# User Authentication and Related Topics: An Annotated Bibliography

Eugene H. Spafford Stephen A. Weeber

Purdue Technical Report CSD–TR–91–086

## Introduction

This bibliography is the result of our examination of the current state of user authentication, with an emphasis on password authentication.

We believe that this bibliography is representative of the most important works in the area in recent years. Many of these citations include notes indicating the content of the work; however, inclusion of the citation or of additional notes does not necessarily indicate we believe the work to be more significant than other items.

We would appreciate being told of any pertinent references missing from this collection.

## Acknowledgments

Our thanks to Matt Bishop for his suggestions of additions to this document.

## References

[1] Proposed federal information processing data encryption standard. *Federal Register (40FR12134)*, March 1975.

[2] Data Encryption Standard. Federal Information Processing Standards Publication 46, National Bureau of Standards, Washington, D.C., January 1977.

[3] Guidelines on evaluation of techniques for automated personal identification. Federal Information Processing Standards Publication 48, National Bureau of Standards, April 1977.

[4] Guidelines on user authentication techniques for computer network access control. Federal Information Processing Standards Publication 83, National Bureau of Standards, Washington, D.C., September 1980.

[5] Password usage standard. Federal Information Processing Standards Publication 112, National Bureau of Standards, May 1985.

[6] Niv Ahituv, Yeheskel Lapid, and Seev Nuemann. Verifying the authentication of an information system user. *Computers and Security*, 6(2):152–157, April 1987. The authors discuss the benefits and problems of different methods of user authentication. A quantitative measure of password strength and 'lasting' power is developed. Five password encryption techniques are discussed and compared using several criteria. Finally, ten authentication guidelines are presented.

[7] Ana Maria De Alvaré. How crackers crack passwords, or what passwords to avoid. Technical Report UCID–21515, Lawrence Livermore National Laboratory, September 1988. The author evaluates several password selection techniques that have been proposed in light of information she collected during interviews with password crackers. A list of recommended techniques for password selection is provided. Passwords and methods crackers have used to break into systems as well as security guidelines for system managers are also discussed.

[8] Ana Maria De Alvaré and E. Eugene Schultz, Jr. A framework for password selection. Technical Report UCRL-99382, Lawrence Livermore National Laboratory, 1988. This paper describes a study on the guessability of passwords. Both easy and difficult passwords were guessed at by subjects, some of which were given cues as to the makeup of the password. The results suggest that only easy passwords with known characteristics are readily guessable. The author concludes that users may select their own passwords securely if they follow guidelines that will make them difficult to guess.

[9] James P. Anderson. Information security in a multi–user computer environment. *Advances in Computers*, 12:2–36, 1972.

[10] L. E. Anderson. UNIX password security. In *USENIX Security Workshop*, page 7. The USENIX Association, August 1988.

[11] R. G. Anderson, D. C. Clark, and D. R. Wilson. See through security. *MIS Week*, April 7, 1986.

[12] Peter Arbouw. Security in multi-company networks. In *Proceedings of the Second European Conference on Computer Audit*, November 1987.

[13] K. P. Badenhorst and Jan H. P. Eloff. Framework of a methodology for the life cycle of computer security in an organization. *Computers and Security*, 8(5):433–442, August 1989.

[14] Ben F. Barton and Marthalee S. Barton. User-friendly password methods for computer mediated information systems. *Computers and Security*, 3:186–195, 1984. This article discusses the need for better password methods given the increase in unauthorized system access and the growing numbers of novice users with access to networked workstations. The authors favor a user-friendly model of password selection over the user-hostile trend that sacrifices memorability for security.
A cognitive model for password selection is proposed based on semantic memory, episodic memory, and information from the environment. Various transformation and mnemonic techniques are also discussed. Finally, the authors assert that materials which would aid users in making good password choices should be readily available on the system.

[15] Richard Baskerville. *Designing Information Systems Security.* John Wiley & Sons, 1988.

[16] Steven M. Bellovin. Security problems in the TCP/IP protocol suite. *Computer Communication Review*, 19(2):32–48, April 1989.

[17] Steven M. Bellovin and Michael Merritt. Limitations of the Kerberos authentication system. In *Proceedings of the 1991 Winter USENIX Conference*, 1991. The authors discuss limitations and weaknesses of the Kerberos authentication system, including vulnerability to password-guessing attacks. They propose a solution based on exponential key exchange.

[18] T. Berson, P. Capek, J. Schweitzer, and C. Weissman. Identification verification (authentication) working group. *ACM SIGSAC*, 6(1):2–9, 1988.

[19] Robert P. Bigelow. Those pesky passwords. *Computer Law Newsletter*, 2(6):3–4, July–August 1985.

[20] Matt Bishop. Privacy-enhanced electronic mail. To appear in the Journal of Internetworking. This paper describes the authentication mechanisms used by privacy-enhanced electronic mail as of June 1991.

[21] Matt Bishop. An application of a fast Data Encryption Standard implementation. *Computing Systems*, 1(3):221–254, 1988. The author describes several improvements to the implementation of the DES algorithm that reduce the required computing time by more than an order of magnitude.

[22] Matt Bishop. UNIX security in a supercomputing environment. In *Supercomputing '89 Proceedings*, pages 693–698, November 1989. This paper describes user authentication in a supercomputing center which uses UNIX systems.

