CHAPTER NOTES

This appendix identifies the sources for information in this book. The notes do not amplify the technical information in the text—they only identify sources. Follow the marker from the text if you need to identify the source of a particular piece of information.

If you want to review all of a chapter's notes, then you should simply read the chapter's notes from start to finish once you've read the chapter's text.

These notes contain only the title and author for each source. Full citations appear in the **Bibliography**. If an item contains no author's name and is the product of a particular company, government agency, or other institution, then I list the institution as the author. If the note refers to a vendor or a Web site, check the book's **Web and Vendor Resources** section for contact information and URLs.

NOTES FOR CHAPTER 1

1. Scholars disagree about how and when the tale of Ali Baba was added to the centuries-old compendium called *The Thousand and One Nights*, or just *The Arabian Nights*. Sir Richard Francis Burton published the classic English translation of those folk tales in the 1880s. Burton added Ali Baba's story to the collection in a supplementary edition. The story was probably copied from a 19th-century Hindustani version of *Hazar Dastan* ("The Thousand Tales") compiled by Totaram Shåyåm. Jack Zipes of the University of Minnesota included Ali Baba's story in his abridged edition of Burton's translation.
2. Standards of due care form a central theme of Donn Parker's important book *Fighting Computer Crime*. The concept is also discussed in the classic book *Firewalls and Internet Security: Repelling the Wily Hacker* by Bill Cheswick and Steve Bellovin.
3. The federal standard for risk analysis was published by the National Bureau of Standards (NBS) in FIPS Publication 65, "Guideline for Automatic Data Processing Risk Analysis," though this official approach was withdrawn in 1995. Tom Peltier's book *Information Security Risk Analysis* provides a step-by-step approach to risk analysis. The Computer Emergency Response Team (CERT) has also developed a risk analysis method, described in the paper "An Introduction to the OCTAVE Method" by Alberts

and Dorofee. Parker discusses risk analysis in *Fighting Computer Crime*, though he does not recommend the practice.

4. The description of CTSS and the introduction of passwords is based on reminiscences of CTSS provided to this author in private communications from Fernando J. Corbató, Richard Mills, and Tom Van Vleck.
5. See Steve Levy's book *Hackers: Heroes of the Computer Revolution* for the evolution of hacker culture, particularly at MIT. See Joseph Weizenbaum's *Computer Power and Human Reason* for a less flattering portrayal of the extremes of computer obsession. Weizenbaum didn't object to "hackers" per se, but in Chapter 4 he portrayed "compulsive programming" as a disorder similar to compulsive gambling.
6. The CTSS story served as a major example in Fernando J. Corbató's Turing Award lecture, "On building systems that will fail." Tom Van Vleck provided additional details in his Multics stories "Multics: Security" and "The IBM 7094 and CTSS," and also in private communications with this author.
7. Maurice Wilkes described the Titan timesharing system (which he referred to as "the Cambridge system") in his book *Timesharing Computer Systems.*
8. Wilkes published the earliest known description of "one-way encryption" in his book *Timesharing Computer Systems* and attributed the idea to R. M. Needham. In a private communication with this author, Roger Needham described the origin of the concept and gave credit to Mike Guy.
9. Tom Van Vleck recounts the story of the weak Multics password hash in the "Multics: Security" story on his Multicians Web site.
10. The "Trusted Computer System Evaluation Criteria" (also called the TCSEC or even "the Orange Book"), written by the National Computer Security Center (NCSC), provides a classic outline of requirements for high-security systems. The NCSC also published the report "A Guide to Audit in Trusted Systems" to further describe how auditing should operate.
11. Jerry Neal Schneider's story is told by Donn Parker in *Crime by Computer*.
12. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, by Katie Hafner and John Markoff, tells the story of the "cheerful technician."
13. CERT reported this attack in CERT Advisory CA-1991-03, "Unauthorized Password Change Requests Via Mail Messages." The e-mail message in the text was copied from the CERT Advisory, misspellings and all.
14. Leo Marks described his wartime experiences with duress signals in his book *Between Silk and Cyanide*.
15. Michael J. McCarthy described business use of keystroke monitors in his *Wall Street Journal* article "Thinking Out Loud."
16. CERT issued their Advisory CA-1994-01, "Ongoing Network Monitoring Attacks," to report the sniffer attacks and recommend countermeasures. Eugene Schultz and Thomas Longstaff described the attacks in their paper "Internet Sniffer Attacks."
17. The TCSEC establishes the requirement to provide a "secure attention" signal as a countermeasure against attacks like Trojan login programs.
18. Wim van Eck's paper was entitled "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?"

19. Win Schwartau described his efforts and concerns with van Eck radiation in Chapter 7 of his book *Information Warfare*.
20. The earliest reference that this author has seen to the characterization of three authentication factors is in FIPS PUB 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974." The factors were also reviewed in detail in the 1988 paper "Alternate Authentication Mechanisms" by Steven Carlton, John Taylor, and John Wyszynski of the NCSC.
21. There are many books describing trivial and common attacks (and more), from how-to guides like *The Happy Hacker*, by Carolyn Meinel, to preventative guides like *Maximum Security*, authored by Anonymous.
22. Clifford Stoll's experiences with the Wily Hacker were entertainingly described in his best-seller *The Cuckoo's Egg*.
23. The Brookings Institution has published two books describing nuclear command and control: *Managing Nuclear Operations*, edited by Carter, Steinbruner, and Zraket, and *The Logic of Accidental Nuclear War*, by Bruce G. Blair. Ross Anderson provides a good summary in Chapter 11 of his book *Security Engineering: A Guide to Building Dependable Distributed Systems*.

NOTES FOR CHAPTER 2

1. The book *Techniques of Safecracking* by Wayne B. Yeager provides an appendix with try-out combinations for eight different manufacturers. Chapter 2 discusses the search for written-down combinations as a safecracking technique. Also see the chapter "Safecracker Meets Safecracker" in *"Surely You're Joking, Mr. Feynman!"* by physicist Richard Feynman.
2. CERT reported on a similar problem on the Unisys U5000 Unix systems in their Advisory CA-1990-03.
3. For information about locks and keys, see *The Complete Guide to Lock Picking* by Eddie the Wire, or *The Complete Book of Locks and Locksmithing*, by Roper and Phillips. Jerry Neal Schneider's story is told by Donn Parker in *Crime by Computer*.
4. See *A Quarter Century of Unix* by Peter H. Salus for the early evolution of Unix.
5. See "Multics—The First Seven Years" by Corbató, Saltzer, and Clingen for an overview of Multics.
6. Lions' commentary was published in two parts: "A Commentary on the Unix Operating System," and "Unix Operating System Source Code Level Six." Although AT&T vigorously discouraged its distribution, the commentary achieved a fairly wide, if underground, audience. The commentary was groundbreaking in that it presented source code as "published," readable material. Similar listings are published today, like the *Linux Core Kernel Commentary* by Scott Maxwell.
7. The classic paper "Password Security: A Case History," by Robert Morris and Ken Thompson, presents an overview of the early development of Unix password security.
8. See "File Security and the Unix Crypt Command" by Reeds and Weinberger.

