FIPS PUB 112

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

1985 MAY 30

U.S. DEPARTMENT OF COMMERCE/National Bureau of Standards

PASSWORD USAGE

CATEGORY: ADP OPERATIONS
SUBCATEGORY: COMPUTER SECURITY

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
30-05-1995		xx-xx-1995 to xx-xx-1995

4. TITLE AND SUBTITLE
Password Usage
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Burrows, James H. ;

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
National Institute of Standards Technology
xxxxx, xxxxxxx

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
IATAC
3190 Fairview Park Drive
Falls Church, VA22042

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES
CATALOGERS: Report date and dates covered should be 1985

14. ABSTRACT
See report.

15. SUBJECT TERMS
IATAC COLLECTION

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	88	email from Booz Allen Hamilton (IATAC), (blank) lfenster@dtic.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	5/30/1985	Report 5/30/1985

4. TITLE AND SUBTITLE
Password Usage (FIPS PUB 112)

5. FUNDING NUMBERS

6. AUTHOR(S)
Burrows, James H.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Department of Commerce,
Technology Administration,
NIST

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

IATAC
3190 Fairview Park Drive
Falls Church, VA 22042

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

The document specifies basic security criteria for two different uses of passwords in an ADP system, (I) personal identity
authentication and (2) data access authorization. It establishes the basic criteria for the design, implementation and use of a password system in those systems where passwords are used. It identifies fundamental ADP management functions pertaining to passwords and specifies some user actions required to satisfy these functions. In addition, it specifies several technical features which may be implemented in an ADP system in order to support a password system. An implementation schedule is established for compliance with the Standard. Numerous guidelines are provided in the Appendices for
managers and users seeking to comply with the Standard.

14. SUBJECT TERMS
IATAC Collection, information security, computer security, data security, passphrase, password, personal identification , systems security

15. NUMBER OF PAGES
87

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

U.S. DEPARTMENT OF COMMERCE, Malcolm Baldrige, Secretary
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Director

Foreword

The Federal Information Processing Standards Publication Series of the National Bureau of Standards is the official publication relating to standards adopted and promulgated under the provisions of Public Law 89-306 (Brooks Act) and under Part 6 of Title 15, Code of Federal Regulations. These legislative and executive mandates have given the Secretary of Commerce important responsibilities for improving the utilization and management of computers and automatic data processing in the Federal Government. To carry out the Secretary's responsibilities, the NBS, through its Institute for Computer Sciences and Technology, provides leadership, technical guidance, and coordination of Government efforts in the development of guidelines and standards in these areas.

The need for physical, administrative, and technological measures to protect Federal information has become an acknowledged fact. Passwords and passphrases have become a commonly used measure to identify the authorized users of computer systems and, in some instances, to control access to data stored within a computer system. Passwords must be administratively controlled since they are issued to and known by people. Passwords must also be technologically controlled since they are stored in and processed by computers. This Standard and the Guidelines in the Appendices of the Standard establish fundamental administrative and technological controls for the proper usage of passwords. If the Standard and the Guidelines are followed properly, the security provided by a password security system will be enhanced.

James H. Burrows, Director Institute for Computer Sciences and Technology

Abstract

The document specifies basic security criteria for two different

uses of passwords in an ADP system, (I) personal identity authentication and (2) data access authorization. It establishes the basic criteria for the design, implementation and use of a password system in those systems where passwords are used. It identifies fundamental ADP management functions pertaining to passwords and specifies some user actions required to satisfy these functions. In addition, it specifies several technical features which may be implemented in an ADP system in order to support a password system. An implementation schedule is established for compliance with the Standard. Numerous guidelines are provided in the Appendices for managers and users seeking to comply with the Standard.

Key words: computer security; data security; passphrase; password; personal identification; systems security.

Natl. Bur. Stand. (U.S.) Fed. Info. Process. Stand. Pub. (FIPS PUB) 112, 55 pages (1985) CODEN:FIPPAT

For sale by the National Technical Information Service, U.S. Department of Commerce, Springfield. VA 22161.

FIPS PUB 112

Federal Information
Processing Standards Publication 112

1985 May 30
Announcing the Standard for

PASSWORD USAGE

Federal Information Processing Standards Publications are issued by the National Bureau of Standards pursuant to section 111 (f) (2) of the Federal Property and Administrative Services Act of 1949, as amended, Public Law 89-306 (79 Stat. 1127), Executive Order 11717 (38 FR 12315, dated May 11, 1973), and Part 6 of Title 15 Code of Federal Regulations (CFR).

1. Name of Standard. Password Usage.

2. Category of Standard, ADP operations, computer security.

3. Explanation. A password is a sequence of characters that can

be used for several authentication purposes. Passwords are often used to authenticate the identity of an automated data processing (ADP) system user and, in some instances, to grant or deny access to private or shared data. This Standard recognizes that passwords are not the only method of personal authentication, nor does it endorse the use of passwords as the best method; however, it recognizes that passwords are widely used in computer systems and networks for these purposes. In these systems and networks, compliance with this Standard will ensure that the passwords are used in accordance with accepted practices.

This Standard specifies basic security criteria for two different uses of passwords in an ADP system, (1) personal identity authentication and (2) data access authorization. A password used for personal identity authentication will be called a personal password; a password used for authorizing access will be called an access password. A personal password should not also be used as an access password. This Standard does not require the use of passwords in an ADP system for either purpose, but establishes the basic criteria for the design, implementation and use of a password system in those systems where passwords are used.

This Standard identifies fundamental ADP management functions pertaining to passwords and specifies some user actions required to satisfy these functions. In addition, it specifies several technical features which may be implemented in an ADP system in order to support a password system. Those technical features desired by the ADP management should be specified in all procurement documents when acquiring new systems, and provisions should be made to ensure that they are included when upgrading existing systems. Technical features which are recommended for an ADP system are marked with an asterisk (*), In order to facilitate use of this Standard, this document includes explanatory and guideline appendices.

Some of the requirements of the Standard may be satisfied either through management functions or through technical features. For example, if the Security Officer specifies that each personal password is to be changed

at least every 6 months, the ADP manager can issue a directive to this effect or the ADP system can be programmed to automatically change a password 6 months after entry of its last change. This Standard does not specify how the criteria shall be met, but only what criteria shall be met. The technical features specified in the Standard are generally recommended, but cost considerations (costs to modify existing systems or additional operational costs)

may require that management functions be utilized temporarily in satisfying the specified criteria.

4. Approving Authority. Secretary of Commerce.

5. Maintenance Agency. U.S. Department of Commerce, National Bureau of Standards, Institute for Computer Sciences and Technology.

The terms "secret" and "compromise" are used in this document in accordance with their dictionary definitions and do not imply National Security (Defense) related definitions. Use of cryptography to generate or transmit passwords for access to, or authentication of, classified information requires prior review and approval of the National Security Agency.

Export Control: Password systems incorporating cryptography and technical data regarding them are subject to Federal Government export control as specified in Title 22, Code of Federal Regulations, Parts 122 through 128. Software, firmware, and hardware incorporating cryptography and technical data regarding them must comply with these regulations.

10. Implementation Schedule. This Standard becomes effective June 1,1986.

11. Waivers. Heads of agencies may request that the requirements of this Standard be waived in instances where it can be clearly demonstrated that there are appreciable performance or cost advantages to be gained and when the overall interests of the Federal Government are best served by granting the requested waiver. Such waiver requests will be reviewed by and are subject to the approval of the Secretary of Commerce. The waiver request must specify anticipated performance and cost advantages in the justification for the waiver.

Forty-five days should be allowed for review and response by the Secretary of Commerce. Waiver requests shall be submitted to the Secretary of Commerce, Washington, DC 20230, and labeled as a Request for a Waiver to Federal Information Processing Standards Publication 112. No agency shall take any action to deviate from this Standard prior to the receipt of a waiver approval from the Secretary of Commerce.

12. Where to Obtain Copies. Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 112 (FIPS PUB 112), and title. When microfiche is desired, this should be specified. Payment may be made by check, money order, or deposit account.

