://www.rfc-editor.org/rfc/rfc1889.txt`

[Selzer, 1957] Edward Selzer. Ali baba bunny, 1957. Cited on: *138*.

[Senie, 2002] D. Senie. Network address translator (nat)-friendly application design guidelines. RFC 3235, Internet Engineering Task Force, January 2002. Cited on: *38*.
`http://www.rfc-editor.org/rfc/rfc3235.txt`

[Seuss, 1957] Dr. Seuss. *The Cat in the Hat*. Random House, 1957. Cited on: *301*.

[Seuss, 1960] Dr. Seuss. *One Fish, Two Fish, Red Fish, Blue Fish*. Random House, 1960. Cited on: *107*.

[Shamir, 1979] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979. Cited on: *15*.

[Shannon, 1948] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(3,4):379–423,623–656, July, October 1948. Cited on: *96*.

[Shannon, 1949] Claude E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, October 1949. Cited on: *96*.

[Shannon, 1951] Claude E. Shannon. Prediction and entropy in printed English. *Bell System Technical Journal*, 30(1):50–64, 1951. Cited on: *96*.

One of the classic papers in information theory.

[Shepler *et al.*, 2000] S. Shepler, B. Callaghan, D. Robinson, R. Thurlow, C. Beame, M. Eisler, and D. Noveck. NFS version 4 protocol. RFC 3010, Internet Engineering Task Force, December 2000. Cited on: *50*.
`http://www.rfc-editor.org/rfc/rfc3010.txt`

[Shimomura, 1996] Tsutomu Shimomura. *Takedown*. Hyperion, 1996. Cited on: *xiii, 23, 308*.

[Shostack, 1997] Adam Shostack, 1997. Cited on: *170*.
`http://www.homeport.org/~adam/dns.html`

[Simpson, 1994] W. Simpson, editor. The point-to-point protocol (PPP). RFC 1661, Internet Engineering Task Force, July 1994. Cited on: *235*.
`http://www.rfc-editor.org/rfc/rfc1661.txt`

[Smart *et al.*, 2000] M. Smart, G. R. Malan, and F. Jahanian. Defeating TCP/IP stack fingerprinting. *USENIX Security Conference IX*, pages 229–239, 2000. Cited on: *130*.

[Smith and Garcia-Luna-Aceves, 1996] B. Smith and J. Garcia-Luna-Aceves. Securing the Border Gateway Routing Protocol. In *Proceedings of Global Internet '96*, pages 103–116, November 1996. Cited on: *30*.

[Smith, 1987] S. L. Smith. Authenticating users by word association. *Computers and Security*, 6:464–470, 1987. Cited on: *142*.

[Sollins, 1992] K. Sollins. The TFTP protocol (revision 2). RFC 1350, Internet Engineering Task Force, July 1992. Cited on: *52*.
`http://www.rfc-editor.org/rfc/rfc1350.txt`

[Somayaji and Forrest, 2000] A. Somayaji and S. Forrest. Automated response using system-call delays. *USENIX Security Conference*, pages 185–197, 2000. Cited on: *281*.
`http://cs.unm.edu/~forrest/publications/uss-2000.ps`

[Song *et al.*, 2001] Dawn Xiaodong Song, David A. Wagner, and Xuquing Tian. Timing analysis of keystrokes and timing attacks on SSH. *Proceedings of the USENIX Security Symposium*, pages 337–352, 2001. Cited on: *154*.

[Song *et al.*, 1999] Dug Song, G. Shaffer, and M. Undy. Nidsbench—a network intrusion detection test suite. In *Recent Advances in Intrusion Detection*, 1999. Cited on: *231, 280*.

[Spafford, 1989a] Eugene H. Spafford. An analysis of the Internet worm. In C. Ghezzi and J. A. McDermid, editors, *Proceedings of the European Software Engineering Conference*, number 387 in Lecture Notes in Computer Science, pages 446–468, Warwick, England, September 1989. Springer-Verlag. Cited on: *43, 100*.
`http://ftp.cerias.purdue.edu/pub/doc/morris_worm/spaf-IWorm-paper-ESEC.ps.Z`

The timeline and effects of the Worm.