[23] Matt Bishop. Collaboration using roles. *Software – Practice and Experience*, 20(5):485–495, May 1990. The author discusses how to share an account without using shared passwords. The scheme developed uses the notion of a 'group account' controlled by an access file, and bases permissions on user identity as proved by a password.

[24] Matt Bishop. An extendible password checker. In *UNIX Security Workshop II*, pages 15–16. The USENIX Association, August 1990. The author describes the implementation of a proactive password checker, designed to test for poor password choices as the user attempts to select a password. The language used to specify tests is discussed, along with several examples.

[25] Matt Bishop. Password checking techniques. In *Proceedings of the Second Workshop on Computer Security Incident Response*, pages IV–D–1:4, June 1990. The author discusses password cracking and countermeasures in a UNIX environment.

[26] Matt Bishop. Authenticating network news. In *Proceedings of the 1991 Winter USENIX Conference*, pages 281–287, January 1991. This paper describes enhancements to USENET news allowing the originator of articles to be authenticated and the integrity to be checked.

[27] Matt Bishop. Metrics for comparing authentication systems. In *Proceedings of the Third Workshop on Computer Incident Handling*, pages G–11–1:10, August 1991. The author discusses how to compare authentication schemes.

[28] Matt Bishop. Password management. In *COMPCON 1991 Proceedings*, pages 167–169, February 1991. The author discusses general issues involved in password management.

[29] Matt Bishop. A proactive password checker. In *Proceedings of the Seventh International Conference on Information Security*, pages 150–158, May 1991. The author discusses a technique for limiting the user's ability to pick a bad password. A UNIX implementation is described.

[30] J. Bologna. Computer insecurities: An analysis of recent surveys on computer related crime and computer security. *Data Processing and Communications Security*, 12(4), Fall 1988.

[31] Russell L. Brand. *Attack of the Tiger Teams: Inside America's Computer Security Crisis*. Tempus Books, August 1989.

[32] Russell L. Brand. Coping with the threat of computer security incidents: A primer from prevention through recovery. Available through anonymous ftp from cert.sei.cmu.edu in directory /pub/info/primer, June 1990. This guide emphasizes planning and prevention as strategies for improving computer security. Several issues relating to password security are covered, including automated checks for bad passwords, machine generated passwords, alternate authentication techniques, and password aging.

[33] Dennis K. Brandstad, (ed.). Computer security and the Data Encryption Standard. Special Publication 500-27, National Bureau of Standards, 1978.

[34] Edwin Brautman. Comparison of learning and retention of all-digit telephone numbers to prefixed and mnemonic coded numbers. *Perceptual and Motor Skills*, 36:267–270, 1973.

[35] Tony Bromfield. Personal authentication devices: Present & future. In *System Security '87, Proceedings of the Conference*, pages 145–157, Pinner, Middlesex, United Kingdom, 1987. Online Publications.

[36] R. Leonard Brown. Computer system access control using passwords. *Computer Security: A Global Challenge*, pages 129–142, 1984.

[37] Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. In *Proceedings of the Twelfth ACM Symposium on Operating Systems Principles*, December 1989. The authors claim that most security protocols found in literature contain redundancies or security flaws. They define a logic of authentication which adds a level of formalism to protocol design. This logic is then used to analyze the Kerberos, Andrew Secure RPC Handshake, Needham-Schroeder Public-Key, and CCITT X.509 protocols.

[38] David W. Bynon. System security, part 1. *DEC Professional*, October 1988.

[39] William Caelli, Dennis Longley, and Michael Shain. *Information Security for Managers*. Macmillan Publishers Ltd., 1989.

[40] William Caelli, (ed.). Computer security in the age of information. In *Proceedings of the Fifth IFIP International Conference on Computer Security*. IFIP/Sec, 1988.

[41] I. R. Cameron and P. C. Millar. Speaker recognition – fact or fiction? In *Proceedings of the IEE Colloquium on MMI in Computer Security*, 1986.

[42] Stephen F. Carlton, John W. Taylor, and John L. Wyszynski. Alternate authentication mechanisms. In *11th National Computer Security Conference Proceedings*, pages 333–338. National Bureau of Standards/National Computer Security Center, October 1988. This paper discusses three classes of authentication mechanisms: things you know, things you have, and things you are. Each mechanism is described, including examples of the mechanism in use; and the strengths and weaknesses of each are analyzed.

[43] John M. Carroll. *Computer Security*. Butterworth Publishers, Stoneham, MA, 2nd edition, 1987.

[44] John M. Carroll. Strategies for extending the useful lifetime of DES. *Computers and Security*, 6(4):300–313, August 1987.

[45] C. Chan. User authentication during the logon process. In *7th International Conference on Computer Communication*, pages 860–865, 1984.

[46] D. Chaum. Security without identification: Transaction systems to make Big Brother obsolete. *Communications of the ACM*, 28(10):1030–1044, October 1985.

[47] Michael Comer, (ed.). Password breaking. *Computer Fraud & Security Bulletin*, 4(2):7–8, December 1981. This article describes the tactics used by 'Computer Freaks' to break passwords.

[48] Michael Comer, (ed.). Underground advice. *Computer Fraud & Security Bulletin*, 4(2):8–11, December 1981. This article contains several pages of technical advice, written by a hacker, detailing how to break into computer systems.

[49] Michael Comer, (ed.). How passwords are cracked. *Computer Fraud & Security Bulletin*, 7(1):1–10, November 1984. This article summarizes many of the ways in which system security is broken. According to the author, three pieces of information are required to overcome security measures: dial-in port numbers, account identification, and passwords. Methods by which these items may be obtained are discussed.

