# The use of passwords for controlling access to remote computer systems and services*

*by* HELEN M. WOOD
*National Bureau of Standards*
Washington, DC

## ABSTRACT

The widespread use of remote computer resources has made the problem of personal authentication most urgent. This paper examines the use of passwords for controlled access to these resources. Password techniques, ways of protecting passwords, and attendant cost considerations are discussed. Similarities between passwords and data encryption keys are noted and general recommendations for the use of passwords are presented.

## INTRODUCTION

With the growth of timesharing and other forms of computer networking, the use of remote computers and their resources has become widespread. However, with this ease of access have come increased operational risks.

Systems without adequate access controls are vulnerable to threats including theft, fraud, and vandalism. Potential losses range from unauthorized use of computing time to unauthorized modification or access to massive amounts of data. Perpetrators of such abuse may be otherwise honest individuals wishing to play a few computer games, or sophisticated corporate spies hoping to learn trade secrets or acquire the list of a competitor's top ten accounts. (See Reference 1 for a more complete treatment of computer abuse perpetrators.) Current privacy legislation and increased public concern with the integrity and protection of data in computer systems have made the problem of personal authentication most urgent.

## AUTHENTICATION

Typically when a user wishes to access resources on a remote computer system, he or she states a claimed identity, perhaps through typing a user identification number. The user is then required to authenticate the claimed identity. This latter process is referred to as personal authentication.

There are three basic methods by which a person's identity may be established for the purpose of allowing access to a remote computer system:

- something the person *knows*
- something the person *has*
- something the person *is*.

The first category includes techniques and items such as passwords and lock combinations. Badges, ID cards, and keys are among the items falling into the second category; while "something a person *is*" includes physical and behavioral characteristics such as one's appearance, voice, fingerprints, signature, and hand geometry. The advantages and limitations of these types of authentication techniques have been discussed extensively elsewhere.[2-4]

The actual authentication techniques selected for a given system should be determined by a risk analysis. This is a consideration of potential threats,[5] the probability of these threats occurring, and the expected losses resulting from a successful penetration of the system.

Password systems cost less at present than many of the other techniques for personal authentication. Consequently, it appears that passwords, perhaps in combination with other techniques such as badges or keys, will continue to be heavily utilized for some time.

The technique of using passwords to authenticate a user to a resource sharing computer system is well-known. However, the simple use of passwords is not sufficient to guarantee system security from unauthorized users. Cotton and Meissner suggest that passwords for most timesharing systems are "notoriously easy to obtain."[2] There are, however, a number of ways to improve the resistance of password-based security systems to penetration. The intent of this paper is to consider the generation of passwords and their effective application to the problem of controlling access to computer resources.

## USES OF PASSWORDS

Personal authentication may be required at any number of points along the path to accessing data. Such points include

- entry to building
- entry to terminal room
- enabling terminal
- encryption interface unit
- login
- file access
- data item access

Physical devices (e.g., cards, keys) are commonly used at the first three access points. While passwords, alone or in conjunction with other techniques, may be used at any of these points, the primary emphasis of this paper is the use of passwords in an on-line environment. Thus we shall only consider the utilization of passwords at login, file access, or data item access time.

Data encryption keys and the banking community's Personal Identification Number (PIN) are equivalent to passwords. An encryption key controls the algorithmic transformation (encryption) performed on data symbol-by-symbol. The PIN is typically a four-to-six-digit number assigned by the bank or selected by the cardholder. It is used in conjunction with a magnetically encoded card. Throughout this paper analogies will be drawn among encryption keys, PIN's, and passwords.

## PASSWORD SCHEMES

Password schemes differ according to

- selection technique
- lifetime
- physical characteristics
- information content

In this section the types of password systems are discussed along with the threats they are most effective against. Examples are presented.

### *Password selection*

A password may be chosen by the system user or assigned. User-selected passwords usually are less secure since people tend to pick words or numbers that have some personal meaning (e.g., birthday, child's name, street address) and consequently are easy to guess.[6] Of course the primary advantage of a user-chosen password is ease of recall, alleviating the need for writing the password down.