9. Bruce Schneier discussed the risks of modifying existing algorithms in his paper "Why Cryptography Is Harder Than It Looks."
10. Daniel Klein performed an elaborate experiment to assess trial-and-error attacks on passwords and described it in the paper "A Survey of, and Improvements to, Password Security." See nearby notes for the other sources.
11. See "UNIX Password Security—Ten Years Later" by David C. Feldmeier and Philip R. Karn for a description of the evolving attack against DES crypt().
12. An early observation of the dictionary attack problem appears in the paper "A User Authentication Scheme Not Requiring Secrecy in the Computer" by Arthur Evans, William Kantrowitz, and Edwin Weiss.
13. Peter Denning edited the book *Computers Under Attack: Intruders, Worms, and Viruses*, which reprints several classic reports on the Internet Worm. The article "With Microscope and Tweezers: The Worm from MIT's Perspective" by Jon Rochlis and Mark Eichin gives a "blow-by-blow" account of the infection and recovery.

    Note that there are two people named "Robert Morris" to keep track of in this book. Robert T. Morris, the Worm's author, is the son of Robert H. Morris, coauthor of "Password Security: A Case History." References to the son in this book will always include his first name and middle initial.
14. Eugene Spafford's article "Crisis and Aftermath" provides a detailed description of the Internet Worm's operation.
15. John Shoch and Jon Hupp report on pioneering experiences (good and bad) at Xerox PARC with worm programs in "The 'Worm' Programs—Early Experiences with a Distributed Computation." Rochlis and Eichin's article, noted earlier, describes how various network managers at MIT dealt with the Internet Worm.
16. Ray Kaplan described the back door in VMS login in a memorable Usenet posting titled "Diary of a Security Incident." CERT reported the problem in the Advisory CA-1992-14. The Interbase problem was reported in CERT Advisory CA-2001-01.
17. See *Firewalls and Internet Security* by Cheswick and Bellovin for a thorough examination of how firewalling works.
18. *Firewalls* by Cheswick and Bellovin also discusses how chroot() can protect Internet servers. This author's paper "Mandatory Protection for Internet Server Software" compares chroot() with other encapsulation technologies for protecting a host against buffer overruns in a server.
19. Both CERT and CIAC have public Web sites where they post announcements of security incidents, problems, and fixes. See the section **Web and Vendor Resources** for URLs.
20. The *Department of Defense Password Management Guideline* was authored by the NCSC in 1985.

NOTES FOR CHAPTER 3

1. Financial fraud statistics can be found in reports like the "Financial Institution Fraud and Failure Report: Fiscal Year 1998," produced by the Federal

Bureau of Investigation (FBI). The report by the CSI/FBI is published as the "2001 FBI/CSI Computer Crime and Security Survey."

2. In the "Project MAC Progress Report III" from MIT, Mills and Van Vleck gave a report on CTSS security that commented briefly on local hacker activity.
3. Donn Parker recounted this story of "Val Smith (not his real name)" in Chapter 9 of *Crime by Computer*.
4. See CERT Advisory CA-1994-01, "Ongoing Network Monitoring Attacks."
5. The story of fraud on optical telegraph systems was retold in Chapter 2 of *The Early History of Data Networks* by Holzmann and Pehrson. Similar stories involving electrical telegraph systems appear in *The Victorian Internet* by Tom Standage.
6. A form of "mind reading" was widely practiced by "spirit mediums" up to the early 20th century. The famous magician Harry Houdini published a book *A Magician Among the Spirits* which described their techniques for gathering information in Chapter 20.
7. The AT&T experience is described in "Password Security: A Case History" by Morris and Thompson. The Purdue experience is described in "Observing Reusable Password Choices" by Eugene Spafford. This author's own studies of password writing and hiding are described in Chapter 6.
8. Estimates of entropy in English text often appear in cryptographic references, notably *Cryptography Theory and Practice*, by Douglas Stinson (Chapter 2) and *Applied Cryptography: Protocols, Algorithms, and Source Code in C* by Bruce Schneier.
9. These password dictionaries came from the "Security Tools and Techniques Library," a CD-ROM produced by the Forum of Incident Response and Security Teams (FIRST).
10. Eugene Spafford's article "Crisis and Aftermath" provides details of the Internet Worm's dictionary attack.
11. Klein's paper "A Survey of, and Improvements to, Password Security" describes his experiments.
12. The size given for Klein's password space is an estimate based on the description in his paper. Klein does not report the actual password space size.
13. Spafford's password study was described in his report "Observing Reusable Password Choices."
14. The 1998 incident was reported as CERT Incident IN-98-03, "Password Cracking Activity." The study by Yan, Blackwell, Anderson, and Grant is titled "The Memorability and Security of Passwords—Some Empirical Results."
15. Crack is described in the paper "CRACK: A Distributed Password Advisor" by Raleigh and Underwood. The l0phtcrack tool is described by its FAQ, written by "l0pht." Dan Farmer's security assessment tool, SATAN, was described in CERT Advisory CA-1995-06.
16. Randall Schwartz provides a lot of material on his Web site regarding the Intel case, including material from his trial and links to information on other sites.
17. NIST published FIPS 181, "Automated Password Generator," in 1993.

18. Morris and Thompson described the weak password generator in their paper "Password Security: A Case History."
19. Ganesan and Davies describe an attack on FIPS 181 password generators in their paper "A New Attack on Random Pronounceable Password Generators."
20. Klein described his strategy for proactive checking in his paper "A Survey of, and Improvements to, Password Security."
21. Spafford describes OPUS in his paper "OPUS: Preventing Weak Password Choices."
22. Both Windows NT and Windows 2000 can enforce password complexity constraints as described in the Microsoft Knowledge Base article Q161990, "How to Enable Strong Password Functionality in Windows NT."
23. Comments by Gen. Eugene E. Habiger, USAF (ret.), were quoted by Vernon Loeb in the story "Energy Chief Touts Security Upgrades at Nuclear Labs."