[50] Michael Comer, (ed.). Password breaking. *Computer Fraud & Security Bulletin*, 6(3):1–5, January 1984. This article describes a program for finding passwords on Prime computers. The program repeatedly attempts to open a file with different passwords until it finds one that succeeds.

[51] Alex P. Conn, John H Parodi, and Michael Taylor. The place of biometrics in a user authentication taxonomy. In *13th National Computer Security Conference Proceedings*, pages 72–79. National Institute of Standards and Technology/National Computer Security Center, October 1990. Biometric authentication is discussed in light of other available authentication techniques. The authors describe the advantages and limitations of both passwords and 'see-through' authentication. They go on to cover in detail the use, security, advantages, and drawbacks of biometric authentication. The authors conclude that the chief disadvantage of biometrics is the fact that biometric characteristics are not secrets.

[52] William Connolly. Bypassing the passwords? *Computer Fraud & Security Bulletin*, 5(9):1–7, July 1983. This article describes several password systems, all of which were broken with a minimum of technical knowledge.

[53] James Arlin Cooper. *Computer & Communications Security*. McGraw-Hill, 1989. This book covers a wide variety of computer and communications security topics. Password authentication is considered as a cost-effective authentication technique. Several implementation factors that affect password security are discussed. A phonetic password generation scheme is also proposed.

[54] Brian J. B. Cope. Biometric systems of access control. *Electrotechnology*, 18(2):71–74, April–May 1990.

[55] Michele D. Crabb. Password security in a large distributed environment. In *UNIX Security Workshop II*, pages 17–29. The USENIX Association, August 1990. Techniques used to

manage a large number of passwords for privileged accounts in a distributed computing environment are discussed. The author details the development of the philosophy, policies, and methods used.

[56] H. D. Crane and J. S. Ostrem. Automatic signature verification using a three-axis force-sensitive pen. *IEEE Transactions on Systems, Man, and Cybernetics*, SMC-13(3):329–337, 1983.

[57] P. Cross. Computing: Beat the hackers. *Health Services Journal*, 100(5205):888–889, June 14, 1990.

[58] David A. Curry. Improving the security of your UNIX system. Technical Report ITSTD-721-FR-90-21, SRI International, Menlo Park, CA, April 1990. This report provides a detailed security checklist for UNIX systems in general, with an emphasis on SunOS 4.x. The author discusses the poor quality of many passwords currently in use, suggests several guidelines for password selection, and recommends the distribution of password policies for all users. Finally, the author suggests checking password security with a password-cracking program.

[59] Marc Dacier and Michel Rutsaert. Dealing with transitivity in security. In *Proceedings of the "Convention Unix 91" AFUU*, 1991.

[60] Datapro Research Group. Host access control software: Market overview. *Datapro Reports on Information Security*, pages IS52–001–101:104, July 1990.

[61] Datapro Research Group. Host access control software: Technology overview. *Datapro Reports on Information Security*, pages IS52–001–121:126, July 1990.

[62] D. W. Davies and W. L. Price. *Security for Computer Networks.* John Wiley & Sons, second edition, 1989.

[63] Don Davis and Ralph Swick. Workstation services and Kerberos authentication at Project Athena. MIT Project Athena, March 3, 1989.

[64] Khosrow Dehnad. A simple way of improving the login security. *Computers and Security*, 8(7):607–611, November 1989. This paper describes a method designed to hinder trial and error guessing of passwords. Using this method, a system will reject correct passwords with a certain probability based on the number of failed login attempts. This denies the penetrator absolute knowledge of the correctness of the password.

[65] Romine R. Deming. Dynamic signatures for personal identity verification. In *Proceedings of the 1986 International Carnahan Conference on Security Technology*, pages 103–106, August 1986.

[66] Dorothy Elizabeth Robling Denning. *Cryptography and Data Security.* Addison-Wesley, Reading, MA, January 1983.

[67] W. Diffie and M. E. Hellman. Privacy and authentication, an introduction to cryptography. *Proceedings of the IEEE*, 67(3):397–427, March 1978.

[68] M. El-Baghdadi. The pivotal role in computer security. *Security Management*, 33(7):63, July 1989.

[69] Norman L. Enger and Paul W. Howerton. *Computer Security*. Amacom, New York, 1980.

[70] David M. England. Zodiac: Personal identification by signature. *Computer Bulletin*, 4:33–34, June 1988.

[71] Arthur Evans, Jr., William Kantrowitz, and Edwin Weiss. A user authentication scheme not requiring secrecy in the computer. *Communications of the ACM*, 17(8):437–442, August 1974. The authors propose a password system that does not require the password file to be stored secretly. They describe a scheme using one-way functions to encrypt passwords.

[72] V. Fåk. Characteristics of good one-way encryption functions for passwords – some rules for creators and evaluators. In *Computer Security: A Global Challenge*, pages 189–191, Amsterdam, September 1984. IFIP, Elsevier Science Publishing.

[73] Daniel Farmer and Eugene H. Spafford. The COPS security checker system. In *Proceedings of the Summer USENIX Conference*. The USENIX Association, June 1990.

[74] Rik Farrow. Security for superusers, or how to break the UNIX system. *UNIX/World*, 3(5):65–70, May 1986. The author describes several methods that may be used to break UNIX security and the steps that can be taken to close the holes.