[Spafford, 1989b] Eugene H. Spafford. The Internet worm program: an analysis. *Computer Communication Review*, 19(1):17–57, January 1989. Cited on: *43, 100*.
`http://ftp.cerias.purdue.edu/pub/doc/morris_worm/spaf-IWorm-paper-CCR.ps.Z`

A detailed description of how the Worm worked.

[Spafford, 1992] Eugene H. Spafford. OPUS: Preventing weak password choices. *Computers & Security*, 11(3):273–278, 1992. Cited on: *96*.
`ftp://coast.cs.purdue.edu/pub/Purdue/papers/spafford/spaf-OPUS.ps`

Discusses how to use Bloom filters to check passwords against dictionaries without consuming large amounts of space.

[Spencer and Collyer, 1992] H. Spencer and G. Collyer. #ifdefs considered harmful, or portability experience with C news. In *Proceedings of the Summer USENIX Conference*, pages 185–198, San Antonio, TX, 1992. Cited on: *154*.

[Spitzner, 2002] Lance Spitzner. *Honeypots: Tracking Hackers*. Addison Wesley, 2002. Cited on: *130, 281*.

[Srinivasan, 1995] R. Srinivasan. RPC: remote procedure call protocol specification version 2. RFC 1831, Internet Engineering Task Force, August 1995. Cited on: *47*.
`http://www.rfc-editor.org/rfc/rfc1831.txt`

[Srisuresh and Egevang, 2001] P. Srisuresh and K. Egevang. Traditional IP network address translator (traditional NAT). RFC 3022, Internet Engineering Task Force, January 2001. Cited on: *37, 37*.
`http://www.rfc-editor.org/rfc/rfc3022.txt`

[Srisuresh and Holdrege, 1999] P. Srisuresh and M. Holdrege. IP network address translator (NAT) terminology and considerations. RFC 2663, Internet Engineering Task Force, August 1999. Cited on: *37*.
`http://www.rfc-editor.org/rfc/rfc2663.txt`

[Stahl, 1987] M. K. Stahl. Domain administrators guide. RFC 1032, Internet Engineering Task Force, November 1987. Cited on: *31*.
`http://www.rfc-editor.org/rfc/rfc1032.txt`

[Staniford *et al.*, 2002] Stuart Staniford, Vern Paxson, and Nicholas Weaver. How to own the Internet in your spare time. In *Proceedings of the 11th USENIX Security Symposium*, San Francisco, CA, USA, 2002. Cited on: *106, 117*.
`http://www.icir.org/vern/papers/cdc-usenix-sec02/`

[Stein, 1997] Lincoln D. Stein. *How to Set Up and Maintain a Web Site*. Addison-Wesley, Reading, MA, Second Edition, 1997. Cited on: *74*.

[Stein, 1999] Lincoln D. Stein. SBOX: Put CGI scripts in a box. *In Proceedings of the 1999 USENIX Technical Conference*, pages 145–156, 1999. Cited on: *86*.

[Steiner *et al.*, 1988] Jennifer Steiner, B. Clifford Neuman, and Jeffrey I. Schiller. Kerberos: An authentication service for open network systems. In *Proceedings of the Winter USENIX Conference*, pages 191–202, Dallas, TX, 1988. Cited on: *11, 52, 314*.

The original Kerberos paper. Available as part of the Kerberos distribution.

[Sterling, 1992] Bruce Sterling. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Bantam Books, New York, 1992. Cited on: *xix*.
`http://gopher.well.com:70/1/Publications/authors/Sterling/hc`

A description of how law enforcement agents went overboard, though often in response to real threats.

[Stevens, 1995] W. Richard Stevens. *TCP/IP Illustrated*, Volume 1. Addison-Wesley, Reading, MA, 1995. Cited on: *19, 27*.

Uses *tcpdump* to show *how* the protocols work.

[Stevens, 1996] W. Richard Stevens. *TCP/IP Illustrated: TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols*, Volume 3. Addison-Wesley, Reading, MA, 1996. Cited on: *19*.

[Stewart, 1999] John W. Stewart. *BGP4 Inter-Domain Routing in the Internet*. Addison-Wesley, January 1999. Cited on: *29*.

[Stewart *et al.*, 2000] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson. Stream control transmission protocol. RFC 2960, Internet Engineering Task Force, October 2000. Cited on: *25*.
`http://www.rfc-editor.org/rfc/rfc2960.txt`

[Stinson, 1995] Douglas Stinson. *Cryptography: Theory and Practice*. CRC Press, Inc, 1995. Cited on: *335*.