Passwords may be assigned to users by the system security officer or by the computer system itself. Although they are generally more secure than user-selected codes, the benefits of assigned passwords may be nullified if they are written down by the user, taken from a master list which is discovered,[7] or generated by an algorithm that is deducible.[8]

Johnson examined the use of pseudorandom numbers as passwords and discovered that various "logistically attractive" periodic password generation systems are in fact vulnerable to simple number-theoretic analysis. The generating systems he considered were of the type

$$x_{n+1}=ax_n+b(\text{mod } 2^u), \quad u\cong 40,$$

where a and b are selected constants and $x_n$ is the nth password generated. This type of generating system would be considered attractive, for example, in a large databank system in which it is not practical to use complex password schemes.[8]

Another example of a computer-generated password scheme is the random word generator developed to run on Honeywell's Multiplexed Information and Computer System (Multics).[9] The random word generator forms pronounceable syllables and concatenates them to create words. This system was developed to enhance the security of some Multics installations, such as the Air Force Data Services Center (AFDSC), where classified information is processed. Installations such as these cannot risk the compromise of users' passwords.

In his chapter on principles of computer security, Bushkin includes the following principle:

> No passwords or other user authentication data shall have been or shall be created or generated either by the human user who will use them or by a non-human agent (e.g., a program) of his creation or under his control . . .

Although it is not claimed that such a principle applies to each and every system, it is apparent that such nonhuman generation of passwords is the preferred method for enhanced system security.[10]

### *Password lifetime*

Current password schemes allow password assignments to be used for an indefinite period of time, for fixed intervals of time (e.g., one month), or for a single use only. The length of time that a password remains in effect is called the password lifetime or period.

Passwords that remain effective indefinitely are the most susceptible to compromise. Due to the length of the password period, these passwords are especially vulnerable to exhaustive testing. Making the password appropriately long, locking-out log-on attempts after several (e.g., three) tries,[11] and enforcing time delays between log-on attempts are some deterrents against exhaustive enumeration attempts.[12]

Another shortcoming of passwords with indefinite lifetimes is the difficulty in detecting a successful compromise of the password. Some systems prohibit a user from being logged onto the system from more than one terminal at a time.[6] However, even if such system constraints are pres-

ent, the odds of a system penetrator and the legitimate user attempting to use the same account at the same time depend upon the frequency of access of each. Thus, when fixed passwords of indefinite lifetime are used, a masquerader can penetrate another user's files over a long period of time with a low probability of detection.

Obviously more frequent password changes are desirable.[7,13] An example of a system which requires password updates at fixed intervals of time is the Air Force Data Security Center. In this system, users are required to change their passwords every six months. The enforcing mechanism is the operating system.

Passwords that can only be used once are recognized as generally providing a higher level of protection.[12-14] Successive passwords may be selected by the system from an internal list,[12] generated by a program,[8,9,15] or selected from lists or cards previously distributed to authorized users.[6,14]

Anderson[13,16] suggests an open, one-time password scheme. He contends that if passwords are changed each time they are used there is "no more risk in writing down the password than in carrying a key to a locked room." Should loss or theft occur, prompt reporting would minimize the risks involved.

As a means of further reducing the risk of carrying a password openly, Anderson mentions the possibility of encoding the new password on a magnetic card.[13] The feasibility of this technique was investigated by Richardson and Potter.[17] The major disadvantage of such a technique is the cost of the magnetic card reader/writer.

Major drawbacks to the use of one-time passwords are the cost and difficulty associated with the distribution of lists to large numbers of users[16] and with the support of users who get "out of step" in a system with a heavy workload.[6]

It has been noted by Petersen and Turn that one-time password schemes alone are not effective against the threat of between-lines or piggyback entry. For protection against these threats, message authentication via attachment of one-time passwords to each message would be required. Encryption at the terminal level is also an effective protection mechanism in this situation.[5]

*Physical characteristics*

Physical characteristics refer to the size of a password and its makeup (i.e., the "alphabet" from which it is made). The number of different passwords possible in a given scheme is called the password space. For example, given a password of length L that is formed using any of the 26 letters in the English alphabet, there are 26**L possible words that could be generated. Enlarging the alphabet increases the password space accordingly. Including nonprinting characters in the alphabet not only increases the password space, but provides some additional protection.[11] Of course, when conditions such as pronounceability are added to the scheme, then some fraction of the total number of possible words would comprise the password space.