[75] Rik Farrow. *UNIX System Security*. Addison Wesley, Reading, MA, 1991. The book contains several sections relating to password security, including password choice, checking the password file, and shadow passwords.

[76] David C. Feldmeier and Philip R. Karn. UNIX password security – ten years later. In *CRYPTO Proceedings*, Summer 1989.

[77] R. C. Ferreira. The smart card: A high security tool in EDP. *Philips Telecommunications Data Systems Review*, 47(3):1–19, September 1989.

[78] Ken J. Fifield. Smartcards outsmart computer crime. *Computers and Security*, 8(3):247–255, May 1989. The author advocates the use of smartcards to overcome the weaknesses of other authentication techniques such as passwords. He claims smartcards provide reliable user authentication and protection from line taps and modified system software.

[79] Philip E. Fites, Martin P. J. Kratz, and Alan F. Brebner. *Control and Security of Computer Information Systems*. Computer Science Press, Rockville, MD, 1989. Comprehensive guide to system security, including recommendations for password authentication.

[80] J. Gait. Easy entry: The password encryption problem. *Operating Systems Review*, 12(3):54–60, July 1978. The author discusses the disadvantages of unencrypted password files and the advantages of password encryption. The encryption techniques used by MULTICS and UNIX are discussed, along with improved encryption algorithms such as DES and EWK. Finally, the use of DES in hardware to provide secure communication is described.

[81] John Gallant. Raid nets computers allegedly used to access NASA files. *Computerworld*, July 1984.

[82] E. Gardner, L. Samuels, and B. Render. Computer security. *The Journal of Information Systems Management*, 6(4):42, Fall 1989.

[83] Simson Garfinkel and Eugene H. Spafford. *Practical UNIX Security*. O'Reilly and Associates, Inc., May 1991. This book, among many other things, describes the specifics of UNIX passwords. Topics such as the structure of the password file, password encryption, salts, shadow password files, and password aging are discussed. Related subjects, such as making good password choices and administrative ideas for password security, are also covered.

[84] Morrie Gasser. A random word generator for pronounceable passwords. Technical Report AD-A017 676, The MITRE Co., Bedford, MA, November 1975.

[85] Morrie Gasser. *Building a Secure Computer System*. Van Nostrand Reinhold, New York, 1988.

[86] F. Grampp and R. Morris. UNIX operating system security. *AT&T Bell Labs Technical Journal*, 63(8):1649–1672, October 1984. This article details several areas of concern in UNIX security, passwords being one. The authors note the ease with which passwords were guessed at several locations. They also suggest several ideas that would make the password mechanism more secure.

[87] M. Greenia. *Computer Security Information Sourcebook*. Lexikon Services, Sacramento, CA, 1989.

[88] Katherine M. Hafner. Is your computer secure? *Business Week*, August 1988.

[89] James A. Haskett. Pass-algorithms: A user validation scheme based on knowledge of secret algorithms. *Communications of the ACM*, 27(8):777–781, August 1984. The author proposes the use of pass-algorithms in addition to passwords for authentication. The paper suggests the complexity of the algorithms should vary based on factors such as login location, username, and time of day. Information on modifying the VAX/VMS operating system to use pass-algorithms is provided.

[90] F. Hayes. Is your system safe? *UNIX World*, 7(6):44, June 1990. In light of the Internet worm, this article discusses the current state of UNIX system security. The author concludes that easily guessed passwords are currently the largest problem.

[91] Colin Hebden. Secure authentication in a local area network. In *System Security: The Technical Challenge*, pages 119–128, London, October 1985. Online Publications. This paper describes the security weaknesses of local area networks. Counter-measures are discussed. In particular, the requirements for a secure authentication server are presented.

[92] Martin Hellman. DES will be totally insecure within ten years. *IEEE Spectrum*, page 32, July 1979.

[93] N. M. Herbst and C. N. Liu. Automatic signature verification based on accelerometry. *IBM Journal of Research and Development*, 16(2):245–253, May 1977.

[94] Israel Herschberg. The hackers' comfort. *Computers and Security*, 6(2):133–138, April 1987. The author discusses the lack of security present in computing environments. According to the author, users overwhelmingly choose poor, unimaginative passwords when allowed to select their own. Users will also avoid requirements about password choice whenever possible. The lack of security of computer generated random passwords is discussed. The author recommends that passwords be screened through the use of dictionaries of poor passwords. Finally, the author criticizes the computing industry for equating user friendliness with the removal of obstacles to system use, and for the habit of adding security measures as an afterthought.

[95] Harold Joseph Highland. QETUOADGJLXVN or the selection and use of passwords for security. *Computer Compacts*, 1(1):280–281, February 1983.

[96] Harold Joseph Highland. *Protecting Your Microcomputer System.* John Wiley & Sons, Inc., 1984.

[97] Harold Joseph Highland. Random bits & bytes. *Computers and Security*, 6(2):99–110, April 1987. A user authentication card that generates a sequence of passcodes is reviewed. The passcodes change every 60 seconds, and the sequence is determined by a seed value. The user's passcode must match the passcode computed by hardware present in the host computer for access to be granted.

[98] Harold Joseph Highland. How to prevent the use of weak passwords. *The EDP Audit, Control, and Security Newsletter*, 18(9), March 1991. A password screening tool called Password Coach is reviewed. The program, developed by Charles Cresson Wood, uses multiple dictionaries and composition rules to reject weak password choices.