Federal Information
Processing Standards Publication 112

1985 May 30
Specifications for
PASSWORD USAGE

CONTENTS

		Page
1.	Terms and Conventions	8
1.1	Access Password	8
1.2	Authentication Process	8
1.3	Authorization Process	8
1.4	Compromise (Verb)	8
1.5	Cryptographic Key	8
1.6	Data	8
1.7	Data Encrypting Key	8
1.8	Encryption	8
1.9	Key Encrypting Key	8
1.10	Passphrase	8
1.11	Password System	9
1.12	Personal Identifier	9
1.13	Personal Password	9
1.14	Replace	9
1.15	Security Officer	9
1.16	System Manager	9
1.17	Valid Password	9

1.18 Virtual Password 9
2. Factors 9
2.1 Composition 9
2.2 Length Range 9
2.3 Lifetime 10
2.4 Source 10
2.5 Ownership 10
2.6 Distribution 10
2.7 Storage 10
2.8 Entry 10
2.9 Transmission 10
2.10 Authentication Period 10
3. Acceptable Basic Criteria 10
3.1 Composition 10
3.2 Length Range 11
3.3 Lifetime 11
3.4 Source 11
3.5 Ownership 12
3.6 Distribution 12
3.7 Storage 12
3.8 Entry 12

3.9 Transmission 13
3.10 Authentication Period 13

APPENDICES

APPENDIX A. PASSWORD USAGE GUIDELINES 14
1. Introduction 14
2. Background 14
3. Factors 14
3.1 Composition 15
3.2 Length 15
3.3 Lifetime 16
3.4 Source 17
3.5 Ownership 17
3.6 Distribution 17
3.7 Storage 18
3.8 Entry 19

3.9 Transmission 20
3. 10 Authentication Period 20
4. Examples of Password Systems 21
4. 1 Password System for Low Protection Requirements 21
4.2 Password System for Medium Protection Requirements 21
4.3 Password System for High Protection Requirements 22
APPENDIX B. EXAMPLES OF COMPLIANCE AND PROCUREMENT DOCUMENTS 23
1. Example of a Minimum Security Compliance Document 23
2. Example of a Procurement Specification for a Minimum Security Password System 24
3. Example of a Medium Security Compliance Document 24
4. Example of a Procurement Specification of a Medium Security Password System 25
APPENDIX C. 95-Character Graphic Subset from FIPS PUB 1-2 26
APPENDIX D. PASSWORD ENCRYPTION AND PASSPHRASE TRANSFORMATION 27
APPENDIX E. PASSWORD MANAGEMENT GUIDELINE 36
1. Introduction 36
2. Scope 36
3. Control Objectives 37
4. Definitions 37
5. Guidelines 38

5.1 SSO Responsibilities 38
5.1.1 Initial System Passwords 38
5.1.2 Initial Password Assignment 38
5.1.3 Password Change Authorization 39
5.1.4 Group IDs 39
5.1.5 User ID Revalidation 39
5.2 User Responsibilities 39
5.2.1 Security Awareness 39
5.2.2 Changing Passwords 39
5.2.3 Login to a Connected System 41
5.2.4 Remembering Passwords 41
5.3 Authentication Mechanism Functionality 41
5.3.1 Internal Storage of Passwords 41
5.3.2 Entry 41
5.3.3 Transmission 42
5.3.4 Login Attempt Rate 42
5.3.5 Auditing 42

5.4 Password Protection 43
5.4.1 Single Guess Probability 43
5.4.2 Password Distribution 43
APPENDIX E.1 PASSWORD GENERATION ALGORITHM 44
1. Password Space 44
2. Random Seeds44
3. Pseudo-Random Number Generator 44
4. "User-Friendly" Passwords 45
APPENDIX E.2 PASSWORD ENCRYPTION ALGORITHM 46
1. Encryption Algorithm 46
2. Assurance for Unique Encrypted Passwords 46
APPENDIX E.3 DETERMINING PASSWORD LENGTH 47
1. Relationship47
2. Guess Rate 47
3. Password Lifetime48
4. Password Space 48
5. A Procedure For Determining Password Length 48
6. Worked Examples 49
7. Passphrases50
APPENDIX E.4 PROTECTION BASIS FOR PASSWORDS 52
1. Systems Containing Only Unclassified Information 52
2. Systems Containing Classified Information 52
APPENDIX E.5 FEATURES FOR USE IN VERY SENSITIVE APPLICATIONS 53
1. One-Time Passwords 53
2. Failed Login Attempt Limits 53
APPENDIX E.6 ON THE PROBABILITY OF GUESSING A PASSWORD 54
APPENDIX E.7 REFERENCES 56

1. Terms and Conventions

The following terms or conventions and associated descriptions are used in the Standard.

1.1 Access Password

A password used to authorize access to data and distributed to all those who are authorized similar access to that data.

1.2 Authentication Process

The actions involving (l) obtaining an identifier and a personal password from an ADP system user; (2) comparing the entered password with the stored, valid password that was issued to, or selected by, the person associated with that identifier; and (3) authenticating the identity if the entered password and the stored password are the same. (Note: If the enciphered password is stored, the entered password must be enciphered and compared with the stored ciphertext or the ciphertext must be deciphered and compared with the entered password.)

1.3 Authorization Process

The actions involving (1) obtaining an access password from an ADP system user (whose identity has already been authenticated, perhaps using a personal password); (2) comparing the access password with the password associated with the protected data; and (3) authorizing access to the data if the entered password and the stored password are the same (see note above).

1.4 Compromise (Verb)

Disclosing a password, or part of a password, to someone not authorized to know, have or use the password.

1.5 Cryptographic Key

A parameter (e.g., a secret 64-bit number for DES) used by a cryptographic process that makes the process completely defined and usable only by those having that key.

1.6 Data

Programs, files or other information stored in, or processed by, a computer system.

1.7 Data Encrypting Key

A cryptographic key used for encrypting (and decrypting) data.

1.8 Encryption

The process of transforming data to an unintelligible form in such a way that the original data either cannot

be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process (two-way encryption).

1.9 Key Encrypting Key

A cryptographic key used for encrypting (and decrypting) data encrypting keys or other key encrypting keys.

1.10 Passphrase

A sequence of characters, longer than the acceptable length of a password, that is transformed by a password system into a virtual password of acceptable length.

1.11 Password System

A system that uses a password or passphrase to authenticate a person's identity or to authorize a person's access to data and which consists of a means for performing one or more of the following password operations: generation, distribution, entry, storage, authentication, replacement, encryption and/or decryption of pass-words.

1.12 Personal Identifier

A data item associated with a specific individual which represents the identity of that individual and may be known by other individuals.

1.13 Personal Password

A password that is known by only one person and is used to authenticate that person's identity.

1.14 Replace

To change a password to a different password selected from all possible acceptable passwords.

1.15 Security Officer

The ADP official, described in OMB Circular A-71, Transmittal Memorandum Number l (July 27,1978), having the designated responsibility for the security of an ADP system.

1.16 System Manager

The ADP official who is responsible for the operation of an ADP system.

1.17 Valid Password

A personal password that will authenticate the identity of an individual when presented to a password system or an access password that will allow the requested access when presented to a password system.

1.18 Virtual Password

A password computed from a passphrase that meets the requirements of password storage (e.g., 64 bits for DES).

2. Factors

The following basic factors shall be considered in the design, implementation, and use of a password system used to authenticate the identity of a person or to control access to data. The factors are:

2.1 Composition

Composition is the set of acceptable characters which may be used in a valid password.

2.2 Length Range

Length Range is the set of acceptable lengths of passwords, expressed as a minimum length through a maximum length (e.g., 4-8), i.e., all the acceptable number of characters in a valid password.

2.3 Lifetime

Lifetime is the maximum acceptable period of time for which a password is valid.

2.4 Source

Source is the set of acceptable entities which can create or select a valid password from among all acceptable passwords.

2.5 Ownership

Ownership is the set of individuals who are authorized to use a password.

2.6 Distribution

Distribution is the set of acceptable methods for providing (transporting) a new password to its owner and to all places where it will be needed in the password system.

2.7 Storage

Storage is the set of acceptable methods of storing a valid password during its lifetime.

2.8 Entry

Entry is the set of acceptable methods by which a password may be entered by an ADP user for authentication or authorization purposes.

2.9 Transmission

Transmission is the set of acceptable methods for communicating a password from its point of entry to its point of comparison with a stored, valid password.

2.10 Authentication Period

Authentication period is the maximum acceptable period between any initial authentication process and subsequent reauthentication processes during a single terminal session or during the period data is being accessed.

3. Acceptable Basic Criteria

A Password Standard Compliance Document shall be prepared by the Security Officer acting in conjunction with the ADP system manager which states for each selected factor, including the 10 basic factors: l) the complete set of criteria to be satisfied; 2) the rationale for selecting the criteria; 3) the criteria to be satisfied with technical features implemented in the ADP password system; 4) the criteria to be satisfied through management functions and user actions. Only technical features required for an ADP password system should be included in procurement specifications. Technical features are noted below by an asterisk (*),

3.1 Composition

3.1.1 Passwords shall be composed using a subset of characters selected by the System Manager and the Security Officer from the set of 95 graphics characters specified in FIPS PUB 1-2 and in Appendix C.

3.1.2 The subset shall not consist of less than 10 characters (e.g., the digits (k-9).

3.1.3 (*) An automated password system shall verify that only characters in the selected subset have been generated or selected whenever a password is created or changed.

3.2 Length Range

3.2.1 Passwords shall have a length range, selected by the System Manager and Security Officer, having a number greater than or equal to four (4) as the minimum length and a maximum length, based on, but not specified in, this Standard.