NOTES FOR CHAPTER 4

1. Christopher Alexander's book, produced with Ishikawa and Silverstein, is titled *A Pattern Language: Towns, Buildings, Construction*. The standard collection of design patterns for object-oriented software is *Design Patterns: Elements of Reusable Object-Oriented Software* by Gamma, Helm, Johnson, and Vlissides.
2. The discussion of architectural patterns for authentication in this chapter originally appeared in the article "Authentication: Patterns of Trust" published by this author in *Information Security* magazine.
3. The privilege modes of the Ferranti Atlas are described in the papers "Manchester University Atlas Operating System" by Kilburn et al., and "The Central Control Unit of the 'Atlas' Computer" by Sumner et al. See the article "Historical Overview of Computer Architecture" by this author for a summary of the relevant features.
4. Processor privilege modes are described in typical books on computer architecture. For example, see Section 7.3 of *Computer Architecture: Concepts and Evolution* by Gerrit Blaau and Fred Brooks.
5. Attacks on BIOS passwords are described in various hacker sources and computer security books, notably the ones by Anonymous, including *Maximum Security* (see Chapter 17) and *Maximum Linux Security* (see Chapter 2).
6. See the "Report of Investigation: Improper Handling of Classified Information by John M. Deutsch," by Snider and Seikaly, paragraph 82, for the experts' concerns about an undetected physical breakin of Deutsch's household computers.
7. See the paper "Tamper Resistance—A Cautionary Note" by Ross Anderson and Markus Kuhn for examples of low-cost attacks against smart cards. Similar techniques appear to work against USB tokens, as described in the paper "Attacks on and Countermeasures for USB Hardware Token Devices" by Kingpin.

8. See the paper "Differential Power Analysis" by Kocher, Jaffe, and Jun. Anderson's *Security Engineering* describes techniques used against smart cards and other cryptographic processors.
9. The FBI used a keystroke monitor to capture PGP keys used by Nicodemo "Little Nicky" Scarfo, an alleged mob boss. See "Scarfo Case Could Test Cyber-Spying Tactic," by George Anastasia.
10. For a summary of the evolution of authentication services in Novell Netware, see Chapter 17 of the book *Network Security: PRIVATE Communication in a PUBLIC World*, by Charlie Kaufman, Radia Perlman, and Mike Speciner. Helen Custer tells the story of Microsoft networking in Chapter 9 of *Inside Windows NT* (first edition only—the second edition is by a different author and doesn't cover networking).
11. For a really good discussion on the notion of protocols, see Chapter 18 of Radia Perlman's book *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols*.

NOTES FOR CHAPTER 5

1. The notion of cycles in computer history was introduced in the paper "On the Design of Display Processors" by Myer and Sutherland in 1968 and is illustrated in this author's paper "A Historical Overview of Computer Architecture."
2. Unix system design criteria are discussed in "The Unix Timesharing System: A Retrospective" by Dennis Ritchie. Windows NT design criteria are discussed in Chapter 1 of *Inside Windows NT*, First Edition, by Helen Custer.
3. Macintosh security features are summarized in the following Apple documents: "Technical Note TN1176: Mac OS 9," "Mac OS 9.1 Specification Sheet," and "Mac OS X Specification Sheet."
4. Bruce Schneier summarizes the strengths and weaknesses of both PKZIP and PGP in *Applied Cryptography*. See *PGP: Pretty Good Privacy* by Simson Garfinkel for more details on PGP. For an attack on PKZIP, see Biham and Kocher's paper "A Known Plaintext Attack on PKZIP Encryption."
5. See *A Guide to Understanding Data Remanence in Automated Information Systems* from the NCSC.
6. The $10,000 bounty may have been an urban legend. A different laptop theft bounty was described in Appendix J of the report *Cryptography's Role In Securing the Information Society (CRISIS)*, a noteworthy report on cryptographic policy by the National Research Council.
7. NIST has published the standard for DES in FIPS PUB 46-3, "Data Encryption Standard," the latest version of which calls out the use of Triple DES. See Schneier's *Applied Cryptography* for a practical description of the other algorithms.
8. William P. Crowell's testimony to Congress took place in a closed session, but a redacted transcript was released and posted on the Cryptome Web site.
9. Problems with cellular phone encryption were described in the papers "Cryptanalysis of the Cellular Message Encryption Algorithm, by Wagner, Schneier, and Kelsey, and "Real Time Cryptanalysis of A5/1 on a PC," by

Biryukov, Shamir, and Wagner. DeCSS, the software for decrypting DVDs, has been snared in legal battles with the motion picture industry, and also yielded a good deal of press coverage. DeCSS has been well covered by *2600* magazine, one of the defendants, particularly in the fall 2000 issue. That issue included the article "DeCSS in Words," attributed to an author named "CSS," that described how DVD encryption worked.

10. The FIPS for AES has not been published as of this writing, although a draft FIPS entitled "Advanced Encryption Standard" has been distributed by NIST for public comment. The paper "Report on the Development of the Advanced Encryption Standard (AES)" by Nechvatal et al. provides a good explanation of how AES was selected from among the five finalist algorithms and describes the analyses performed on those algorithms. See the article "Deciphering the Advanced Encryption Standard" by this author, for an overview of the algorithm, its selection, and its promise.
11. Susan Landau published a readable summary of DES in her article "Standing the Test of Time: The Data Encryption Standard." See Schneier's *Applied Cryptography* for the other algorithms.
12. Complementation is a well-known property of DES. It was described in Chapter 6 of Alan Konheim's textbook *Cryptography: A Primer* in 1981. In Chapter 3 of *Cryptography Theory and Practice*, Douglas Stinson presented it as an exercise to the reader, provable from the high-level description of the DES algorithm.
13. Whitfield Diffie's proposal was published in the paper "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," coauthored with Martin Hellman. The history of DES cracking is well covered in the Electronic Frontier Foundation's book *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design*.
14. Gordon E. Moore first published his observations in the magazine *Electronics* in 1965. Noyce amplified on these observations in the 1977 article "Microelectronics" in *Scientific American*. Also see Chapter 2 of *Computer Engineering: A DEC View of Hardware Systems Design*, by Bell, Mudge, and MacNamara.
15. Michael J. Wiener's report was entitled "Efficient DES Key Search." See the RSA Security Web site for summaries of results of various DES cracking challenges. The report on key lengths is entitled "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security" by Matt Blaze, Whitfield Diffie, Ron Rivest, et al. The RSA site also maintains copies of their Cryptobytes newsletter. The RSA Security article "DES-II Challenges Solved," appearing in the summer 1998 issue, describes the challenge results.
16. The *coup de grace* for DES as a strong encryption algorithm was delivered in 1998 with the publication of *Cracking DES* by the Electronic Frontier Foundation.
17. Seth Lloyd presented this approach for estimating the upper limit of computation speed in his paper "Ultimate Physical Limits to Computation."
18. NIST published the key escrow standard as FIPS 185, titled the "Escrowed Encryption Standard." The story of the Clipper chip was well covered in the press, and Steve Levy tells the story in his entertaining book *Crypto: How*