[99] L. J. Hoffman. *Modern Methods for Computer Security and Privacy.* Prentice-Hall, Englewood Cliffs, NJ, 1977. The author's discussion of user authentication includes the topics of password choice, length, expected safe time, one-time passwords, and question-answer authentication.

[100] J. Paul Holbrook, (ed.), Joyce K. Reynolds, (ed.), Dave Curry, Sean Kirkpatrick, Tom Longstaff, Greg Hollingsworth, Jeffrey Carpenter, Barbara Fraser, Fred Ostapik, Allen Sturtevant, Dan Long, Jim Duncan, and Frank Byrum. Security policy handbook. This document is being developed by the Security Policy Handbook Working Group of the Internet Engineering Task Force. It includes information on threat identification, user responsibilities for password security, authentication systems, and password management, 1991.

[101] Jan Hruska and Keith Jackson. *Computer Security Solutions.* CRC Press, Boca Raton, FL, 1990. This book provides solutions to numerous security problems associated with all types of computers.

[102] Gordon Hughes. Disjointed Australian assault on hackers. *Computer Law & Practice*, 6(1):28–31, 1989.

[103] IBM Corporation. Data security controls and procedures – a philosophy for DP installations. Technical Report G320-5649, IBM Corporation, New York, 1976.

[104] IBM Corporation. Information systems security controls and procedures – a philosophy for DP installations. Technical Report G320-5649, IBM Corporation, February 1986.

[105] IBM Corporation. PR/SM MVS guide for storage recording. Technical Report GC28-1365, IBM Corporation, 1988.

[106] IBM Corporation. IBM transaction security system. Technical Report G52-6704, IBM Corporation, 1989.

[107] IBM Corporation. VM/SP security and integrity enhancements. Technical Report GC24-5312, IBM Corporation, 1989.

[108] IBM Corporation. AS-400 programming: Security concepts and planning. Technical Report SC21-8083, IBM Corporation, 1990.

[109] Interbank Card Association. PIN manual: A guide to the use of personal identification numbers in interchange, September 1980.

[110] Mary Jander. The naked network. *Computer Decisions*, 21(4):39–42, April 1989.

[111] David L. Jobusch and Arthur E. Oldehoeft. A survey of password mechanisms: Weaknesses and potential improvements. Part 1. *Computers and Security*, 8(7):587–603, November 1989. This paper discusses authentication and password mechanisms. The focus of the first section is user authentication; qualities of a good authentication scheme and basic methods of identifying users. The second section concentrates on password authentication schemes. Ten aspects of passwords are discussed: composition, length, lifetime, source, ownership, distribution, storage, entry, transmission, and authentication period. The final section of the paper analyzes the 4.3BSD password mechanism in terms of each of the ten aspects above.

[112] David L. Jobusch and Arthur E. Oldehoeft. A survey of password mechanisms: Weaknesses and potential improvements. Part 2. *Computers and Security*, 8(8):675–689, December 1989. The first section of this paper summarizes four attacks on computers that took advantage of password weaknesses. Next, methods for improving password mechanisms are discussed. They include methods to improve passwords, such as password generators and monitors; and methods to improve password mechanisms, such as encryption, secondary passwords, pass-algorithms, aging, shadow password files and authentication servers.

[113] Robert E. Johnston. Comparison of access control software for IBM operating systems – ACF2, RACF, SAC, SECURE, & TOP SECRET. *Computer Security Journal*, Fall–Winter 1983.

[114] Daniel V. Klein. Foiling the cracker: A survey of, and improvements to, password security. In *UNIX Security Workshop II*, pages 5–14. The USENIX Association, August 1990. The author presents the results of his attempts to crack 14,000 passwords using a large dictionary of possible passwords. A proactive password checker is proposed, which performs security tests on passwords as the user attempts to select them, thus preventing poor password choices.

[115] R. Knotts and R. Richards. Computer security: Who's minding the store? *The Academy of Management Executive*, 3(1):63, February 1989.

[116] Leonard I. Krauss and Aileen MacGahan. *Computer Fraud and Countermeasures*. Prentice-Hall Inc., Englewood Cliffs, N.J., 1979.

[117] Stanley A. Kurzban. A dozen gross 'mythconceptions' about information processing security. *Security, IFIP/Sec'83*, pages 15–25, 1983.

[118] Stanley A. Kurzban. Easily remembered passphrases – a better approach. *ACM SIGSAC Review*, 3(2–4):10–21, Fall–Winter 1985. The paper proposes the use of passphrases for user authentication. The author claims passphrases of three or four words are more easily remembered than passwords of sufficient length to provide an equivalent combination space. The proposed scheme, Easily Remembered Passphrases (ERP), uses computer generated phrases constructed from lists of adjectives, actors, verbs, and things.

[119] Kenneth J. Kutz. An intrusion from the Netherlands: An Internet and UNIX security case study. This paper provides a detailed description of attacks on computers at Bowling Green State University and other sites around the world. Nearly all penetrations were the result of poor password choices. The steps taken to monitor the activities of the intruders and eventually secure the systems are described, 1991.

[120] L. Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772, November 1981. The paper describes a password authentication scheme that remains secure even if an intruder has access to the system's data and can eavesdrop on communication between the user and system. The scheme requires a one-way encryption function and a smart terminal.

[121] Bill Landreth. *Out of the Inner Circle: A Hacker's Guide to Computer Security*. Microsoft Press, New York, 1984. An ex-hacker discusses the history of hacking, how hackers break into systems, and how to protect computers from being cracked.