Meissner[4] emphasizes that, in order to adequately assess the security of a given password scheme, one must consider the number of *allowable* combinations for valid passwords, rather than simply the theoretical number of combinations based upon the size of the alphabet and the generated password.

In Reference 13, Anderson considers passwords generated as random strings of letters or numbers. He presents a formula for determining the random password length required to provide a given degree of protection against systematic testing. The assumption is that tests occur at the maximum line transmission rate, as would be the case if another computer were attempting penetration by exhaustive enumeration. In his formula, the password size is found by solving

$$(R/E)4.39\times10^4(M/P)\leq A^S \quad (1)$$

for S, where S is the password size in characters. Here, R is the transmission rate of the line in characters per minute, E is the number of characters exchanged in a log-on attempt, P is the probability that a proper password will be found, M is the period over which the systematic testing is to take place, and A is the size of the alphabet from which the password is made.

As an example, Anderson determines the password size drawn from the English alphabet that gives a probability of no more than 1/1000 of recovery after three months of systematic testing. He assumes a line speed of 300 characters/minute, and an exchange of 100 characters during a log-on attempt. The computation is as follows:

$$\frac{300}{100}\times4.39\times10^4\times3\times10^3\leq26^S \quad (2)$$

$$3.951\times10^8\leq26^S \quad (3)$$

$$26^S=3.089\times10^8 \quad \text{for} \quad S=6 \quad (4)$$

$$26^S=8.03\times10^9 \quad \text{for} \quad S=7 \quad (5)$$

Therefore, in this example S=7 is the reasonable choice. Note that increasing the alphabet to 128 characters (e.g., for 7-bit ASCII) reduces S to 5.

*Information content*

The password may provide information in addition to personal authentication. The University of Western Ontario's generalized information retrieval sytem (GIRS) incorporates the use of assigned, functional passwords whose contents reveal the users' authorization levels.[18] In this system an additional password is needed to effect the initial log-on to the computer system. The functional password is only used by the information retrieval system.

Besides imparting authorization information, it has been suggested that passwords could be constructed to contain check digits or some other sort of self-checking code. "Check digitry" is already being successfully used in other environments, as discussed in a series of articles by Alan Taylor.[19-21] Techniques such as these, combined with some elementary analysis, could help more sophisticated pass-

word systems discriminate between entry-errors (such as transpositions of digits) and actual penetration attempts, especially attempts via exhaustive testing.

This idea is similar to that embodied in Kaufman and Auerbach's general model of an electronic funds transfer (EFT) system. Their system incorporates the use of cryptographic check digits derived *from* the PIN.[22]

*Other schemes*

Many of the disadvantages associated with password systems are minimized or cease to exist altogether if authentication is accomplished via the successful execution of an algorithm. Such procedures are often referred to as "handshaking" or "extended handshakes."[6,23] Some of these procedures directly involve the use of passwords; others can only marginally be considered password schemes.

The ADEPT-50 time-sharing system incorporates a handshaking scheme.[12] In order to gain admittance to the system, the user must supply information items including user identification, passwords, and accounting data. The terminal identification is also compared against the terminal id list for which the user was franchised.

In several systems handshaking is accomplished by a dialog between the system and the user. In such procedures the user may be required to answer personal questions (e.g., child's name, brand of mouthwash) asked in a semi-random fashion, or to supply additional passwords and/or account information.[24]

In another variation, credited to Les Earnest by Hoffman,[25] the system presents the user with a pseudorandom number and requires that the user perform a mental transformation T on that number. The result is then sent back to the computer, which performs an appropriate transformation and compares the results. Thus, the user has performed T on a number x and transmitted y=T(x). Consequently, an eavesdropper monitoring the transmission would at most see x and y.

Hoffman asserts that even simple T's such as

$$T(x)=[(\sum_{\text{i odd}} \text{digit i of } x)^{3/2}]+(\text{hour of the day})$$

raise the work factor in breaking the scheme significantly.

