User Authentication and Related Topics: An Annotated Bibliography

Eugene H. Spafford
Purdue University, spaf@cs.purdue.edu

Stephen A. Weeber

Report Number:
91-086
USER AUTHENTICATION AND RELATED TOPICS: AN ANNOTATED BIBLIOGRAPHY

Eugene H. Spafford
Stephen A. Weeber

CSD-TR-91-086
December 1991
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


[6] Niv Ahituv, Yehezkel 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.
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.


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.


[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.


[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.


[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.


[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.


[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.


[51] Alex P. Conn, John H. Parodi, and Michael Taylor. The place of biometrics in a user authentication taxonomy. In *12th 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.


[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.


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.


[58] David A. Curry. Improving the security of your UNIX system. Technical Report ITSTD-721-50-21, 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.


[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.


[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.


[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.


[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.


[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.


[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.


[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.


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.


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.

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.


[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.


[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.


[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.


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.


[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.

[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.


[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.


[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.


[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.


[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.


[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.


[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.


[182] Jennifer G. Steinier, 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.


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 of 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.


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.