[122] John Leggett and Glen Williams. Verifying identity via keystroke characteristics. *International Journal of Man-Machine Studies*, 28(1):67–76, January 1988.

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

[124] A. Liebert. Access by autograph. *System Integrity*, 17(9):45, September 1989.

[125] John Linn. Practical authentication for distributed computing. In *Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy*, pages 31–40, May 1990.

[126] David L. Lipton. Authentication by hash transformation. Technical Report CR-ATH-PR2, Caliban Research Labs, Concord, California, August 1984.

[127] David L. Lipton. Authentication by pattern recognition. Technical Report CR-ATH-PR3, Caliban Research Labs, Concord, California, August 1984.

[128] David L. Lipton. Logical authentication methods. *ACM SIGSAC Review*, 4(2):9–20, Spring 1986. The author describes logical authentication methods, as opposed to physical authentication methods. Prior research in the area and vulnerability of the techniques to compromise

are discussed. The author provides a taxonomy of pass-algorithms that are easy to memorize, easy to execute, and induce large cryptanalytic costs.

[129] David L. Lipton and Harry Wong. Modern trends in authentication. *ACM SIGSAC Review*, 3(2–4):36–42, Fall–Winter 1985. This paper provides a survey of authentication techniques and criteria for choosing among them. The techniques discussed fall into five categories: who the user is, what the user does, what the user has, what the user knows, and what the user recognizes. Criteria for comparison include difficulty of forgery, amount of time and inconvenience for the user, and the amount of system resources used.

[130] J. Lobel. *Foiling the System Breakers: Computer Security and Access Control*. McGraw-Hill, 1986.

[131] M. Luby and C. Rackoff. A study of password security. *Journal of Cryptology*, 1(3):151–158, 1989. The article discusses, in formal terms, the security of the UNIX password mechanism in terms of password length.

[132] Teresa F. Lunt. Automated audit trail analysis and intrusion detection. In *Proceedings 11th National Computer Security Conference*, pages 65–73, October 1988.

[133] Teresa F. Lunt. Access control policies: Some unanswered questions. *Computers and Security*, 8(1):43–54, February 1989.

[134] Lex Luthor and the Legion of Hackers. Hacking IBM's VM/CMS. *2600*, pages 4–5, 16–18, 20–21, November 1987.

[135] R. D. McCrie. Computer security: PCs growing as management challenge, password strategy suggested. *Security Letter XVII*, January 5, 1987.

[136] John E. McEnroe and Curtis C. Verschoor. Biometric personal identification systems: The potential for bank use. *Bank Administration*, 62(11):40–46, November 1986.

[137] Paul Meissner. Evaluation of techniques for verifying personal identity. In *Proceedings, ACM-NBS Fifteenth Annual Technical Symposium*, pages 119–127. National Bureau of Standards, June 17, 1976.

[138] Belden Menkus. DP auditors are offered new ways to evaluate – and to recommend improvements in – password use. *Data Processing Auditing Report*, 34:2–4, February 1986.

[139] Belden Menkus. Understanding password compromise. *Computers and Security*, 7(6):549–552, December 1988. The author discusses several aspects of attacks on passwords. Motivation of the attacker, vulnerabilities of password protection, and methods and strategies employed by the attacker are considered.

[140] Belden Menkus. Understanding the use of passwords. *Computers and Security*, 7(2):132–136, April 1988. This article is a general primer on password security. A background on the use of passwords for authentication is provided, along with several recommendations for secure use. These recommendations include password lengths of 6-8 characters, aging passwords every 10-15 days, and penalties for password disclosure.

[141] Chris Mitchell. Limitations of challenge response entity authentication. *Electronics Letters*, 25(17):1195–1196, August 17, 1989.

[142] Chris Mitchell and Michael Walker. The password predictor – a training aid for raising security awareness. *Computers and Security*, 7(5):475–481, October 1988. This paper describes a password guessing program for UNIX systems that exposes weak password choices and encourages users to make stronger selections. The paper also provides a general background in UNIX password security, a detailed description of the construction and operation of the password predictor, and a summary of the performance of the predictor. Finally, the authors propose two changes in UNIX to improve password security: the removal of world read access to the password file, and addition of audit trails for unsuccessful logins.

[143] Robert Morris and Ken Thompson. Password security: A case history. *Communications of the ACM*, 22(11):594–597, November 1979. The authors discuss the history of password authentication, deficiencies of the methods used, and the improvements that have led to the techniques used today.

[144] D. Morschedian. How to fight password pirates and win. *IEEE Computing*, 19(1):104–105, January 1986.

[145] Neil Munro. Simple password opens Navy computer to hacker. *Government Computer News*, 7(15):61, July 1988.

[146] National Computer Security Center. Password management guideline. Technical Report CSC-STD-002-85, U.S. Department of Defense, 1985.

[147] National Computer Security Center. Trusted computer system evaluation criteria. Technical Report DoD 5200.28-STD, U.S. Department of Defense, 1985.

[148] National Computer Security Center. Computer security subsystem interpretation of trusted computer system evaluation criteria. Technical Report NCSC-TG-009, U.S. Department of Defense, 1988.

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

[150] Evi Nemeth, Garth Snyder, and Scott Seebass. *UNIX System Administration Handbook*. Prentice Hall, Englewood Cliffs, NJ, 1989. Contains a chapter on UNIX security, including a section on passwords.