3.2.2 The selected password composition and length range shall allow for a minimum of 104 (10,000) possible passwords.

3.2.3 The selected password length range shall provide a level of protection commensurate to the value or sensitivity of the

resources or data it protects.

3.2.4 Passphrases (i.e., passwords or encrypted passwords which cannot be stored in 64 bits) which are interchanged among ADP systems shall be transformed to a 64-bit virtual password (e.g., using the transformation algorithm specified in Appendix D) for storage.

3.2.5 (*) An automated password system shall verify that only passwords having a length within the acceptable length range shall be generated or selected whenever a password is created or changed.

3.3 Lifetime

3.3.1 Passwords shall have a maximum lifetime of 1 year.

3.3.2 Passwords shall have the shortest practical lifetime, selected by the Security Officer in conjunction with the Systems Manager, which provides the desired level of protection at the least possible cost (i.e., passwords should be changed often but only if the cost of replacement is reasonable and the owner is able to adopt the new password easily).

3.3.3 Passwords shall be replaced as quickly as possible but at least within l working day from the time that a compromise of the password is suspected or confirmed.

3.3.4 Passwords shall be deleted or replaced with an invalid password as quickly as possible but at least within 3 working days from the time that an owner is no longer an authorized ADP system user or any one of a set of owners is no longer authorized access to the data.

3.3.5 Passwords forgotten by their owner shall be replaced, not reissued.

3.3.6 (*) An automated password system shall allow the Security Officer to delete or replace a password (subsequent to authenticating the identity of the Security Officer).

3.3.7 (*) An automated password system shall have the capability of maintaining a record of when a password was created and changed.

3.4 Source

3.4.1 The source of passwords shall be selected by the Security Officer and the System Manager, and shall be one or more of the following: user, security officer, or automated password generator.

3.4.2 All passwords that may be included in a new system when it is delivered, transferred or installed (e.g., passwords for the operator, system programmer, maintenance personnel or Security Officer) shall be immediately changed by the Security Officer to: (a) passwords that are invalid to the password system; (b) random passwords that may be subsequently changed; or (c) valid passwords that are owned by authorized users of the system and created in accordance with this Standard.

3.4.3 Passwords that are created by the Security Officer for new users of the system during initial system access shall be selected at random from all acceptable passwords (i.e., default passwords or formatted passwords related to the new users identity or assignment shall not be used).

3.4.4 Users that create or select their own personal password shall be instructed to use a password selected from all acceptable passwords at random, if possible, or to select one that is not related to their personal identity, history or environment.

3.4.5 (*) Passwords selected or created by users or the Security Officer shall be tested by the automated password system to assure that they meet the specifications of composition and length established for the ADP system before they are accepted as valid passwords.

3.5 Ownership

3.5.1 Personal passwords used to authenticate identity shall be owned (i.e., known) only by the individual having that identity.

3.5.2 Access passwords used to protect private data shall be owned (i.e., known) only by the individual who created the private data.

3.5.3 Access passwords used to protect shared data shall be owned (i.e., known) only by the set of individuals authorized the same access privileges to that data.

3.5.4 The personal password of any individual who is authorized access to shared data, and the access password of that shared data shall not be intentionally selected or set to be identical.

3.5.5 Bach individual shall be responsible for providing protection against loss or disclosure to passwords in their possession.

3.6 Distribution

3.6. 1 Personal passwords shall be distributed from the password source in a way that only the intended owner may see or obtain the password.

3.6.2 Passwords shall be distributed in a way that an audit record, containing the date and time of a password change and the identifier associated with the password (but not the old or new password), can be made available to the Security Officer.

3.6.3 Passwords shall be distributed from the password source in such

a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner(s) and the protected password system.

3.6.4 (*) An automated password system that generates and distributes passwords shall keep an automated record of the date and time of password generation and to whom it was distributed (but not the password itself).

3.7 Storage

3.7.1 (*) Stored passwords shall be protected in such a way that only the password system is authorized access to a password.

3.7.2 (*) Passwords that are encrypted before they are stored shall be protected from substitution (i.e., protection shall be provided such that one encrypted password cannot be replaced with another unless the replacement is authorized).

3.8 Entry

3.8.1 Passwords shall be entered by the owner when requested by the password system in a manner that protects the password from disclosure to anyone observing the entry process.

3.8.2 The number of allowed password entry attempts (retries after incorrect password entry) shall be limited to a number selected by the Security Officer.

3.8.3 The response to exceeding the maximum number of retries shall be specified by the Security Officer.

3.9 Transmission

3.9. 1 Passwords that are transmitted between the place of entry and the place that the entered password is compared with the stored password shall be protected to the degree specified by the Security Officer and at least equivalent to the protection required for the entity (ADP system or data) that the password is

protecting.

3.9.2 (*) Passwords transmitted between the place of entry and the place of comparison with the stored password shall be encrypted at the place of entry if the data that the password is protecting are encrypted at the place of data entry.

3.9.3 (*) Passwords that are used as encryption keys shall be selected at random from the set of all possible keys (e.g., 236 keys for the DES) and shall be used either as Data Encrypting Keys or Key Encrypting Keys, but not both.

3.9.4 (*) Unencrypted passwords shall be transmitted as ASCII characters if interchanged between ADP systems; encrypted passwords and virtual passwords shall be transmitted either as a 64-bit binary field in bit-oriented communications, or as ASCII representations of the hexadecimal character set (i.e., the 16 characters in the set [0-9, A-F] in character-oriented communications).

3.10 Authentication Period

3.10.1 (*) Personal Passwords shall be authenticated each time a claim of identity is made, e.g., when "logging onto" an interactive system.

3.10.2 (*) Access passwords shall be authenticated during the initial request for access to protected data.

APPENDIX A

PASSWORD USAGE GUIDELINES

1. Introduction

This appendix contains background information, a discussion of the factors specified in the Password Usage Standard (herein called the Standard) and the rationale for the minimum criteria specified in the Standard. It also provides guidance in selecting parameters of password systems based on increasing security requirements. Examples of three password systems meeting increasing levels of security requirements are included.

2. Background

Passwords are the most common method of personal identification used in conjunction with remote terminals to deter unauthorized access to computer systems and networks. The effectiveness of passwords has often been questioned, primarily because they can be easily forgotten or given to another person. However, passwords can provide reasonable deterrence to unauthorized access if properly handled by people authorized to use them and if properly stored and processed in the password verification system. Within its Computer Security and Risk Management Program, the Institute for Computer

Sciences and Technology of the National Bureau of Standards developed this Standard for secure password usage to assure reasonable handling, storage and processing of passwords. This Standard is one in a series of Standards and Guidelines issued by NEBS in the field of Computer Security. Another in this series, Federal Information Processing Standards Publication (FIPS PUB) 48, Guidelines on Evaluation of Techniques for Automated Personal Identification, describes various techniques for verifying identity and provides a set of criteria for the evaluation of automated identification systems embodying these techniques.

Shortly after issuing FIPS PUB 48, NEBS published Special Publication 500-9, The Use of Passwords for Controlled Access to Computer Resources. This publication considered the generation of passwords and their effective application to the problem of controlling access to computer resources. Following analysis and use of this document, a project was initiated to establish a fundamental performance standard for the use of passwords and a guideline on how to use this Standard to achieve the degree of protection that passwords were intended to provide.

The Password Usage Standard was developed within the Computer Security and Risk Management Program of the Institute for Computer Sciences and Technology with considerable assistance from representatives of Federal organizations and private industry. In 1980, NEBS developed and distributed a draft Password Usage Standard to government and industry representatives for comments and then held a workshop to discuss the benefits and impact of the draft Standard. The draft Standard identified 10 factors to be considered in the implementation of password systems and quantified security criteria in a hierarchical manner for each of the 10 factors. It also proposed five levels of security and specified minimum criteria for each level. The workshop participants felt that the 10 factors were useful in structuring the design of password systems, but that the proposed five levels were unworkable as a basis of a password Standard. As a result of the workshop recommendations, the Standard was revised to specify minimum criteria for the factors of a password system. An Appendix was drafted which provided guidelines for achieving higher levels of security. This revised Standard and the draft guidelines were published for public comment and for agency comment in July, 1981. The received comments were used in revising the proposed Standard and draft guidelines in preparing the published Standard and guidelines.

3. Factors

Ten factors of an automated password system are specified in the Standard. These factors constitute the fundamental elements which

must be considered, specified and controlled when designing and operating a password system. The rationale for the factors and for the minimum acceptable criteria for the factors specified

in the Standard are provided in the following discussion. Guidance on how to meet the minimum criteria and reasons for exceeding the minimum criteria are also provided.