## PASSWORD PROTECTION

The previous section has been concerned with the selection of a password scheme that, in addition to being convenient to use, is secure from discovery through guessing or exhaustive enumeration. However, regardless of the password scheme implemented, protection of the password is vital.

The three times during which the password must be protected, are during

- initial distribution
- storage
- transmission.

In this section we shall address the requirements for guarding the passwords against potential threats that might occur at such times.

*Initial distribution*

The initial distribution of passwords to users is a special case of password assignment, selection, and transmission. Two items must be considered in this situation:

- user identification
- distribution method.

It is usually the practice that first-time users of a system make application in person for authorization to to use the system resources. At that time a temporary password, assigned by the system security officer, can be given to the user. The user then has the responsibility for logging onto the system and changing the password to one known only to him.

In another form of password distribution, more useful when users are great distances from the computing facility, the password is transmitted by mail to the user. PIN's are normally distributed in this manner. If more assurance of receipt is required, registered mail or special messengers can be used.

Initial distribution of encryption keys could be handled in a similar manner, with the magnetic stripe card bearing the first key being sent via registered mail.

*Password storage*

Passwords may be stored in the computer system (e.g., on a disk), or by users (e.g., on paper or magnetically encoded on a card). Dangers inherent in writing down passwords have already been addressed. The storage of passwords on the system and on cards is considered in this section.

Most password schemes employ the use of tables or lists which contain the current password for each authorized system user. (A notable exception would be the user-transformation scheme described above.)[25] As these tables and lists are perhaps the most vulnerable part of a password system, efforts should be taken to protect them. Internal lists from which one-time passwords are assigned should likewise be guarded.

R. M. Needham is credited with being the first to recognize the vulnerability of password lists. An encipherment algorithm attributed to him has been implemented at Cambridge, England. The cipher produced by this algorithm is a "one-way cipher." This is a cipher for which no simple deciphering algorithm exists. In such a scheme, the user's password is encrypted as soon as it is received by the system, and the transformed password is then compared with the encoded table entry.[26]

A discussion of Needham's system and the merits of various others can be found in Reference 27. Purdy[28] also

describes the Needham scheme, discusses the selection of good one-way ciphers, and suggests the use of polynomials over a prime modulus.

There are still potential threats involved in such schemes. One is the interception of passwords prior to encryption, and another is the selection of a poor cipher. The first problem will be dealt with in the next section.

An example of a poor cipher would be one that is highly degenerate (i.e., one in which many combinations encrypt to the same value).[29] Under such a scheme the simple exposure of the encrypted list could give enough information to a would-be penetrator to allow him to, if not break the algorithm, at least access the files of any users whose passwords in their encrypted form were identical to his.

As a part of their Multics vulnerability analysis the Air Force considered the threat of exposure of password files.[30] Their report asserts that accessing the system password file is of minimal value to a system penetrator. Assuming that the password file is the most highly protected file in the system, anyone who succeeded in accessing this file could conceivably penetrate *any* other file in the system! Furthermore, if the password list were enciphered, then it would be much easier to simply ignore it than to attempt to decode it.

For completeness the Air Force study did analyze the "non-invertible" encipherment scheme used at that time by the Multics system. In a report soon to be published the details of their successful penetration of that scheme will be detailed.[31]

In some systems using magnetic stripe cards the PIN itself is stored on the card in an encrypted form. When discussing the threats to bank card systems presented by the underworld,[32] Industrial National Bank Vice President Ernest Northup described the components of a card-based electronic funds transfer system and noted that the "use of a standard PIN scrambling technique or algorithm for bank interchange would require that its elements be widely known, at least among equipment vendors. This increases its vulnerability."

In Reference 22, Kaufman and Auerbach present a comprehensive set of security principles for EFT systems. Concerning the storage of PIN's they state that "there should be no way to derive the PIN from information on the card," although they observe that many current schemes are based upon such risky techniques.