[151] B. Neugent. Password-based authentication. *ACM SIGSAC Review*, 5(4):10–13, Fall 1987. A humorous article poking fun at many of the authentication schemes currently in use.

[152] Michael Newberry. Minos: Extended user authentication. In *Advances in Cryptology – AUSCRYPT '90 International Conference on Cryptology, Proceedings*, pages 410–423, 1990.

[153] Adrian R. D. Norman. *Computer Insecurity*. Chapman and Hall, London, 1983.

[154] Marcus Page. Passwords are still best security method. *Government Computer News*, July 19, 1985.

[155] I. Palmer and G. Potter. *Computer Security Risk Management.* Van Nostrand Reinhold, New York, 1989.

[156] Donn B. Parker. *Crime by Computer.* Charles Scribner's Sons, New York, 1976.

[157] Donn B. Parker. *Computer Security Management.* Reston Publishing, Reston, VA, 1981.

[158] Donn B. Parker. *Fighting Computer Crime.* Charles Scribner's Sons, New York, 1983.

[159] Richard D. Peacocke and Daryl H. Graf. An introduction to speech and speaker recognition. *Computer 90*, 23(8):26–33, August 1990.

[160] C. Pfleeger. *Security in Computing.* Prentice-Hall, Englewood Cliffs, N.J., 1989.

[161] Sigmund N. Porter. A password extension for improved human factors. *Computers and Security*, 1(1):54–56, January 1982. The author discusses the security benefits and implementation considerations of passphrases.

[162] W. L. Price. A review of methods of personal identity verification. Technical Report DITC 73/86, National Physical Laboratory, July 1986.

[163] George B. Purdy. A high security log-in procedure. *Communications of the ACM*, 17(8):442–445, August 1974. The author discusses the use of polynomials over a prime modulus as opposed to one-way ciphers derived from Shannon codes.

[164] T. M. Raleigh and R. W. Underwood. CRACK: A distributed password advisor. In *USENIX UNIX Security Workshop Proceedings*, pages 12–13, August 1988. The authors describe a network service known as CRACK. The service responds to requests to test how crackable a given encrypted password is.

[165] Bruce L. Riddle, Muray S. Miron, and Judith A. Semo. Passwords in use in a university timesharing environment. *Computers and Security*, 8(7):569–578, November 1989. The authors of this paper analyze the passwords used for 7,014 accounts in a university computing environment. They classify the passwords in several ways: length and character set, mnemonics, names, English and foreign words, and numbers. The passwords used are compared to the list of passwords used by the Internet worm. The article concludes with a psychological discussion of password choices.

[166] Glenn Rinkenberger and Ron Chandos. Non-forgeable personal identification system using cryptography and biometrics. In *13th National Computer Security Conference Proceedings*, pages 80–89. National Institute of Standards and Technology/National Computer Security Center, October 1990. The authors propose an authentication system that they claim provides unforgeable proof of identity. The system employs biometrics, public key cryptography, and memory card technology. An application of the system for secure network login is discussed.

[167] Deborah Russell and G. T. Gangemi Sr. *Computer Security Basics.* O'Reilly & Associates, Cambridge, MA, 1991. This book covers a broad range of computer security topics, including several authentication issues. Hints for choosing and protecting passwords are discussed. Token and biometric based authentication schemes are also presented.

[168] Tsuyoshi Sakaguchi, Osamu Nakamura, and Toshi Minami. Personal identification through facial images using isodensity lines. *SPIE Volume 1199 Visual Communications and Image Processing IV*, pages 643–654, 1989.

[169] Martin Samociuk. Hacking or the art of armchair espionage. *Computer Fraud & Security Bulletin*, Supplement to Volume 7:1–32, 1985. This article is an overview of computer 'hacking.' It covers the techniques used, potential targets, types of hackers, legal issues, and several steps that can be taken to prevent most hacking.

[170] James A. Schweitzer. Computer security: Make your passwords more effective. *The EDP Audit Control and Security Newsletter*, 10(8):6–11, February 1983.

[171] Donn Seeley. Password cracking: A game of wits. *Communications of the ACM*, 32(6):700–703, June 1989. This article describes the password cracking techniques employed by the Internet worm. The four steps used by the worm, as well as the fast encryption algorithm used, are discussed. Finally, the author offers his opinions as to whether the worm caused damage, whether it was malicious in nature, and whether publication of worm details further harm security.

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

[173] T. Shannon. An introduction to VAX/VMS security mechanisms and techniques. *Computers and Security Journal*, 4(2):39–47, Winter 1987.

[174] Kamaljit Singh. On improvements to password security. *Operating Systems Review (ACM)*, 19(1):53–60, January 1985. This paper describes improvements to operating systems that would make passwords less vulnerable to attack. The first improvement prevents eavesdropping on communications through the use of public-key cryptography. The author proposes a protocol for secure communication. The second improvement is an algorithm allowing the use of long password phrases, which prevent the success of exhaustive password searches.

[175] J. Sinha. *Computer Security Manual.* Computer Security Institute, 1983.

[176] Martin R. Smith. *Commonsense Computer Security.* McGraw-Hill, 1989. This book provides a thorough review of general issues in computer security, including sections on password selection, aging, and distribution.

[177] Sidney L. Smith. Authenticating users by word association. *Computers and Security*, 6(6):464–470, December 1987. The author proposes the use of word association lists for user authentication. A study of four subjects who were allowed to select their own lists was conducted, and the memorability and security of the lists selected is analyzed.