the Code Rebels Beat the Government—Saving Privacy in the Digital Age. See *Internet Cryptography* by this author for a high-level description of how FIPS 185 escrowed encryption was supposed to work.

19. For a survey of key escrow techniques, see "A Taxonomy of Key Recovery Encryption Systems" by Denning and Branstad.

NOTES FOR CHAPTER 6

1. See the *DOD Password Management Guideline*, produced by the NCSC.
2. See Chapter 2 of Schneiderman's *Designing the User Interface*. For a point of view more focused on usability and security, see the papers "Usability of Security: A Case Study," and "Why Johnny Can't Encrypt," by Alma Whitten and J. D. Tygar.
3. See Chapter 10 of *Designing the User Interface: Strategies for Effective Human–Computer Interaction* by Ben Shneiderman, and George Miller's article "The Magical Number Seven–Plus or Minus Two." An interesting review of memorization problems for textual passwords is provided by "The Design and Analysis of Graphical Passwords" by Jermyn, Mayer, et al.
4. In Chapter 3 of *The Design of Everyday Things*, Donald Norman talks about the problem of memory and the impracticality of techniques to improve memory.
5. Forcing functions are discussed in Chapter 5 of Norman's *Design of Everyday Things*.
6. Edward Tenner was inspired to write *Why Things Bite Back: Technology and the Revenge of Unintended Consequences* after noticing how much more paper gets used in a modern "paperless" office. Tenner summarized his taxonomy of revenge effects in Chapter 1.
7. These memorability and training experiments were reported by Yan, Blackwell, Anderson, and Grant, in their paper "Memorability and Security of Passwords—Some Empirical Results."
8. Houdini described "mind reading" techniques based on gathering personal information in Chapter 20 of his book, *A Magician Among the Spirits*. News articles about e-commerce legislation at the time reported President Clinton's password, including the article "Agencies Expect E-Sign Law to Spur E-Gov," by Christopher J. Dorobek.
9. Klein discussed this in his paper "A Survey of, and Improvements to, Password Security."
10. See "Palm OS Password Lockout Bypass" by Kingpin.
11. An example program for Palm-based systems is "Read This!" from PixIL. First reports of subverted software for Palm devices surfaced in the fall of 2000. See "Palm Virus Hits, But Don't Worry" by Michelle Delio for a published report from *Wired News*.
12. Password Safe and an introductory description stored in its help file are available from the Counterpane Web site.
13. See the Apple documents on Mac OS 9, including "Technical Note TN1176: Mac OS 9" and "Mac OS 9.1 Specification Sheet."

14. See "56 Bits?????" in the Apple Mailing List Archives for a discussion of the initial response to Mac OS 9 encryption features.
15. Al Sicherman, a newspaper columnist at the *Minneapolis Star Tribune*, has written a number of columns about his troubles with computer passwords. His column "By Any Other Name, He Probably Could Log On Somewhere" describes the classic technique of taking pairs of words from a song or poem and concatenating them to form the password.
16. Apple Computer recommended this strategy for choosing strong but memorable passwords in "Mac OS 9: File Security—Choosing a Good Password."
17. Leo Marks' *Between Silk and Cyanide* describes poem codes and their problems.

NOTES FOR CHAPTER 7

1. For further discussion of the promise of biometrics, see "Biometrics: The Future of Identification," by Pankanti, Bolle, and Jain, published in *IEEE Computer*. Ann Davis surveys biometrics in the *Wired* article "The Body as Password," and *The Economist* examined the topic in the article "Biometrics: The Measure of Man."
2. The book *Fingerprints: The Origins of Crime Detection and the Murder Case That Launched Forensic Science* by Colin Beavan describes 19th-century efforts to address the identification problem in law enforcement. Chapter 15 of *Biometrics: Personal Identification in Networked Society*, edited by Jain, Bolle, and Pankanti, talks about the problems of large-scale biometric databases.
3. Chapter 12 of Denning's *Information Warfare and Security* notes the use of biometrics in Connecticut and in other places. The article "How Biometrics Have Tamed Welfare Double Dipping" by Paul Clolery summarizes statistics from several states on cost savings. The paper "Privacy and Biometrics: An Oxymoron or Time to Take a 2nd Look?" by Ann Cavoukian identifies existing and proposed biometric systems for controlling welfare fraud, and notes their privacy policies.
4. See "Biometrics: Identifying Law and Policy Concerns" by John Woodward for a thorough review of the issues. The Cavoukian paper "Privacy and Biometrics" briefly reviews privacy issues related to biometrics from the point of view of a privacy commissioner in Canada.
5. The book *Biometrics: Personal Identification in Networked Society*, edited by Jain, Bolle, and Pankanti, provides a comprehensive survey of biometric technologies.
6. Fingerprint recognition is a well-established technique. *Fingerprints* by Beavan describes their early use. See "Practical Systems for Personal Fingerprint Identification" by Lawrence O'Gorman, "Fingerprint Biometric Devices" by Ben Rothke, and Chapter 2 of Jain et al. for information on computer-based fingerprint applications.
7. See "An Iris Biometric System for Public and Personal Use" by Negin et al. Also see Chapter 5 of *Biometrics* by Jain et al.