*Password transmission*

Passwords are vulnerable to several threats during their transmission from terminal to computer. Potential threats include wiretapping, electronic eavesdropping, and piggyback infiltration. The password may also be discovered later in the trash if a hardcopy terminal was used, or observed on a CRT screen immediately after entry. These latter two problems are usually dealt with by masking (the over-printing or under-printing of a series of characters) or echo-suppression. However, as pointed out by Carroll and McLellan,[33] in general the "use of a mask affords no protection to users on CRT visual display terminals." Another method sometimes used incorporates non-printing characters as a part or all of the password.[4,11]

In a discussion of piggyback infiltration, Carroll and Reeves described a situation in which unsuspecting terminal users could be "exploited by a process which mimics the real system long enough to obtain a password. . . ."[34] Of course, echo-suppression and masking are of no help in countering this type of threat. If a more intelligent device than a terminal is used to intercept the conversation, then non-printing characters also lose their effectiveness.

The user-transformation schemes described by Hoffman[25] and Carroll[35] are one way of effectively shielding the password in transit. Here the user, when presented with a random number, performs a pre-determined transformation on it and transmits the result back to the computer for verification. The incorporation of a date-time group into this transformation is recommended to provide additional protection against piggyback infiltration.[35]

Optimal protection of the transmitted password, as with any data, can be realized by encryption of the communications link during the entire conversation.[15,36] The NBS encryption algorithm would be suitable for this purpose.[37]

Brandstad notes that encryption keys and authentication codes may be in effect the same item. In his proposed network access control machine, these keys are never transmitted through the network, but rather are loaded simultaneously by interface units into a primary encryption device. Thus, authentication can be considered complete at that level (at least) if a message can be encrypted, transmitted, and correctly decrypted.[36,38]

In a recent master's thesis on encryption-based protection protocols, Kent addresses encryption key distribution protocols.[39] He identifies two basic transmission techniques:

- chained key changes
- two-level key distribution systems.

Under the chained key system, each new key is enciphered using the last key issued. This new key is then used until another change occurs. Under the two-level distribution system, a special key is used solely for transmitting new keys to remote users. Kent describes protocols for using these schemes and considers the use of magnetic stripe cards for distribution of keys.

## COST CONSIDERATIONS

The costs of a given password scheme are those incurred

- by the protector
- by the intruder.

These costs must be considered in conjunction with the value of the information to be protected. (See Reference 40 for a discussion on the value of personal information in qualitative terms.)

The costs to the protector include not only the hardware

and software costs involved, but also the effect on overall system performance. Processing time required and communications channel loading may result in severely degraded system response time.

Password schemes have been described which involve authentication to the file or data item level. Turn observes that the "costs of access control operations reflect themselves in increased processing time and storage space requirements."[41] He relates the results of a study of these costs which revealed a 22 to 140 percent processing time increase in file access operations, depending upon when access controls are applied (e.g., at file open time, or data item access time). Such implementation costs in a computer networking environment are considered in Reference 42.

The cost to the system intruder includes the investment in time and equipment (i.e., the work factor) necessary to determine the password or password-generating algorithm. Risk can also be considered part of the penetration cost.

As an example, consider the intruder's cost of acquiring passwords through wiretapping. These could range from the cost of recording equipment (a few hundred dollars), to the cost of a minicomputer and associated software development (several thousand dollars). Risks include possible legal prosecution.[40]

As aptly stated by Petersen and Turn,[5] "the level of work factor which is critical for a given information system depends, of course, on an estimate of the magnitude of threats and of the value of the information." They suggest that a work factor of one day of continuous computation required to break a single encryption key might be adequate against low-level threats.

Of course, the cost of the system utilized in the penetration effort must also be considered. For example, Diffie and Hellman have suggested a configuration consisting of 1,000,000 chips and associated controlling and power supply hardware costing around $20,000,000. They assert that such a system could search the key space of the proposed NBS encryption algorithm in about a day, assuming the possession of a matching block of encrypted and unencrypted text.[43]

## CONCLUSIONS

Passwords can be a highly effective form of personal authentication when care is taken in their selection and protection. We have categorized the types of password schemes, identified their capabilities and limitations, and indicated the points at which password protection mechanisms are needed.

The exact password scheme appropriate for a given system depends, of course, upon the required level of security as determined by risk analysis. Cost is also a factor in the selection of the "right" password system.

Until other forms of personal authentication become more cost-effective, the password will remain the most widely used means of controlling access to remote computing systems and services.