[178] Eugene H. Spafford. The Internet worm: Crisis and aftermath. *Communications of the ACM*, 32(6):678–687, June 1989.

[179] Eugene H. Spafford. The Internet worm program: An analysis. *ACM Computer Communication Review*, 19(1):17–57, January 1989. (Also issued as Purdue technical report TR-CSD-823.) This is the original, full-length description of how the Internet Worm operated and what it did.

[180] Eugene H. Spafford. Preventing weak password choices. In *Proceedings of the 14th National Computer Security Conference*, pages 446–455, Oct 1991. This paper describes the OPUS project. OPUS uses a probabilistic hash function mechanism to prevent users from setting weak passwords. The design of the system is presented, along with some of the features that make it particular useful in workstation and network environments.

[181] T. Steinberg. Developing a computer security charter. *SIGSAC*, 6(4):12, Winter 1989.

[182] Jennifer G. Steiner, Clifford Neuman, and Jeffrey I. Schiller. Kerberos: An authentication service for open network systems. In *Proceedings of the Winter USENIX Conference*, Dallas, 1988. This paper describes the Kerberos authentication system. A database of clients, which may be users or applications, and private keys is used to provide authentication for users, services, and hosts.

[183] Cliff Stoll. *The Cuckoo's Egg*. Doubleday, NY, NY, October 1989.

[184] R. Summers and S. A. Kurzban. Potential applications of knowledge-based methods to computer security. *Computers and Security*, 7(4):373–385, August 1988.

[185] John Tunstall. Smartcards – their applications & security features. In *System Security: The Technical Challenge*, pages 1–7, London, October 1985. Online Publications. The author discusses the applications of smartcard technology in the financial world.

[186] D. Umphress and Glen Williams. Identity verification through keyboard characteristics. *International Journal of Man-Machine Studies*, 23:263–273, 1985.

[187] United States General Accounting Office. Computer security. Technical Report GAO/IMTEC-89-57, Washington, D.C., June 1989.

[188] United States General Accounting Office. Computer security: Unauthorized access to a NASA scientific network. Technical Report GAO/IMTEC-90-2, Washington, D.C., 1989.

[189] A. Utter. The four essentials of computer and information security. *The Internet Auditor*, 46(6):44, December 1989.

[190] S. Vallabhaneni. *Auditing Computer Security: A Manual with Case Studies*. Wiley, New York, NY, 1989.

[191] G. H. Warfel. *Identification Technologies: Computer, Chemical, and Optical Aids to Personal ID*. Thomas Publishers, 1979.

[192] Harold Weiss, (ed.). How passwords are cracked. *The EDP Audit Control and Security Newsletter*, 3(3), 1985.

[193] Mark S. Weitz. Handheld password generators: Market overview. *Datapro Reports on Information Security*, pages IS36–001–301:302, March 1991.

[194] Mark S. Weitz. Handheld password generators: Technology overview. *Datapro Reports on Information Security*, pages IS36–001–321:324, March 1991.

[195] Raymond M. Wong, Thomas A. Berson, and Richard J. Feiertag. Polonius: An identity authentication system. In *IEEE 1985 Symposium on Security and Privacy*, pages 101–107, Silver Spring, MD, April 1985. IEEE Computer Society Press. This paper describes an authentication method making use of personal authentication devices known as PassPorts. The devices implement a form on one-time pad encryption. When a user attempts to logon to a host, the host transmits a seven digit challenge. The user keys the challenge along with a PIN into the PassPort and receives a seven digit response. The response is keyed into the terminal, and if it matches what the host expected, the user is authenticated.

[196] C. Wood, W. Banks, S. Guarro, A. Garcia, V. Hampel, and H. Sartorio. *Computer Security: A Comprehensive Controls Checklist.* John Wiley and Sons, 1987.

[197] Charles Cresson Wood. Effective information security with password controls. *Computers and Security*, 2(1):5–10, January 1983. The need for improved password use is discussed in light of several computer break-ins attributed to poor password selection. The author considers the trade-offs between user-friendliness and security, the construction and administration of passwords, and implementation issues.

[198] Charles Cresson Wood. Administrative controls for password-based computer access control systems. *Computer Fraud & Security Bulletin*, 8(3):5–13, January 1986. The author proposes a set of policies for the administration of a password-based access control system. The policies are grouped into four categories: prerequisites to a successful implementation, monitoring logs and security events, accounts administration, and system design considerations. The author concludes that simply having an access control package is not enough; it must be properly installed, used, and administrated to be effective.

[199] Helen M. Wood. On-line password techniques. In *Trends and Applications 1977: Computer Security and Integrity*, pages 27–31, Gaithersburg, MD, May 1977. IEEE Computer Society/National Bureau of Standards.

[200] Helen M. Wood. The use of passwords for controlled access to computer resources. Special Publication 500-9, U.S. Department of Commerce/National Bureau of Standards, May 1977.

[201] Patrick H. Wood and Stephen G. Kochan. *UNIX System Security.* Hayden Book Company, 1987.

[202] T. K. Worthington, T. J. Chainer, J. D. Williford, and S. C. Gunderson. IBM dynamic signature verification. *Security, IFIP/Sec'85*, pages 129–154, 1985.

[203] Joel Zimmerman. The human side of computer security. *Computers and Security Journal*, 3(1):7–19, Summer 1984.

[204] Joel Zimmerman. Is your computer insecure. *Datamation*, May 1985.