3.1 Composition

A password is a sequence of characters obtained by a selection or generation process from a set of acceptable passwords. A good password system has a very large set of acceptable passwords in order to prevent an unauthorized person (or intruder) from determining a valid password in some way other than learning it from an authorized person (i.e., owner). The set of acceptable passwords should be large enough to assure protection against searching and testing threats to the password system (and hence the data or resources that it protects) commensurate with the value of the data or resources that are being protected. The set of acceptable passwords must be such that it can be specified easily, that acceptable passwords can be generated or selected easily, that a valid password can be remembered, can be stored reasonably, and can be entered easily. Composition is defined as the set of characters which may comprise a valid password.

The composition of a password depends in part on the device from which the password is going to be entered. It also depends on how and where the password is going to be stored and how the stored password will be compared with the entered password. Federal Information Processing Standards Publication 1-2 (FIPS PUB 1-2) incorporates the American Standard Code for Information Interchange (ASCII) which specifies a set of characters for interchanging information between computers. Federal Information Processing Standards Publication 1-2 (FIPS PUB 1-2) defines several proper subsets of this set to be used for special applications. The 95-character graphics subset specified in FIPS PUB 1-2 is the set from which the System Manager and Security Officer should select the acceptable composition for a particular system. While backspaces can be used effectively to mask printed passwords, several comments on the draft guidelines described the special use of backspace in many computer systems and recommended that it not be allowed.

The minimum composition contains 10 characters because some systems (e.g., financial transaction systems) use a 10-digit PIN PAD (Personal Identification Number entry device) for entering the password which is called a PIN. The PIN PAD looks very similar to the keyboard of a push button telephone. Some systems being developed use the push button telephone for data entry and retrieval. Users of these systems stated their desire to use the Standard. A better composition contains 16 characters which includes the 10 digits plus (A,B,C,D,E,F). This set can represent hexadecimal characters, each of which is a four-bit (binary digit) code. For example, 16 hexadecimal characters are used to represent a Data Encryption Standard key (see FIPS PUB 46) which can be used as a personal key in a cryptographic system. Many passwords are composed only of the 26 lower case letters (a-z) or the 26 upper case letters (A-Z). However, using either of these sets often encourages the selection of a person's initials, name, nickname, relative, hometown, or common word easily associated with the person. Even allowing all possible 4-letter, 5-letter or 6-letter English words greatly restricts the number of passwords when compared to all possible passwords of length range 4-6 with the same composition. Totally alphabetic password composition should be discouraged. The best password composition is the 95-character graphic set as specified in FIPS PUB 1-2 (see app. C).

3.2 Length

Length is closely associated with composition in assessing the potential security of a password system against an intruder willing to try exhaustively all possible passwords. The length of a password provides bounds on the potential security of a system. A length of exactly 1 reduces the potential number of valid passwords to the number of characters in the acceptable composition set. A length of 2 squares this number; a length of 3 cubes this number; a composition of 10 and a length of exactly 4 provides for 10^4 (read 10 raised to the fourth power) or 10,000 possible passwords. PINs are typically four digits because of low security requirements, for ease of remembering by a large customer base and for speed and accuracy of entry. A PIN verification system generally prevents a person from quickly trying all 10,000 possible PIN's for a particular valid financial account in order to find the valid PIN. If the trial and error process can be automated, even on a small home computer, the valid PIN can be found in a few minutes. Having a length range of 4-6 increases the possible number of PIN's to 1,110,000 ($10^6+10^5+10^4$).

If all other factors are temporarily ignored, the security provided by a password is directly proportional to the allowed length of the password. In other words, longer passwords are more

secure. However, other factors cannot be ignored in practical password systems. Long passwords take longer to enter, have more

chance of error when being entered, and are generally more difficult to remember (the latter may not be true unless the password consists of random characters). Sixteen random hexadecimal characters are very difficult to remember and are very difficult to enter quickly and accurately. For this reason, DES keys are usually not personal passwords and vice versa. However, long passphrases can be transformed to virtual passwords of exactly 64 bits (or 56 bits with the other 8 bits recomputed to be parity bits). Long passphrases can be easy to remember but still take longer to enter.

The length range should include a number of lengths, probably from 5-8 characters, and the composition should be a large set so that a high level of security can be provided easily.

A passphrase is an understandable sequence of words (sentence, sentence segment, phrase) that can be transformed and stored as 64 bits, and which is used as a password. A passphrase is generally easy to remember by the owner of the passphrase, and hence is allowed on some systems because of this characteristic. Since the number of distinct possibilities of understandable passphrases is considerably smaller than for a random sequence of characters of the same length, a longer passphrase is preferable to a shorter one. For example, the number of understandable 64-character long passphrases composed using the 27-character set A-Z and space, is considerably less than 27^{64}, which is the number of possibilities if the characters are selected randomly.

A passphrase may be used that is equivalent to a password as specified in the Standard. A passphrase may be transformed into a virtual password by using a transformation such as a hashing function or a cryptographic function. These functions should compute a value using the entire passphrase as input such that any change in the passphrase should result in a different computed value (within some probability). The value that is computed is the virtual password and must be 64 bits as specified in the Standard. This allows all password systems to allocate a maximum of 64 bits for storing each password, and therefore allows up to 2^{64} possible passwords (many thousands of years of security against exhaustive searching attacks). Such a passphrase thus provides the benefits of being easily remembered at the added cost of additional time to enter the longer passphrase and the time needed to compute the

virtual password. The Data Encryption Standard (FIPS PUB 46) and the cipher block chaining mode specified in the DES Modes of Operation Standard (FIPS PUB 81) are suggested as the transformation (see app. D).

3.3 Lifetime

The security provided by a password depends on its composition, its length, and its protection from disclosure and substitution. The risk associated with an undetected compromise of a password can be minimized by frequent change. If a password has been compromised in some way and if a new password is created that is totally independent of the old password, then the continued risk associated with the old password is reduced to zero. Passwords thus should be changed on a periodic basis and must be changed whenever their compromise is suspected or confirmed.

The useful lifetime of a password depends on several variables, including:

- The cost of replacing a password;
- The risk associated with compromise;
- The risk associated with distribution;
- The probability of "guessing" a password;
- The number of times the password has been used;
- The work of finding a password using exhaustive trial and error methods.

Password systems should have the capability of replacing the password quickly, initiated either by the user or the Security Officer. Passwords should be changed voluntarily by the owner whenever compromise is suspected and should be changed periodically with a maximum interval selected by the Security Officer. The interval may be a period of time or depend on a number of uses. The password system itself should have automated features which enforce the change schedule and all the security criteria for the installation. The system should check that the new password is not the same as the previous password. Very sensitive applications may require that a new password not be the same as any of the previous two, three, ..., N passwords. Such

a system requires storage for N passwords for each user. It should not be a requirement of a system that the password for each user be unique. Having a new password rejected for this reason confirms that another user has the password.

3.4 Source

Passwords should be selected at random from the acceptable set of passwords by either the owner or the password generator. However, this guidance may not be possible in all cases and may not be desirable in some cases. The Security Officer often selects a password for a new user of a system. This can be used for the first access to the system. The system may then require that the user replace this password which the Security Officer may know with a password that only the user knows. Passwords that are created or selected by a user should be checked by the automated password system as meeting all of the criteria of the password system. Passwords that do not meet all the criteria should b(' rejected by the automated password system. A record that an attempt to select an unacceptable password may be made by some automated systems but is not required by the Standard.

If passwords are generated by the system, the method of generation should not be predictable. Commonly used random number generators that are available. in computer systems for statistical purposes should be avoided because the sequence of random numbers that they generate are predictable. The DES algorithm, together with a non-deterministic parameter such as the least significant bits of a high resolution computer system clock may be used. The results of a random generator are then combined with password selection rules to obtain a password which meets mandatory and desirable criteria.

3.5 Ownership

A personal password should be individually owned rather than owned in common by a group of individuals in order to provide individual accountability within a computer system. This is desirable even though a group of people all have common access privileges to the same resources or data. Individual ownership of

personal passwords is required because:

- It can establish individual accountability for the determination of who accessed what resources and for what purposes.

- It can establish illicit use of a password or loss of a password.

- It can be used for an audit trail of the activities of a user.

- It avoids the need to change the password of an entire group when a single member of the group leaves or loses authorization privileges.

3.6 Distribution

A password must be transported from the owner to the authentication system if selected by a user, from the authentication system to the owner if generated by the password system or from the Security Officer to both the owner and the authentication system if generated by the Security Officer. The initial password is often distributed in a different manner than subsequent replacement passwords. The initial password is generally created and issued directly, either orally or in writing, Curing the meeting at which a user is initially authorized use of the computer system or access to a set of data. This may be a one-time password which must be changed after the initial access request is granted. Changing of a password by a user generally requires that the user supply the old password and then the replacement password. The replacement is checked for meeting the security requirements of the system, checked that it is different than the old password, and then entered into the storage location of the old password. An audit record should be made of the replacement, containing the date and time of the change, but not the new password Forgotten passwords should be replaced and a new password issued in a manner similar to, if not identical with, issuance of the initial password.