8. See "Face Recognition for Smart Environments" by Pentland and Choudhury for technical summary of face recognition technology. Also, see Chapter 3 of *Biometrics* by Jain et al.
9. The voice authentication feature in Apple's Mac OS 9 is summarized in the "Mac OS 9.1 Specification Sheet." Also see "Keep Your Secrets Safe with Voice-Activated Software" by Michael Himowitz, and Chapter 8 of Jain et al.
10. The lab experiments are described in the article "Six Biometric Devices Point the Finger at Security" by Willis and Lee.
11. Chapter 3 of *Internet Cryptography* by this author describes "rewrite attacks" that modify the contents of encrypted messages without having to guess the key.
12. The paper "Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy?" by George Tomko suggests using "biometric encryption" to control its use by institutions. The paper "Privacy and Biometrics" by Ann Cavoukian explains how the province of Ontario passed legislation that requires "biometric encryption" in any biometric systems used by social service agencies. The paper also summarizes a plan by the City of Toronto to install a biometric uniqueness validation system to control welfare fraud.

NOTES FOR CHAPTER 8

1. See a telecommunications reference, like *Technical Aspects of Data Communications* by John McNamara, for technical details about local telephone service.
2. For further information, see "Wardialing Brief" by Kingpin of @Stake. Examples of commercial wardialer programs include ModemScan by VerTTex Software and PhoneSweep by Sandstorm Enterprises.
3. This author worked for a company that was a customer of that particular modem vendor, at least until we discovered the back door.
4. Peter Neumann reported Oregon's Caller ID proposal in Chapter 6 of his book *Computer Related Risks*.
5. Penetrations of Internet service providers and telephone systems are described in Section 5.1.1 of *Computer Related Risks* by Peter Neumann. John Draper first received media attention in a 1971 article in *Esquire* magazine, and Chapter 12 of *Hackers* by Steve Levy summarizes his exploits.
6. Kevin Mitnick's activities have been chronicled by Katie Hafner and John Markoff in *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, *The Fugitive Game* by Jonathan Littman, and *Takedown* by Tsutomu Shimomura with John Markoff.
7. The Phonemasters story was reported in the news article "Phone Hex" by John Simons, which was quoted in Richard Power's book *Tangled Web*.
8. See *The SAGE Air Defense System* by John F. Jacobs.
9. See BBN Report 1822, "Interface Message Processor," for a description of ARPANET addressing. Details of IMP security are based on the author's own experience working at BBN's ARPANET Network Control Center.
10. See Chapter 7 of *Interconnections* by Perlman for additional information about X.25 and ATM addressing.

11. See Chapter 2 of *Interconnections* by Perlman for more information about IEEE 802 addresses.
12. Internet addressing is briefly described in RFC 791 by Jon Postel. For further information, see Comer's *Internetworking with TCP/IP, Volume 1*, Stevens' *TCP/IP Illustrated, Volume 1*, or Perlman's *Interconnections*.
13. Perlman refers to the problem of address discovery as "autoconfiguration" and discusses it in Chapter 11 of *Interconnections*.
14. The TCP synchronization protocol is described in RFC 793 by Jon Postel. Descriptions also appear in the books by Comer, Stevens, and Perlman noted above.
15. Laurent Joncheray described a way to perform TCP splicing in his paper "Simple Active Attack Against TCP." Although papers like Joncheray's and others in the mid-1990s led to protocol stack improvements to resist such attacks, not all improvements have been effective. CERT Advisory CA-2001-09, "Statistical Weaknesses in TCP/IP Initial Sequence Numbers," summarizes these problems.
16. Mike Neumann described IP-Watcher in the paper "Monitoring and Controlling Suspicious Activity in Real-Time with IP-Watcher."
17. The SYN flood attack is described by CERT Advisory CA-1996-21.
18. The DDOS attacks were described in CERT Advisories CA-1999-17 and CA-2000-01.
19. Effects of the DDOS attacks in February 2000 were developed and reported by APB News, and reported in "CSI Special Report on DDOS: Part 1" by Richard Power.
20. RFC 2401, "Security Architecture for the Internet Protocol," by Kent and Atkinson, provides an overview of the IPSEC protocol, its security objectives, and how it works. RFC 2402, "IP Authentication Header," by Kent and Atkinson, describes how IPSEC implements authentication.
21. MD5 is described in RFC 1321 by Ron Rivest, and SHA is described in FIPS PUB 180-1, by NIST.
22. The initial version of IPSEC is described in the now obsolete RFC 1826 by Atkinson. The HMAC construction is described in "Keying Hash Functions for Message Authentication" by Bellare, Canetti, and Krawczyk, and in RFC 2104, "HMAC: Keyed-Hashing for Message Authentication," by Krawczyk et al. MAC alternatives to use with AES are described under "Modes of Operation" on NIST's AES web site.
23. The story of the attack is told in the book *Takedown* by Tsutomu Shimomura. If one struggles past the book's lurid braggadocio, one finds a well-documented example of a computer-based manhunt, comparable to *Cuckoo's Egg* by Cliff Stoll.
24. IP spoofing is described in the paper "Attack Class: Address Spoofing" by Todd Heberlein and Matt Bishop. CERT Advisory CA-1995-01 also describes IP spoofing.
25. Robert T. Morris described the problem in his report "A Weakness in the 4.2BSD Unix TCP/IP Software," and Steve Bellovin included it in his paper "Security Problems in the TCP/IP Protocol Suite."

26. See *Firewalls and Internet Security* by Bill Cheswick and Steve Bellovin for more information about RPC, NFS, and NIS vulnerabilities.
27. The weakness in the public key system was described in the paper "Computation of Discrete Logarithms in Prime Fields" by LaMacchia and Odlyzko.
28. See *Global Positioning System: Theory and Practice* by B. Hofmann-Wellenhof, H. Lichtenegger, and J. Collins for technical background on GPS.
29. GPS-based location authentication is described in the paper "Location-Based Authentication: Grounding Cyberspace for Better Security" by Dorothy Denning and Peter MacDoran. Also see the CyberLocator Web site.
30. In Chapter 7 of *Information Warfare and Security*, Dorothy Denning briefly summarizes reports of GPS jamming products and technology. While there are no reports of jammers that forge GPS signals, some observers fear that this wouldn't pose a major technological challenge.