[Stoll, 1988] Cliff Stoll. Stalking the wily hacker. *Communications of the ACM*, 31(5):484, May 1988. Cited on: *159, 293*.

[Stoll, 1989] Cliff Stoll. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Doubleday, New York, 1989. Cited on: *159, 293*.

A good read, and the basis for an episode of Nova.

[Stone, 2000] Robert Stone. CenterTrack: An IP overlay network for tracking DoS floods. In *Proceedings of the Ninth USENIX Security Symposium*, August 2000. Cited on: *114*.
`http://www.usenix.org/publications/library/proceedings/sec2000/full_papers/stone/stone.ps`

[Stubblefield *et al.*, 2002] Adam Stubblefield, John Ioannidis, and Aviel D. Rubin. Using the Fluhrer, Mantin, and Shamir attack to break WEP. In *Proceedings of the 2002 Network and Distributed Systems Security Symposium*, pages 17–22, San Diego, California, February 2002. Cited on: *39*.

[Sun Microsystems, 1987] Sun Microsystems. XDR: external data representation standard. RFC 1014, Internet Engineering Task Force, June 1987. Cited on: *48*.
`http://www.rfc-editor.org/rfc/rfc1014.txt`

[Sun Microsystems, 1990] Sun Microsystems. *Network Interfaces Programmer's Guide*. Mountain View, CA, March 1990. SunOS 4.1. Cited on: *47, 50*.

[Thayer *et al.*, 1998] R. Thayer, N. Doraswamy, and R. Glenn. IP security document roadmap. RFC 2411, Internet Engineering Task Force, November 1998. Cited on: *318*.
`http://www.rfc-editor.org/rfc/rfc2411.txt`

[Thomas and Vilhuber, 2002] M. Thomas and J. Vilhuber. Kerberized Internet negotiation of keys (KINK), 2002. Work in progress. Cited on: *320*.

[Tolkien, 1965] J. R. R. Tolkien. *Lord of the Rings*. Ballantine Books, New York, 1965. Cited on: *xiii, 73, 95, 137, 332*.

[Townsley *et al.*, 1999] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, and B. Palter. Layer two tunneling protocol "L2TP". RFC 2661, Internet Engineering Task Force, August 1999. Cited on: *234*.
http://www.rfc-editor.org/rfc/rfc2661.txt

[Treese and Wolman, 1993] Win Treese and Alec Wolman. X through the firewall, and other application relays. In *USENIX Conference Proceedings*, pages 87–99, Cincinnati, OH, June 1993. Cited on: *188*.

[Tsirtsis and Srisuresh, 2000] G. Tsirtsis and P. Srisuresh. Network address translation—protocol translation (NAT-PT). RFC 2766, Internet Engineering Task Force, February 2000. Cited on: *37*.
http://www.rfc-editor.org/rfc/rfc2766.txt

[Ts'o, 2000] T. Ts'o. Telnet data encryption option. RFC 2946, Internet Engineering Task Force, September 2000. Cited on: *59*.
http://www.rfc-editor.org/rfc/rfc2946.txt

[Vaha-Sipila, 2000] A. Vaha-Sipila. URLs for telephone calls. RFC 2806, Internet Engineering Task Force, April 2000. Cited on: *78*.
http://www.rfc-editor.org/rfc/rfc2806.txt

[Vincenzetti *et al.*, 1995] David Vincenzetti, Stefano Taino, and Fabio Bolognesi. STEL: Secure TELnet. In *Proceedings of the Fifth USENIX* UNIX *Security Symposium*, Salt Lake City, UT, 1995. Cited on: *59*.

[Violino, 1993] Bob Violino. Hackers. *Information Week*, 430:48–56, June 21, 1993. Cited on: *131*.

A discussion of the wisdom and prevalence of hiring hackers as security experts.

[Vixie, 1999] P. Vixie. Extension mechanisms for DNS (EDNS0). RFC 2671, Internet Engineering Task Force, August 1999. Cited on: *33*.
http://www.rfc-editor.org/rfc/rfc2671.txt

[Voyager, 1994] Voyager. Janitor privileges. *2600*, Winter(5), 1994. Cited on: *8*.