Passwords that are distributed in writing should be contained in a sealed envelope marked "To be opened by addressee only." Delivery may be by courier, internal 'nail, or by U.S. Mail. Instructions to the user should be to:

-Destroy the written password after memorizing it; or

-Return the written password to the Security Officer after signing the receipt for the password and after sealing it in the return mailer.

-Use the password as soon as possible and, if the password can be changed by the user, change the password.

Some systems distribute passwords in a sealed mailer that has been printed by a computer. The mailer is designed so that it cannot be resealed once it is open. The password is printed only on the inside of the mailer on the second page using carbon paper attached to the back of the mailer's front page. The instructions say to remove the front of the mailer, which shows the name of, 'the intended recipient, to destroy the front and save the password (in a protected place readily accessible only to the intended recipient). The part of the mailer that has the password has no other identification which would associate the password with either the system or the owner. Thus, anyone finding a lost password would usually not be able to use it. While not as desirable as memorizing the password and destroying the distribution medium, this system is useful when passwords are not routinely used and would be written in a location which-is more easily associated with the owner.

When distributed by a secure mailer, a receipt for the password may be validated by positive response or on an exception basis. When password distribution is done on an unscheduled basis, a positive response,is required. When passwords are distributed regularly, the user should be expecting a new password and should report any failure to obtain a new password. In either case, a record must be kept of the fact that a new password was issued.

There may be a transition period in which it is uncertain if the old password is valid or if the new password is valid. Some systems may allow either password to be valid during the transition period. This means that both passwords must be stored and compared with an entered password. Some systems may have no transition period (e.g., a password becomes valid at 8:06 P.M. exactly) and record attempts at using the old password in an audit file. A report of such attempts should be sent securely to the password owner as notification that usage of an old password was attempted. The owner can verify that the use was an

accidental rather than an unauthorized use of an old password by an intruder.

3.7 Storage

Passwords should be stored in the authentication system in a manner which minimizes their exposure to disclosure or unauthorized replacement. Several methods have been used to protect passwords in storage. Most systems have a password file that can be legitimately read only by the "LOGON" program. The file is protected by a file access mechanism which checks a protection bit in a file access table. Only the privileged LOGON program has access to read the file and only (:he password program has access to write the file. Some systems separate the password file from the authorized user file. An index file is used to provide the correspondence between the user and the user's password. Some systems encrypt the passwords, either reversibly (two-way) or irreversibly (one-way) using a Data Ecrypting Key (DEK) or the password itself as a key. Of course, any key (e.g., a Data Encrypting Key) retained in storage would also need protection by encryption using a Key Encrypting Key (KEK). The type of 'protection provided to the passwords should be commensurate with the protection desired for the system or data and hence a protection system should be used to provide the desired protection.

One-way encryption of passwords is allowed in the Standard when encryption is used for stored password protection. One-way encryption systems transform the password in such a way that the original password can not be recovered. This protects the original password from everyone, including the Security Officer and the systems programmers. When a user is logging onto such a system, the password that is entered by the user is one-way encrypted and compared in encrypted form with the stored encrypted password. The same encryption method and key must be used to encrypt the valid password before storage and to encrypt the entered password before comparison.

Two-way encryption of passwords is also allowed in the Standard. Given the correct key, the original password may be determined from the encrypted password. A user entered password

may be compared with the decrypted stored password (which was encrypted), or the user's password may be encrypted and compared with the stored password as is done with one way encrypted passwords.

3.8 Entry

Entry of a password into an automated authentication system in a secure manner is often a difficult task. An observer often is able to detect part or all of a password while the user is entering the password. Typing keyboards are the typical entry device. A user that is not a trained typist often enters the password with one finger. A long, random password that is difficult to enter may be more vulnerable to observation than a short easily entered password. The Standard specifies that a password shall be entered by a user in such a manner that the password will not be revealed to anyone observing the entry process. The following discussion provides some techniques which the user may find useful in achieving this goal and which the computer systems operation staff may find useful in assisting the user.

The computer terminal, keyboard, push-buttons, or password entry device should provide a means for minimizing the exposure of the password during entry. The password should not be printed on the terminal during the entry process. If the keyboard and the terminal display or printer are directly coupled, then the password should be masked by obliterating (understriking) the space where the password is going to be printed. The password may be masked further by overstriking the area after password entry. Computer generated masks used during password entry to disguise the entered password should not always be the same. In any case no printed or displayed copy of the password should exist after password entry.

CRT terminals which use half-duplex communications may present a problem because the password overwrites the understriking and remains visible on the display. The display should be immediately cleared by the password entry program after password entry in such systems. Users should be instructed to manually clear the display following password entry if the screen cannot be cleared by the password entry program.

When submitted as a part of a remote entry batch processing request, the password should be added to the request at the last possible moment and physically protected. Batch processing requests submitted in punched cards should have the password card added by the user just prior to submission. The computer operations staff should maintain the card decks in a protected

area and should remove and destroy the password card after the deck has been read by the system. The password should never be printed on any output media. One-time passwords that are distributed to the owner in the form of a password list and sequentially used for sequential batch processing requests may be used. The Standard requires that such lists be physically protected by the owner.

Users should be allowed more than one attempt to enter a password correctly in order to allow for inadvertent errors. However, there should be a maximum number of trials allowed for a password to be entered correctly. A maximum of three (3) attempts is considered adequate for typical users of a computer system. The system should also prevent rapid retries when a password is entered incorrectly. Several seconds should elapse before another password is requested. This prevents an automated, high speed, trial-and-error attack on the password system. A security record should be maintained of the fact that incorrect passwords were entered but the incorrect password should not be kept in the record. A security alarm should be generated if:

1. The maximum number of allowed password retries is exceeded;

2. The maximum number of allowed failed logons from one terminal is exceeded;

3. The maximum number of allowed failed logons for a time period is exceeded.

These parameters must be set according to the sensitivity of the data being protected, the profile of the typical system user and the policy of the organization. Some organizations will be willing to set the parameters high to prevent customer dissatisfaction while other organizations will set the parameters low to prevent security compromises. Terminals should be disabled and users should be denied service if these parameters are exceeded. The Security Officer should be the only one who can enable the terminal and restore the service of the user following these events.

The system should inform the user, following a successful LOGON procedure, of the last successful access by the user and of any unsuccessful intervening access attempts. This will aid in uncovering any unauthorized accesses or attempted accesses which may have occurred between successful accesses. The user can do several actions to prevent an observer from learning the password by watching the password entry process. First, entry of the password can be practiced so that it can be quickly entered using several fingers. Second, the body can be used to prevent the observer from seeing the keys being pressed during password entry. Third, the user can request that a guest not watch the password entry process. Fourth, the user can perform the password entry prior to demonstrating use of the system.

3.9 Transmission

Passwords are typically used to authenticate the identity of a user attempting to gain access to a shared computer system or network from a terminal. In order to be authenticated, the password is typically transmitted from the terminal to the computer via the communication line between the terminal and the computer. Unless the communication line is physically protected or encrypted, the password is vulnerable to disclosure. Most communication lines between terminals and computers are not afforded this protection at present. Therefore, users should be aware that their passwords can very easily be disclosed via passive wiretapping.

Computer systems can also be easily spoofed. This can occur if an intruder has inserted an active wiretap between a terminal and the computer. An active wiretap can be built today for several hundred dollars by a home computer hobbiest. The wiretap can be built into a briefcase and consists of a hobby computer with a receive/transmit communication chip which receives data from the terminal and computer and then retransmits data to the computer and terminal, having scanned and modified the data. The active wiretap can replace one user's password with another user's password, even if the passwords are encrypted at the terminal. Spoofing occurs when the system is fooled into "believing" one user is at the terminal when another user is actually there. Reverse spoofing occurs when a user is fooled into believing that communication is with the intended computer when another computer is there. In the latter case, an authorized user can be spoofed into providing the valid user's password by simulating the

"LOGON" request of the intended computer. After the password is obtained, the intruder that is controlling the spoofing computer informs the user that the requested service is temporarily unavailable. During this exchange the intruder has obtained a valid password without the user's knowledge.

These threats can be prevented by one of two encryption methods. First, the communication line between the terminal and the computer can be protected by encryption devices which use a secret key (e.g., a Data Encrypting Key) for encrypting all communication between the terminal and the computer. Transmitted passwords are thus protected from disclosure. In addition each transmission can be numbered so that a previous transmission cannot replace a later transmission (.i.e., a previously used valid password cannot be saved and used to replace an invalid password, even if both are encrypted). Passwords are thus protected to the same degree as the data as specified in the Standard.

Alternatively, the password can be used as the encryption key or as part of the encryption key. Suppose a user enters a password to be used as an encryption key at the terminal (i.e., never transmitted to the computer) and the user's password is retrieved from the computer's memory and used as the encryption key at the computer (i.e., never transmitted to the terminal). Then the terminal and the computer are mutually authenticated if normal communication can occur using the encryption and decryption processes at the terminal and computer, both using the password as the key (or a part of the key). This alternative is also allowed in the Standard.