NOTES FOR CHAPTER 9

1. The cost estimate comes from a summary of magnetic card technology entitled "Why Use Magnetic Stripe Cards?" by Larry Nickel.
2. The story of Tania Ventura, a 26-year-old cashier at Bloomingdale's, was briefly noted in Richard Power's *Tangled Web*.
3. Stories of ATM fraud abound. See "Why Cryptosystems Fail," by Ross J. Anderson. ATM fraud problems are also summarized in Section 5.6 of *Computer Related Risks* by Peter Neumann.
4. The paper "Tamper Resistance—A Cautionary Note" by Anderson and Kuhn describes low-cost experiments in penetrating smart cards. Also see "Breaking Up Is Hard to Do: Modeling Security Threats for Smart Cards" by Schneier and Shostack.
5. See "Attacks on and Countermeasures for USB Hardware Token Devices" by Kingpin.
6. This story was heavily covered by wire services and major newspapers, including the *Minneapolis Star Tribune* (19 August 1995), the *St. Petersburg* (Russia) *Press* (issue 141, 9 January 1995) and the *San Francisco Chronicle* (19 August 1995). Richard Power assembled a very good review of the case in Chapter 7 of *Tangled Web*.
7. Technical features of SafeWord tokens are described in the *SafeWord DES Gold Supervisor Guide*, by Secure Computing, posted on the SafeWord Web site. Also see "When Passwords Are Not Enough," by Bob Bosen. Note that some SafeWord technical material resides on its own Web site instead of the Secure Computing corporate web site. The SafeWord resynchronization procedures are described on the SafeWord product pages on the Secure Computing Web site.
8. ActivCard technical features are described in a white paper titled "ActivCard Synchronous Authentication" by PC Dynamics, that is posted on the PC Dynamics Web site.
9. See the paper "Initial Cryptanalysis of the RSA SecurID Algorithm" by Mudge and Kingpin. Although experts have occasionally identified weaknesses in parts of the overall SecurID system (which are discussed else-

where in this book), there is no evidence that SecurID has been "cracked" in the cryptographic sense. Despite the rumors that occasionally sweep the computer security community, no technical description of an efficient cracking procedure has appeared as of this writing, nor have there been reports of victims of cracked SecurID authentication.

10. The technical features of the SecurID system are summarized in a white paper by RSA Security called "Strong Enterprise User Authentication: RSA ACE/Server" that is posted on the RSA Security Web site.
11. A widely discussed set of attacks appeared in the paper "Weaknesses in SecurID" by PieterZ. The paper's attacks require more sophistication, timing, and luck than other attacks, like TCP splicing. See the rebuttal "SecurID White Paper—A Comment" by Vin McLellan.
12. These attacks are described in CERT Advisory CA-1995-01, and started the events described in the book *Takedown* by Tsutomu Shimomura.
13. See "The Design and Implementation of Tripwire: A File System Integrity Checker" by Kim and Spafford, or Chapter 13 of *Internet Besieged*, edited by Denning and Denning.
14. PIN implementation for ATMs is described in various standards developed by the American Bankers Association. For example, see the "PIN Security Compliance Guideline" developed by the X9 Financial Services Committee.
15. See "Probability Theory for Pickpockets—ec-PIN Guessing" by Marcus Kuhn for an example of constrained PIN guessing on EuroCheque cash cards.
16. The duress PIN is described in the "SafeWord DES Gold Supervisor Guide," by Secure Computing.
17. See the report "SafeWord e.iD Palm Authenticator PIN Extraction" by Kingpin.

NOTES FOR CHAPTER 10

1. Bob Bosen and his brother Bill recounted the story of challenge response and 80 Space Raiders in private communications with this author. Enigma Logic is now a part of Secure Computing Corporation.
2. See "Financial Institution Message Authentication (Wholesale)" (X9.9), by the X9 Financial Services Committee, and "Computer Data Authentication" (FIPS 113), of the Federal Information Processing Standards.
3. See "The S/Key One Time Password System" by Neil Haller. The original concept was published in "Password Authentication with Insecure Communication" by Leslie Lamport.
4. See Haller's paper for a discussion of S/Key usage experience, and also see "One Time Passwords in Everything (OPIE): Experiences with Building and Using Stronger Authentication" by McDonald, Atkinson, and Metz.
5. See "Technical Guideline: Managing Risk and Mitigation Planning: Withdrawal of ANSI X9.9" by the X9 Committee.
6. For some background on the cryptography community's attitudes on proprietary technology, see Bruce Schneier's article "Why Cryptography Is Harder Than It Looks" and C. Matthew Curtin's "Snake Oil FAQ."

7. The early history of Microsoft networking is outlined in Chapter 9 of *Inside Windows NT*, first edition, by Helen Custer.
8. Several books have been published describing Samba, and there is also a Samba Web site containing source code and documentation. The pwdump utility is described in its documentation note "Windows NT Password Dump Utility" by Jeremy Allison, and the software is usually made available by Samba sites.
9. The LANMAN hash format is described in several places, including the Samba documentation and in the article "Windows NT Password Security" by Eugene Schultz.
10. The attack on the LANMAN hash is described in "FAQ: NT Cryptographic Password Attacks and Defenses" by Alan Ramsbottom.
11. The TENEX password-cracking story was recounted many times while this author worked at BBN, the creators of the TENEX operating system. Anderson called this a *timing attack* in Section 3.4.1.4. of *Security Engineering*.
12. The Windows challenge response protocol is described in Microsoft Knowledge Base article Q102716: "User Authentication with Windows NT." A description also appears in the "Cryptography" chapter of *Windows NT Security Guide* by Stephen Sutton, as well as in many of the Windows references noted above.
13. The NT hash procedure is described in Ramsbottom's FAQ and in the Schultz article.
14. Ramsbottom's FAQ also describes how to attack the NT hash using the LANMAN hash.
15. Microsoft describes the System Key in the Knowledge Base article "Windows NT System Key Permits Strong Encryption of the SAM."
16. "Windows NT Security Guidelines: A Study for NSA Research," by Steve Sutton, provides recommendations on using the System Key. Russ Cooper has also published recommendations on protecting the SAM database in his report "SAM Attacks v1.1."

NOTES FOR CHAPTER 11

Regarding the chapter's opening quotation: This important folk theorem of computer science is noted briefly in the paper "Authentication in Distributed Systems: Theory and Practice" by Lampson, Abadi, Burrows, and Wobber. A footnote explains that Roger Needham attributes the statement to David Wheeler of Cambridge University.

1. This observation came from satire attributed to Lauren Weinstein and exchanged among ARPANET users around 1980. The satire consisted of an alleged typescript of a lost investigative report from the television show *60 Minutes*, entitled "ARPANET Terror." TIP security concerns were also noted by Bob Metcalfe in RFC 602: "The Stockings Were Hung by the Chimney With Care," published in 1973.
2. Craig Finseth has briefly documented the history of TACACS in RFC 1492, titled "An Access Control Protocol, Sometimes Called TACACS."