[Voydock and Kent, 1983] V. L. Voydock and S. T. Kent. Security mechanisms in high-level network protocols. *ACM Computing Surveys*, 15(2):135–171, June 1983. Cited on: *339*.

[Wagner and Schneier, 1996] David A. Wagner and Bruce Schneier. Analysis of the SSL 3.0 protocol. *Proceedings of the Second USENIX Workshop on Electronic Commerce*, pages 29–40, November 1996. Cited on: *325*.

[Wahl *et al.*, 2000] M. Wahl, H. Alvestrand, J. Hodges, and R. Morgan. Authentication methods for LDAP. RFC 2829, Internet Engineering Task Force, May 2000. Cited on: *65*.
http://www.rfc-editor.org/rfc/rfc2829.txt

[Waitzman, 1990] D. Waitzman. Standard for the transmission of IP datagrams on avian carriers. RFC 1149, Internet Engineering Task Force, April 1990. Cited on: *235*.
`http://www.rfc-editor.org/rfc/rfc1149.txt`

[Waitzman, 1999] D. Waitzman. IP over avian carriers with quality of service. RFC 2549, Internet Engineering Task Force, April 1999. Cited on: *235*.
`http://www.rfc-editor.org/rfc/rfc2549.txt`

[Winkler and Dealy, 1995] Ira S. Winkler and Brian Dealy. Information security technology? Don't Rely on It. A case study in social engineering. In *Proceedings of the Fifth USENIX UNIX Security Symposium*, Salt Lake City, UT, June 1995. Cited on: *122, 231*.

[Winternitz, 1984] Robert S. Winternitz. Producing a one-way hash function from DES. In *Advances in Cryptology: Proceedings of CRYPTO '83*, pages 203–207. Plenum Press, 1984. Cited on: *347*.

[Woodward and Bernstein, 1974] Carl Woodward and Robert Bernstein. *All the President's Men*. Simon and Schuster, New York, 1974. Cited on: *105*.

[Wray, 2000] J. Wray. Generic security service API version 2: C-bindings. RFC 2744, Internet Engineering Task Force, January 2000. Cited on: *327*.
`http://www.rfc-editor.org/rfc/rfc2744.txt`

[Wright and Stevens, 1995] Gary R. Wright and W. Richard Stevens. *TCP/IP Illustrated: The Implementation*, Volume 2. Addison-Wesley, Reading, MA, 1995. Cited on: *19*.

A walk through the 4.4BSD implemenation of TCP/IP.

[Wu and Wong, 1998] David Wu and Frederick Wong. Remote sniffer detection, 1998. Cited on: *159*.
`http://citeseer.nj.nec.com/wu98remote.html`

Nice work. A shame it wasn't submitted for publication.

[Wu, 1999] Thomas Wu. A real-world analysis of kerberos password security. *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, pages 13–22, 1999. Cited on: *96, 315, 317*.

[Ye and Smith, 2002] Zishuang Ye and Sean Smith. Trusted paths for browsers. *Proceedings of the Eleventh USENIX Security Symposium*, pages 263–279, 2002. Cited on: *82*.

[Yeong *et al.*, 1995] W. Yeong, T. Howes, and S. Kille. Lightweight directory access protocol. RFC 1777, Internet Engineering Task Force, March 1995. Cited on: *64, 65*.
`http://www.rfc-editor.org/rfc/rfc1777.txt`

[Ylönen, 1996] Tatu Ylönen. SSH—secure login connections over the internet. In *Proceedings of the Sixth USENIX* UNIX *Security Symposium*, pages 37–42, July 1996. Cited on: *59, 61, 322*.

Description of a cryptographic replacement for *rlogin* and *rsh*.

[Yuan and Strayer, 2001] Ruixi Yuan and W. Timothy Strayer. *Virtual Private Networks: Technologies and Solutions*. Addison-Wesley, Reading, MA, 2001. Cited on: *233*.

[Zalewski, 2002] Michal Zalewski. Strange attractors and tcp/ip sequence number analysis - one year later, 2002. Cited on: *24*.
`http://lcamtuf.coredump.cx/newtcp/`

[Ziemba *et al.*, 1995] G. Ziemba, D. Reed, and P. Traina. Security considerations for IP fragment filtering. RFC 1858, Internet Engineering Task Force, October 1995. Cited on: *21*.
`http://www.rfc-editor.org/rfc/rfc1858.txt`