In order to prevent compromise of the level of security provided by the cryptographic mechanism, the Standard specifies that personal passwords that are used as keys as described above be selected at random from the set of all possible encryption keys used by the cryptographic process. It also specifies that passwords that are used as Data Encrypting Keys should not also be used as Key Encrypting Keys, and vice versa. This is to minimize any possibility of attempting to recover the key (and hence the password) through cryptanalytic techniques.

3.10 Authentication Period

Interactive "sessions" between a user and a computer via a remote terminal often last several hours. While security policy should state that a terminal that is "logged onto" a computer should never be left unattended

by the user that is "logged onto" the computer, in practice this often occurs. Many systems have a feature which automatically logs a user off the system if the terminal has been inactive for some period of time. This is to prevent someone who encounters an unattended terminal from using it. Some access control systems require that a user be reauthenticated on a periodic basis in addition to the initial authentication process. These systems often antagonize the user if the authentication frequency is set too high. The message that the authentication process must be performed again often comes in the middle of the work that a user is performing. If this work happens to be a large printout of final text of a paper to be published, the user is rightfully upset. For this reason the Standard did not specify a minimum reauthentication period. Reauthentication should only be required to satisfy high security requirements, and then only requested if the terminal has been inactive for a period of time. This should prevent the authentication process from occurring in the middle of some important work.

4. Examples of Password Systems

The following examples of password systems which satisfy various security requirements are provided as assistance to Security Officers and System Managers. Determination of the parameters for each of the 10 factors discussed above will permit the preparation of the Password Standard Compliance Document. These examples should not be considered as the only selection of the parameters for the 10 password system factors.

4.1 Password System for Low Protection Requirements

A hypothetical password system might have the following parameters for the 10 factors which will both satisfy the Standard and satisfy requirements for protection which are considered to be minimal. The example is similar to that found in many retail, customer initiated financial transaction systems in which the maximum liability of the customer is $50 and the

maximum liability of the bank is limited by the number of transactions allowed per day. This example is also typical of many government-owned, government-leased computer systems in which no sensitive applications are performed. Small scientific systems, special purpose systems and systems not making critical automated decisions may fall in this category. Systems which have limited financial liability and those which require only accountability and control of computer usage and costs may also be considered in this category.

1. Length Range: 4-6
2. Composition: Digits (0-9)
3. Lifetime: l year
4. Source: User
5. Ownership: Individual (personal password); group (access passwords)
6. Distribution: Unmarked envelope in U.S. Mail
7. Storage: Central computer on-line storage as plaintext
8. Entry: Non-printing "PIN-PAD"
9. Transmission: Plaintext
10. Authentication Period: Each transaction

4.2 Password System for Medium Protection Requirements

Government systems which process limited "sensitive" applications may fall in this category. These are applications which process data leading to or directly related to monetary payments or process data subject to the Privacy Act of 1974. Agency management may determine that additional applications should be designated as sensitive. Computer systems that are subject to fraud, theft, erroneous payments or other loss of sensitive information may also fall into this category. Government systems which make payments (e.g., Social Security, Treasury), keep inventories (e.g., Armed Forces), and process personal information (e.g., Internal Revenue

Service, Department of Education) would be examples of systems which would have requirements of this
nature and probably would be satisfied by this type of password

system.

1. Length Range: 4-8
2. Composition: U.C. Letters (A-Z), L.C. Letters (a-z), and digits (0-9)
3. Lifetime: 6 months
4. Source: System generated and user selected
5. Ownership: Individual
6. Distribution: Terminal and special mailer
7. Storage: Encrypted passwords
8. Entry: Non-printing keyboard and masked-printing keyboard
9. Transmission: Cleartext
10. Authentication Period: Login and after 10 minutes of terminal inactivity.

4.3 Password System for High Protection Requirements

Computer systems which process information of a sensitive nature and which rely on passwords to provide personal identification may have high protection requirements that could be satisfied by a password system for personal identification having these characteristics.

Systems having high protection requirement's may include those which have unusually high potential for fraud or theft, have a high economic benefit to a system intruder, and have a substantial impact on safety or the well being of the society. Some computer systems of the Department of Defense or the Federal Reserve Communication System may fall into this category. Systems having very high security requirements may require methods of personal identification which are based on physical characteristics of a person (signature, voice, fingerprint) or on a combination of something unique that the person has (e.g., badge, ID card) and something unique that the person knows (i.e., a password). A risk analysis should be performed for each government owned or leased computer system to determine its security requirements and then a personal identification system should be selected which best satisfies these requirements.

1. Length Range: 6-8
2. Composition: Full 95 character set
3. Lifetime: One month
4. Source: Automated password generator within the authentication system
5. Ownership: Individual

6. Distribution: Registered mall, receipt required; personal delivery, affidavit required
7. Storage: Encrypted passwords
8. Entry: Non-printing keyboards
9. Transmission: Encrypted communication with message numbering
10. Authentication Period: Login and after 5 minutes of terminal inactivity.

APPENDIX B

EXAMPLES OF COMPLIANCE AND PROCUREMENT DOCUMENTS

1. Example of a Minimum Security Compliance Document

ORGANIZATION: XYZ Agency
TYPE OF SYSTEM: Inventory
PREPARING OFFICIAL: Samual V. Jones
DATE: 14 February 1986

JUSTIFICATION:
Analysis of the security requirements for the inventory system to be used by this agency indicates the desirability of implementing a password authentication system. It was further determined that a minimum compliance with the Federal Information Processing Password Usage Standard would fulfill the security needs of this system. Accordingly, the following criteria have been selected for the 10 basic factors specified in the Standard.

1. Length Range: 4-6
Rationale: A minimum level of security for the data is required.

2. Composition: Digits (0-9)
Rationale: Personnel are accustomed to PINs for their financial transactions and to combination locks. A numeric keypad is used.

3. Lifetime: One year
Rationale: The maximum password lifetime is more than

adequate for this system.

4. Source: User Rationale: Users desire to select passwords which are easy to remember, but will be instructed to select random passwords rather than those having particular significance to them.

5. Ownership: Individual (personal passwords); group (access passwords)
Rationale: The Standard requires individual ownership of personal passwords. The group password is used for access control for this minimum level security system.

6. Distribution: Initial password given to any current authorized user to enter; subsequent passwords from a terminal following access authorization
Rationale: All personnel authorized to use the system can receive passwords from the Security Officer.

7. Storage: Central computer on-line storage as plaintext
Rationale: Data is not highly sensitive.
8. Entry: Non-printing keypads
Rationale: Inexpensive and available.

9. Transmission: Plaintext
Rationale: All data is contained in one building.

10. Authentication Period: Login
Rationale: Minimum security requirements.

2. Example of a Procurement Specification for a Minimum Security Password System

The operating system shall include a password system which includes the following features as a minimum.

(a) A password length range of 4-6 characters; characters to be selected from the digits 0-9.
(b) Passwords are to be selected by the users. Individual authorized users must have the capability of entering new users onto the system and deleting current users from the system. All interactions with the password system will be via video terminals.

(c) Passwords stored in the system may be stone as plaintext.
(d) User authentication shall be performed during the login process.

3. Example of a Medium Security Compliance Document

ORGANIZATION: Department of Secrecy
TYPE OF SYSTEM: Personnel Records
PREPARING OFFICIAL: Constance Johns
DATE: 7 July 1985

JUSTIFICATION:
The computer system containing the Department's personnel records currently uses passwords to authenticate an individual's identity for access to the system. A security analysis has determined that a level of protection greater than the minimum level of protection specified in the Federal Information Processing Password Usage Standard is required for this system. The following criteria have been selected as adequate to meet our requirements, and are hereby submitted for approval.

1. Length Range: 48
   Rationale: This allows a wide range of passwords from which to select.

2. Composition: (A-Z), (a-z) and (0-9)
   Rationale: Ease of password creation and remembering. Together with the length, this allows for selection of $62^8+62^7+62^6+62^5+62^4$ possible passwords if characters are selected randomly.

3. Lifetime: 6 months
   Rationale: Analyzed sensitivity of the data.

4. Source: Automatic password generator within the system. The user may refuse generated pass-words and request that another be generated.
   Rational: To eliminate the possibility that users will select passwords significant to them and easily guessed by others.

5. Ownership: Individual
   Rationale: Bach person is to be individually authenticated.

6. Distribution: Initial password from Security Officer access mailer; subsequent passwords from a terminal following access authorization
Rationale: All entry and retrieval is performed using video terminals.

7. Storage: Encrypted passwords with access only by the password system
Rationale: Sensitivity of the data. Passwords are used as the encryption keys to encrypt the identifiers, and the result is stored at the central system.

8. Entry: Video terminals, non-printing
Rationale: All entry and retrieval operations are performed at these terminals. Passwords are not displayed on the terminal during entry.