## REFERENCES


1. Parker, Donn B., "Computer Abuse Perpetrators and Vulnerabilities of Computer Systems," *Proceedings of the National Computer Conference,* AFIPS Press, Montvale, N.J., 1976, p. 65-73.
2. Cotton, Ira W. and Paul Meissner, "Approaches to Controlling Personal Access to Computer Terminals," *Proceedings of the 1975 Symposium Computer Networks: Trends and Applications,* IEEE Computer Society, 1975, p. 32-39, 19 refs.
3. Browne, Peter S., "Computer Security—A Survey," *Proceedings of the National Computer Conference,* AFIPS Press, Montvale, N.J., 1976, p. 53-63, 134 refs.
4. Meissner, Paul, *Guideline on Evaluation of Techniques for Automated Personal Identification,* National Bureau of Standards, Washington, D.C., 1977 [in press].
5. Petersen, H. E. and R. Turn, "System Implications of Information Privacy," *Proceedings of the Spring Joint Computer Conference,* AFIPS Press, Montvale, N.J., 1967, p. 291-300, 14 refs.
6. Beardsley, Charles W., "Is Your Computer Insecure?" *IEEE Spectrum,* January 1972, p. 67-78, 16 refs.
7. Winkler, Stanley, and Lee Danner, "Data Security in the Computer Communication Environment," *Computer,* February 1974, p. 23-31, 7 refs.
8. Johnson, S. M., *Certain Number Theoretic Questions in Access Control,* Rand Corporation, Report R-1494-NSF, January 1974.
9. Gasser, M., *A Random Word Generator for Pronounceable Passwords,* The MITRE Corporation, Bedford, Mass., AD-A017 676, November 1975, 183p., 3 refs.
10. Bushkin, Arthur A., *A Framework for Computer Security,* System Development Corporation, McLean, Va., AD-A025 356, June 1975, 158p.
11. Held, Gilbert, "Locking Intruders Out of a Network," *Executive Guide to Data Communications,* McGraw-Hill Publications Co., New York, 1976.
12. Weissman, C., "Security Controls in the ADEPT-50 Time-sharing System," *Proceedings of the Fall Joint Computer Conference,* AFIPS Press, 1969, p. 119-133, 20 refs.
13. Anderson, James P., "Information Security in a Multi-user Computer Environment," *Advances in Computers,* Vol. 12, 1972, Academic Press, Inc., New York, p. 1-36.
14. Peters, Bernard, "Security Considerations in a Multi-programmed Computer System," *Proceedings of the Spring Joint Computer Conference,* AFIPS Press, Montvale, N.J., 1967, p. 283-286.
15. Baran, Paul, *On Distributed Communications: IX. Security, Secrecy, and Tamper-free Considerations,* Rand Corporation, August 1964, AD-444 839, 39p.
16. Anderson, James P., *On Centralized Distribution of One-time Passwords in Resource Sharing Systems,* James P. Anderson and Co., Fort Washington, Pa., August 1971, 8p.
17. Richardson, Mark H. and James V. Potter, *Design of a Magnetic Card Modifiable Credential System Demonstration,* Electronic Systems Division (AFSC), Hanscom Field, Mass., MCI-73-3, December 1973, 65p.
18. Carroll, John M., Robert Martin, Lorine McHardy and Hans Moravec, "Multi-dimensional Security Program for a Generalized Information Retrieval System," *Proceedings of the Fall Joint Computer Conference,* Vol. 39, 1971, p. 571-577, 5 refs.
19. Taylor, Alan, "Darmstadt System Eliminates Check-Digit Loopholds," *Computerworld,* September 17, 1975, p. 13.
20. Taylor, Alan, "Deeds Check-Digit Method Possibly Valuable DP Tool," *Computerworld,* October 22, 1975, p. 11.
21. Taylor, Alan, "Statistics Improving State of Art in 'Check-Digitry'," *Computerworld,* February 23, 1976, p. 17.
22. Kaufman, D. and K. Auerbach, "A Secure National System for Electronic Funds Transfer," *Proceedings of the National Computer Conference,* AFIPS Press, 1976, p. 129-138, 6 refs.
23. Campaigne, Howard and Lance J. Hoffman, "Computer Privacy and Security," *Computers and Automation,* 22:7, July 1973, p. 12-17, 6 refs.
24. Lupton, William Lloyd, *A Study of Computer Based Data Security Techniques,* Naval Postgraduate School, Monterey, California, AD-765 677, 1973, 77p., 141 refs.
25. Hoffman, Lance J., "Computers and Privacy: A Survey," *Computing Surveys,* 1:2, June 1969, p. 85-103, 69 refs.