3. Dave Carrel and Lol Grant of Cisco wrote up "The TACACS+ Protocol." It isn't clear that this document exists outside of Cisco except as an expired Internet Draft.
4. The RADIUS protocol is published in RFC 2865 by Rigney et al.
5. NT pass-through authentication is described in Microsoft's Knowledge Base article Q102716: "User Authentication with Windows NT." Also see the *Windows NT Server 4 Security Handbook* by Hadfield et al., and the *Windows NT Security Guide* by Stephen Sutton.
6. Chapter 3 of *Internet Cryptography* by this author provides a further discussion of rewrite attacks.
7. Reference books on cryptography all discuss block modes; see Section 3.4 of Stinson's *Cryptography* or Chapter 9 of Schneier's *Applied Cryptography*. NIST has officially specified DES modes in FIPS PUB 81. As of this writing, AES modes are still under discussion, as noted on the AES Web site.
8. Microsoft Knowledge Base article Q183859, "Integrity Checking on Secure Channels with Domain Controllers" describes the problem and solution. Windows NT Service Pack 4 adds integrity checking to the channels.
9. Anti-replay mechanisms were incorporated in IPSec in the 1998 revision, as described in RFC 2402 "IP Authentication Header" by Kent and Atkinson.
10. Export control regulations for all products, including those containing cryptography, are posted on the Bureau of Export Administration Web site. The National Research Council report *Cryptography's Role In Securing the Information Society* (the CRISIS report) provides a thorough description of export controls, and the rationale behind them, before their phased relaxation began in the late 1990s.
11. Matt Blaze's report was entitled "Protocol Failure in the Escrowed Encryption Standard." See "Key-Experiments—How PGP Deals With Manipulated Keys" by Ralf Senderek for an example of how adding extra "recovery" keys can open a weakness in an encryption package that previously had a reputation for reasonable security.
12. Sutton's *Guide*, noted above, describes how domain controllers establish encrypted links with other computers in the domain.
13. Schneier and Mudge published the report "Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP)" describing these vulnerabilities.
14. The NSA Web site contains detailed coverage of the Venona project, including numerous decryptions that were significant to the history of the Cold War.
15. Schneier, Mudge, and Wagner published a follow-on to the PPTP paper when Microsoft released a revised PPTP to address their concerns: "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)."
16. Russ Cooper describes security problems with the SAM in his report "SAM Attacks v1.1.
17. Shamir and van Somerin discussed these techniques in the paper "Playing Hide and Seek with Stored Keys."
18. Shamir and van Somerin note this technique. Also see *Disappearing Cryptography* by Peter Wayner.

NOTES FROM CHAPTER 12

1. The ANSI X9.17 standard, titled "Financial Institution Key Management (Wholesale)," is authored by the X9 Financial Services Committee. Fr. M. Blake Greenlee describes the practical problems that drove the banking industry to X9.17 in his entertaining paper "Requirements for Key Management Protocols in the Wholesale Financial Services Industry." Dennis Branstad's pioneering approach to KDCs is described in his paper "Encryption Protection in Computer Data Communications."
2. Needham and Schroeder introduced these protocols in their paper entitled "Using Encryption for Authentication in Large Networks of Computers."
3. Denning and Sacco's concept appeared in their paper "Timestamps in Key Distribution Protocols."
4. The classic introduction to Kerberos is the paper "Kerberos: An Authentication Service for Open Network Systems" by Jennifer Steiner, Clifford Neuman, and Jeffrey Schiller. Also see "Kerberos: An Authentication Service for Computer Networks" by Clifford Neuman and Theodore Ts'o. There is also the book *Kerberos: A Network Authentication System* by Brian Tung. Bill Bryant produced a clever description of the rationale behind Kerberos in "Designing an Authentication System: a Dialogue in Four Scenes," in which two developers named "Athena" and "Euripides" discuss the design requirements for a distributed authentication system.
5. As of this writing, Kerberos V5 is a proposed Internet standard, published as RFC 1510 by John Kohl and Clifford Neuman. Theodore Ts'o et al. produced a revised version.
6. Steve Bellovin and Michael Merritt outlined the clock problem and a number of other Kerberos security problems, mostly for Version 4, in their paper "Limitations of the Kerberos Authentication System." For further discussion of timestamps in security protocols, see "A Note on the Use of Timestamps as Nonces" by Neuman and Stubblebine.
7. Microsoft has written a white paper describing their Kerberos implementation entitled "Windows 2000 Kerberos Authentication." Additional information appears in another Microsoft Web article entitled "Secure Networking Using Windows 2000 Distributed Security Services." Jalal Feghhi and Jalil Feghhi have written a book on Windows 2000 Kerberos and related security services entitled *Secure Networking with Windows 2000 and Trust Services*.

NOTES FROM CHAPTER 13

1. Two of the pioneers of public key mathematics have published well-known articles describing its foundations: Martin Hellman wrote "The Mathematics of Public-Key Cryptography," and Whitfield Diffie wrote "The First Ten Years of Public Key Cryptography."
2. Rivest, Shamir, and Adelman first described the RSA algorithm themselves in their 1978 paper "A Method for Obtaining Digital Signatures and Public Key Cryptosystems." However, a brief description of their algorithm was also published by Martin Gardner several months earlier in the dramatically

mistitled *Scientific American* article "A New Kind of Cipher That Will Take Millions of Years to Break."