9. Transmission: Cleartext communications
Rationale: While personnel data is sensitive, it is not necessary to encrypt the data during communication within the facility.

10. Authentication Period: Login and after 10 minutes of terminal inactivity.
Rationale: Wish to avoid having carelessly vacated terminals used by unauthorized individuals.

4. Example of a Procurement Specification of a Medium Security Password System

The operating system shall contain a password system which will authenticate the identity of authorized users whose personal passwords are stored in the system. The password system shall consist of the following features at a minimum.

(a) Passwords shall be composed of the characters A-Z, a-z, and 0-9. The system shall verify that only these legal characters are used in passwords.

(b) The length of a password shall be from 4 to 8 characters. The system shall not allow passwords to be selected outside this range, and shall requery for a valid entry.

(c) The system shall maintain a record of the date of password creation and last password modification, and shall enforce a password update at a time interval entered during SYSGEN.

(d) Passwords shall be generated by an automatic password generation program in the system whose algorithm has been approved by this Agency. Users shall have the capability of refusing any generated password and requesting another to be generated. The system shall not allow further system activity by a user until a new password has been selected.

(e) The initial password for a user shall be entered by a Security Officer after entering a special Security Officer password. Thereafter, passwords are to be changed by users after successful access authorization. A record shall be maintained of the date and time of password assignment/modification along with the identity of the individual with whom the password is associated. However, no record shall exist of the plaintext password selected.

(f) Passwords are to be stored in encrypted form, and this information shall only be accessible by the password system. Personal passwords shall be stored along with the identifier of the user owning the password. These passwords shall be encrypted by using the plaintext password as a key to encrypt the identifier using DES in the ECB mode.

(g) Entry of passwords shall be performed using video terminals. Entered passwords shall not be visible on the terminal. A maximum of three entry attempts shall be allowed. A time delay of at least 15 seconds shall be enforced before another set of three entry attempts may be made. A record shall be made of unsuccessful entry attempts. After three sets of unsuccessful attempts within a 5-minute interval, a message shall be displayed on the system operator's console and a bell shall be continuously sounded until the message is acknowledged.

(h) Transmissions to remote terminals shall be cleartext. Messages to remote terminals shall include message

sequence numbers.

(i) User authentication shall be requested during login and after 10 minutes of terminal inactivity. Service shall be denied when the correct passwords are not entered.

APPENDIX D

PASSWORD ENCRYPTION AND PASSPHRASE TRANSFORMATION

The FORTRAN program provided herein is a suggested method for password encryption and passphrase transformation. The program transforms a user identifier (USER-ID) and a user password (4-8 characters) or passphrase (9-64 characters) into 64-bit values for subsequent encryption. This capability was suggested by several people in comments to NBS on the Password Usage Standard. Limited experience has indicated that passphrases (greater than eight characters) are easier to remember and enter than passwords consisting of any combination of eight characters from the 95 character set suggested in the Standard. The method provided in this appendix is cryptographic algorithm independent, although 64-bit vectors are used. Key consists of 56 significant bits plus eight bits of parity. Input and output are each 64 bits in length.

The program allows the entry of passwords consisting of all characters from the 95 character set. Acceptable entries include passwords (4-8 characters), passphrases (9-64 characters), the equivalent eight character virtual password, or the equivalent 16 hexadecimal digit pass key. The last two are printed whenever a passphrase is entered. User IDs up to 64 characters long may also be entered. However, the transformed virtual value for the user ID is not (normally) printed. User IDs and passwords which are entered and are not a multiple of eight characters in length are padded with spaces.

A virtual password or user ID is calculated whenever a value greater than 8 characters in length is entered and (for passwords only) which does not consist of precisely 16 hexadecimal characters. The virtual value is produced by CBC encryption using the first eight bytes as key, and subsequent 8-byte blocks as input to the CBC algorithm. The virtual value is selected in 7-bit groups from the final output of this operation. These 7 bits are

stored in the right-most bits of a byte, and the left-most bit is set to zero. Seven bit values which are not represented in the 95-character set result in discarding the left-most bit and adding the next bit from the final output value of the encryption operation. If all bits from this final output value are used before a complete
8-byte virtual password or user ID has been calculated, the output value is again processed by the encryption