26. Wilkes, M. V., *Time Sharing Computer Systems,* American Elsevier, New York, 1975.
27. Evans, Arthur Jr. and William Kantrowitz, "A User Authentication Scheme Not Requiring Secrecy in the Computer," *Communications of the ACM,* 17:8, (August 1974), p. 437-442, 8 refs.
28. Purdy, George B., "A High Security Log-in Procedure," *Communications of the ACM,* 17:8, August 1974, p. 442-445, 8 refs.
29. Fletcher, J. G., *Software Security in Networks,* Lawrence Livermore Laboratory, University of California, 1975, 17p.
30. Karger, Paul A. and Roger R. Schell, *Multics Security Evaluation: Vulnerability Analysis,* Electronic Systems Division (AFSC), Hanscom AFB, Mass., ESD-TR-74-193, Vol. II, June 1974, 156p., 33 refs.
31. Downey, Peter J., *Multics Security Evaluation: Password and File Encryption Techniques,* Electronic Systems Division (AFSC), Hanscom AFB, Mass., ESD-TR-74-193, Vol. III, in preparation.
32. Northup, Ernest H., "Bank Cards Vs. the Underworld," *Banking,* 67:9, September 1975, p. 66, 68, 70, 73.
33. Carroll, John M. and P. M. McLelland, "The Data Security Environment of Canadian Resource-sharing Systems," *INFOR, Canadian Journal of Operational Research and Information Processing,* 9:1, March 1971, p. 58-67, 17 refs.
34. Carroll, John M. and Paul Reeves, "Security of Data Communications: A Realization of Piggyback Infiltration," *INFOR, Canadian Journal of Operational Research and Information Processing,* 11:3, (October 1973), p. 226-231, 2 refs.
35. Carroll, J. M. and P. M. McLelland, "Fast 'Infinite-key' Privacy Transformation for Resource-sharing Systems," *Proceedings of the Fall Joint Computer Conference,* AFIPS Press, 1970, p. 223-230, 12 refs.
36. Branstad, Dennis K., "Encryption Protection in Computer Data Communications," *Proceedings of the Fourth Data Communications Symposium,* IEEE Computer Society, October 1975, p. 8-1-8-7, 2 refs.
37. National Bureau of Standards, "Proposed Standard Encryption Algorithm for Computer Data Protection," *Federal Register,* 40:52, August 75, 12134-12140.
38. Branstad, Dennis K., "Security Aspects of Computer Networks," *Proceedings of AIAA Computer Network Systems Conference,* American Institute of Aeronautics and Astronautics, New York, N.Y., April 1973, 8p.
39. Kent, Stephen T., "Encryption-Based Protection Protocols for Interactive User-Computer Communication," (Master's Thesis), Massachusetts Institute of Technology, Cambridge, Mass., AD-A026 911, May 1976, 122 p., 42 refs.
40. Turn, Rein and Norman Z. Shapiro, "Privacy and Security in Databank Systems—Measures of Effectiveness, Costs, and Protector-intruder Interactions," *Proceedings of the Fall Joint Computer Conference,* AFIPS Press, Montvale, N.J., 1972, p. 435-444, 26 refs.
41. Turn, Rein, *Privacy Protection in Databanks: Principles and Costs,* The Rand Corporation, Santa Monica, California, AD-A023 406, September 1974, 21 p., 19 refs.
42. Lientz, Bennet P. and Ira R. Weiss, *On the Evaluation of Reliability and Security Measures in a Computer Network,* Office of Naval Research, Arlington, Va., AD-A002 996, December 1974, 28p., 19 refs.
43. Meissner, Paul, *Report of the 1976 Workshop on Estimation of Significant Advances in Computer Technology,* National Bureau of Standards, NBS-IR 76-1189, August 30-31, 1976, 70p., [in press].