3. The RSA example was adapted from Diffie's paper "The First Ten Years of Public Key Cryptography."
4. Don Knuth describes some classic factorization algorithms in Chapter 4 of *Seminumerical Algorithms*.
5. Rivest's prediction appeared in the *Scientific American* article by Martin Gardner mentioned above in Note 2.
6. Atkins et al. described how they cracked the 129-digit RSA key in their article "The Magic Words Are Squeamish Ossifrage." The article's odd title is actually the text of the message that had been encrypted with the 129-digit key. Mark Uehling also reported on the crack in the *Popular Science* article "Cracking the Uncrackable Code."
7. RSA Data Security published the press release "RSA Crypto Challenge Sets New Security Benchmark" on August 26, 1999, to announce the cracking of RSA-155. In the summer of 2000, Eric Murray published his "SSL Server Security Survey," which examined the strength of cryptographic software used by secure Web sites.
8. Cryptographic texts often contain the equation to estimate the run time of factoring algorithms: see Chapter 4 of Stinson's *Cryptography*. A historical survey of factoring and the results of RSA factoring challenges appears in "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths" by Robert Silverman.
9. Rabin published his scheme in the report "Digital Signatures and Public-Key Functions as Intractable as Factorization." Typical cryptographic texts also cover Rabin: see Section 4.7 of Stinson's *Cryptography* or Section 19.5 of Schneier's *Applied Cryptography*.
10. Dorothy Denning described several of these attacks along with the solution in her paper "Digital Signatures with RSA and Other Public-Key Cryptosystems."
11. The practical deployment of public key technology is described in Steve Levy's book *Crypto*. For a contemporary look at the controversy surrounding the Digital Signature Standard, see the July 1992 issue of *Communications of the ACM*.
12. The "Digital Signature Standard" was published as FIPS PUB 186-2 by NIST.
13. The index calculus method is described in Chapter 5 of Stinson's *Cryptography*.
14. The Tessera Authentication Protocol was developed under Contract MDA904-92-G-0284 for the Maryland Procurement Office, and described in the contract's final report, CDRL B001, "Technical Report for the Tessera Authentication Protocol Specification Program," by Earl Boebert and Chuck Nove.
15. The standard for public key authentication was published as FIPS PUB 196 by NIST in1997.
16. Netscape's history is reasonably covered in Steve Levy's *Crypto*.

17. The protocol specification for SSL 3.0 was written up by Freier, Karlton, and Kocher in 1996. See the book *SSL and TLS: Designing and Building Secure Systems* by Eric Rescorla for an in-depth look at the protocol.
18. David Wagner and Bruce Schneier examined SSL vulnerabilities in their paper "Analysis of the SSL 3.0 Protocol."

NOTES FROM CHAPTER 14

1. Leon Kornfelder, a student of RSA co-inventor Len Adelman, proposed digital certificates in his bachelor's thesis "Towards a Practical Public-Key Cryptosystem."
2. Microsoft published a security bulletin, "Erroneous VeriSign-Issued Digital Certificate Poses Spoofing Hazard," that describes the problem.
3. The relationship between Netscape, RSA Data Security, and Verisign is briefly described in *Crypto* by Steve Levy.
4. This is described in the Microsoft security bulletin noted above.
5. Certificates are defined by ITU-T X.509. Internet use of X.509 certificates is in RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" by Russ Housley, Warwick Ford, Tim Polk, and Dave Solo.
6. The example certificate comes from RFC 1422, "Privacy Enhancement for Internet Electronic Mail: Part II—Certificate-Based Key Management" by Steve Kent.
7. The cost of STU III management was presented in Section 2.5.1 of the National Research Council's CRISIS report.
8. Certificate authorities like Verisign generally post their certification practices statements on their Web site.
9. The PEM certification hierarchy is also described in RFC 1422 by Kent, noted above.
10. DASS is described in the paper "SPX: Global Authentication Using Public Key Certificates" by Tardo and Alagappan. It is also described in Chapter 4 of *Authentication Systems for Secure Networks* by Rolf Oppliger.
11. PGP is thoroughly described in Simson Garfinkel's book *PGP: Pretty Good Privacy*.
12. CRLs for Internet usage are described in RFC 2459 by Housley, Ford, Polk, and Solo.
13. Microsoft's CRL patch is described in the Knowledge Base article "Update Available to Revoke Fraudulent Microsoft Certificates Issued by VeriSign."
14. One approach for on-line certificate checking has been published as a proposed Internet standard in RFC 2560: "X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol—OCSP" by Myers et al.
15. Rivest describes this strategy in "Can We Eliminate Certificate Revocation Lists?"
16. PKINIT is described in "Public Key Cryptography for Initial Authentication in Kerberos" by Tung, Neumann, Hur, et al.
17. The Windows 2000 implementation is described in the Microsoft Windows 2000 white paper "Smart Card Logon."

NOTES FROM CHAPTER 15

1. Schneier presents recommendations for generating random primes in Section 11.5 of *Applied Cryptography*.
2. Rabin describes the Miller-Rabin algorithm in his paper "Probabilistic Algorithm for Testing Primality." The algorithm also appears in cryptographic texts like Schneier (Section 11.5) and Stinson's *Cryptography* (Section 4.5).
3. Garfinkel describes PGP key generation in *PGP: Pretty Good Privacy*.
4. The Lotus Notes ID file is described in Section 17.6 of *Network Security* by Kaufman, Perlman, and Speciner.
5. Mike Miller wrote the "pgpcrack" program to perform trial-and-error cracking of PGP passphrases. As of this writing, its traditional home on the Web has disappeared, but it tends to show up in other places as well. Also see Peter Gutman's note "Where do your encryption keys want to go today?"
6. Keystroke monitors can capture PGP keys. See "Scarfo Case Could Test Cyber-Spying Tactic," by George Anastasia.
7. Datakey published press releases on these applications of their smart cards, specifically "Datakey multi-purpose smart cards deployed by the FDIC for secure online communications and building access," and "Datakey smart card used by President Clinton to sign e-signature law."
8. Performance of the Datakey 330 appears on Datakey's sales materials, particularly "Technical Specifications: Datakey's Cryptographic Smart Card and Smart Key."
9. The paper "Smartcard Based Authentication" by Ratha and Bolle describes a system that uses biometrics with smart cards in which the matching is off-loaded from the card.
10. DASS is described in the paper "SPX: Global Authentication Using Public Key Certificates" by Tardo and Alagappan. It is also described in Chapter 4 of *Authentication Systems for Secure Networks* by Rolf Oppliger.
11. The Novell protocol is described in Section 17.2 of *Network Security* by Kaufman, Perlman, and Speciner. Radia Perlman and Charlie Kaufman examine additional approaches in their paper "Secure Password-Based Protocol for Downloading a Public Key."
12. Secure Computing has published a white paper entitled "SafeWord Plus Virtual Smart Card Server Solution."
13. The classic paper on the topic is "Reducing Risks from Poorly Chosen Keys" by Lomas, Gong, Saltzer, and Needham.
14. Bellovin and Merritt introduced their protocols in the paper "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks."
15. The paper "Strong Password-Only Authenticated Key Exchange" by David Jablon provides a good overview of techniques. Recent work has been reported by Taekyoung Kwon in "Authentication and Key Agreement via Memorable Password." These authors and others have established IEEE study group "P1363a" for Password-Based Authenticated Key Exchange Methods, which has its own Web site, hosted by the IEEE.