operation to produce an additional 64 bits from which to complete the virtual password or user ID calculation. The value which is ultimately stored as the encrypted password is produced by encrypting the user ID (or virtual user ID) by a key which is the exclusive OR of the password (or virtual password) and a system key. The system key may be set to 0 for system independent operation (i.e., for intercommunication between systems).


```
C     PASSWORD ENCRYPTION AND PASSPHASE TRANSFORMATION DEMONSTRATION PROGRAM.
      FC   VERSION 1.2
C     THIS PROGRAM WAS PRODUCED BY THE COMPUTER INTEGRITY AND SECURITY STAFF,
C     INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY
C     TECHNOLOGY A-216
C     NATIONAL BUREAU OF STANDARDS
C     GAITHERSBURG, MARYLAND 20899
C     (301)921-3427
C
C
C     THE PROGRAM 15 DESIGNED TO COMBINE A USER'S
C     IDENTIFIER WITH THE ASSOCIATED PASSWORD 50 THAT THE RESULT CAN NEVER BE
C     DIVIDED OR DECIPHERED.  THE RESULT IS AN ENCRYPTED PASSWORD
C     WHICH CAN BE COMPARED WITH A PREVIOUSLY ENCRYPTED AND
C     STORED PASSWORD.  THE DESIGN GOALS INCLUDE HAVING A SYSTEM FOR
C     ENCRYPTING PASSWORDS THAT DOES NOT USE A STORED CRYPTOGRAPHIC KEY.
C     SUCH SYSTEMS CAN EASILY PASS AN ENCRYPTED PASSWORD TO ANOTHER COMPUTER
C     SYSTEM FOR VALIDATION.  FOR SYSTEMS THAT DO NOT WISH TO USE ANOTHER
C     COMPUTER TO VALIDATE PASSWORDS OR TO INTERCHANGE PASSWORDS, A SYSTEM
C     KEY VARIABLE IS PROVIDED WHICH SHOULD BE RANDOMLY SET FOR EACH SYSTEM.
C     THE SYSTEM KEY SHOULD BE SET TO ZERO FOR INTERCHANGE AND A SECRET VALUE
C     FOR NO INTERCHANGE.  IDENTICAL TRANSFORMATIONS ARE USED FOR THE
C     USER-ID AND PASSPHRASE.
C
C
C     THE USER-ID AND THE PASSPHRASE CAN EACH CONTAIN UP TO 64 CHARACTERS.
C     PASSPHASES AND LONG USER-IDS (MORE THAN 8 CHARACTERS EACH)
C     ARE TRANSFORMED TO 64 BIT VALUES.  THE RESULTS, CALLED THE VIRTUAL
C     USER-ID AND VIRTUAL PASSWORD, ARE THEN USED TO PRODUCE AN ENCRYPTED
C     PASSWORD USING A ONE-WAY ENCRYPTION FUNCTION.
```

```
C
C     A USER-ID AND A PASSPHRASE (PASSWORD/PASS KEY) ARE ENTERED BY A
C     PERSON DESIRING USE OF A SYSTEM.  THE USER-ID AND PASSPHRASE ARE
C     TRANSFORMED. THE VIRTUAL PASSWORD IS USED AS A KEY TO ENCRYPT
C     THE VIRTUAL USER-ID AND THE RESULT IS COMPARED WITH THE STORED
C     VALUE FOR THE AUTHORIZED USER OF THE SYSTEM.
C
C     BOTH THE PASSWORD ENCRYPTION AND PASSPHASE TRANSFORMATION OPERATIONS
C     USE THE DATA ENCRYPTION STANDARD (DES) ALGORITHM, BUT ANY BLOCK
C     ENCIPHERING ALGORITHM CAN BE USED.
C
C     CALLS TRANSF, PARITY, CBC, HEXKEY, PACK, UNPBIN, DES AND SETKEY ROUTINES
C     DESCNT IS THE NUMBER OF TIMES TO ENCRYPT PASSWORD (ODD *).
      INTEGER DESCNT/5/
      INTEGER USERID(64) , PASSWD(64) . SYSKEY(8)
      INTEGER SPACE /' '/,IDLEN, PWLEN , HEXFLG
      INTEGER IDBIN(64) ,KEYBIN(64) , SYSBIN(64)
C     THE SYSTEM KEY SHOULD BE ALL ZEROS FOR INTERCHANGE WITH OTHER SYSTEMS.
C     FOR SYSTEMS THAT WILL NOT INTERCHANGE PASSWORDS WITH OTHER SYSTEMS,
C     THE SYSTEM KEY SHOULD BE SET TO RANDOM EVEN NUMBERS BETWEEN O AND 254
C     DECIMAL (INCLUSIVE) IN EACH OF THE EIGHT ENTRIES.  THIS IS THE EQUIVALENT
C     OF A DES KEY WITH THE RIGHT-MOST BIT OF EACH OCTET RESERVED FOR PARITY.
C     **NOTE:  THE FOLLOWING SHOULD BE CHANGED FOR EACH SYSTEM INSTALLATION.**
      DATA SYSKEY/120,98,46,76,22,2,254,128/
C     INITIALIZE USER-ID AND PASSPHRASE VECTORS
1     DO 4 1=1,64
      USERID( I) =0
4     PASSWD(I)-O

C     GET USER ID AND PASSPHRASE AND DETERMINE THEIR LENGTHS
5     WRITE(6,800)
800   FORMAT(//' ENTER USER ID: ')
      READ(S, 100) USERID
      CALL TSTVAL( 64 , USERID, IDLEN)
      IF(IDLEN.LE.0) STOP
```

```
C      FOLLOWING STATEMENT IS PROGRAM DEBUG STATEMENT
C      WRITE(6,500) (USERID(M),M=1,IDLEN)
500    FORMAT(' ASCII= ',8Z2.2)
10     WRITE(6,900)
900    FORMAT(' ENTER PASSWORD, PASSPHRASE OR 16-DIGIT HEX KEY ')
100    FORMAT(64A1)
       HEXFLG=0
       READ(s, 100)PASSWD
       CALL TSTVAL( 64, PASSWD, PWLEN)
       IF (PWLEN.LT.4) GO TO 10
C      CHECK FOR A PASSWORD ENTERED AS A HEXADECIMAL KEY IF (PWLEN. EQ. 16) CALL HEXKEY(PWLEN,
       PASSWD,HEXFLG)
C      PASSWORD MUST BE DIFFERENT THAN USER-ID; CHECK AND REPORT.
       IF (IDLEN.NE.PWLEN) GO TO 23 DO 22 I=1,IDLEN
                                 IF (PASSWD(I).NE.USERID(I)) GO TO 23
22               CONTINUE
                 WRITE(6,200)
200              FORMAT(' PASSWORD MUST NOT EQUAL THE USER ID')
                 GO TO 10
23     CONTINUE
C      FOLLOWING STATEMENT IS FOR PROGRAM DEBUG. WRITE(6.500) (PASSWD(M),M=1,PWLEN)
C      TRANSFORM LONG USER-ID INTO VIRTUAL USER-ID IF REQUIRED.
       IF (IDLEN .LE. 8) GO TO 43 CALL TRANSF( IDLEN , USERID)
C                FOLLOWING STATEMENT IS FOR PROGRAM DEBUG.
C                WRITE(6,650)(USERID(I),I=l,8)
650              FORMAT(' VIRTUAL USER ID IN 95 CHARACTER SET IS ',8A1)
43     CONTINUE
C      HEXFLG IS A 1 IF SIXTEEN HEX CHARACTERS WERE ENTERED.
C      SIXTEEN HEX CHARACTERS ARE USED AS A KEY, NOT A PASSPHRASE IF (HEXFLG .EQ. 1) GOTO 46
C      TRANSFORM PASSPHRASE INTO VIRTUAL PASSWORD IF MORE THAN
            8 CHARACTERS. IF (PWLEN .LE. 8) GO TO 44
                 CALL TRANSF(PWLEN, PASSWD)
                 WRITE(6,660) (PASSWD(I),I=1,8)
660              FORMAT(' VIRTUAL PASSWORD IN 95 CHARACTER SET IS ',8A1)
C                SHIFT EACH BYTE LEFT ONE BIT FOR DES PARITY BIT COMPUTATION
44          DO 45 1=1,8
                 PASSWD(I) = 2*PASSWD(I)
45          CONTINUE
                   IF (PWLEN .LE. 8)GO TO 46 WRITE(6,670) (PASSWD(I),I=1,8)
       670         FORMAT(' THE PASSWORD IN HEXADECIMAL IS ',8Z2.2)
       46    CONTINUE
       C     CALL SUBROUTINE TO UNPACK PASSWORD INTO BINARY VECTOR, ONE BIT PER WORD. CALL
             UNPBIN(8 ,8, PASSWD,KEYBIN)
       C     CALL SUBROUTINE TO UNPACK SYSTEM KEY MASK INTO BINARY VECTOR. CALL UNPBIN(8 ,8,
             SYSKEY, SYSBIN)
       C     EXCLUSIVE OR THE PASSWORD AND THE SYSTEM KEY TO MAKE AN ENCRYPTION KEY DO 24
             1=1,64
       24    KEYBIN(I)=MOD(KEYBIN(I)+SYSBIN(I),2)
       C     SET PARITY OF KEY CORRECTLY BEFORE USING
             CALL PARITY(KEYBIN)
       C     THE FOLLOWING TWO STATEMENTS MAY BE USED FOR PROGRAM DEBUG.
       C     CALL PACK(8,8,KEYBIN,PASSWD(9))
       C     WRITE(6,510) (PASSWD(M),M=9,16)
```

```
510  FORMAT(' THE KEY FOR PASSWORD ENCRYPTION IS: ',8Z2.2)
C    NOW LOAD THE KEY
     CALL SETKEY(KEYBIN)
C    UNPACK THE USER ID OR VIRTUAL ID INTO IDBIN FOR ENCRYPTION CALL UNPBIN(8,8
     ,USERID, IDBIN)
C    NOW CALL THE DES ROUTINE THE NUMBER OF TIMES SPECIFIED. DO 30 I=1,DESCNT
C    THIS CALLS THE DES ROUTINE AND ONE-WAY ENCRYPTS IDBIN INTO IDBIN.
```

```
30     CALL DES(0.IDBIN,IDBIN)
C      NOW PACK UP THE RESULTS OF THE ENCRYPTION INTO PASSWD. CALL PACK( 8,8, IDBIN,
       PASSWD)
C      ENCRYPTED  PASSWORD  NAY  NOW  BE  STORED  (PRINTED  FOR  DEMONSTRATION).  WRITE(6,300)
       (PASSWD(M),M-1,8)
C      Z FORMAT PRINTS HEXADECIMAL CHARACTERS.
300    FORMAT(' THE ENCRYPTED PASSWORD IS: ,8Z2.2)
       GO TO 1
       END



       SUBROUTINE TRANSF(LEN, STRING)
C      TRANSFORM A LONG STRING INTO A STRING OF 8 CHARACTERS INTEGER LEN,STRING(*),KEYBIN(64)
       ,TEMP(128), IV(64)

C      LOAD THE FIRST 8 BYTES AS KEY AFTER SHIFTING EACH BYTE LEFT,
C      UNPACKING AND COMPUTING ODD PARITY.
      DO 10 1-1,8
10     TEMP(I)-2*STRING(I)
       CALL UNPBIN( 8 , 8 , TEMP , KEYBIN)
       CALL PARITY(KEYBIN)
C      CALL PACK(8,8,KEYBIN,TEMP)
C      WRITE(6,500) (TEMP(M),M=1,8)
500    FORMAT(' THE KEY FOR THE VIRTUAL TRANSFORMATION IS: ',8Z2.2) CALL SETKEY(KEYBIN)

C      CBC ENCRYPT THE REST OF THE STRING
       DO 20 1=1,64
20     IV(I)=O
       CALL CBC(IV,LEN-8,STRING(9) STRING)

C      DETERMINE THE VIRTUAL ENTITY.  ACCEPT ONLY THE 95 LEGAL CHARACTERS C (32-126)
       CALL UNPBIN( 8 , 8, STRING, TEMP) J=1
       DO 50 1=1,8
C      GET ADDITIONAL BITS IF NECESSARY
30     IF(J.GE.59) CALL DES(0,TEMP,TEMP(65))
C      EXTRACT 7 ASCII BITS AND CHECK FOR VALIDITY
       CALL PACK(1,7,TEMP(J),STRING(I))
       IF((STRING(I).EQ.127).OR.(STRING(I).LT.32)) THEN
C     SHIFT TO NEXT 7-BIT SET IF ILLEGAL
       J=J+1
       GO TO 30
       ENDIF
C      OTHERWISE, SHIFT TO NEXT 7-BIT SET
50     J=J+7
       RETURN
       END



       SUBROUTINE CBC(IV,LEN, PLAIN,MAC)
C      COMPUTES A 64-BIT MAC ON PACKED PLAINTEXT (LENGTH-LEN)
C      LEN MUST BE A MULTIPLE OF 8 AND PLAIN MUST BE PADDED.
       INTEGER IV(64).LEN,PLAIN(*),MAC(8).INP(64).OUTP(64)
C      USE INITIAL VECTOR
```

```
 10       DO 10 1-1,64
          DO 30 I-1,LEN,8
          CALL UNPBIN(8,8,PLAIN(I) .INP)
          DO 20 J-1,64
 20       INP(J)-MOD(OUTP(J)+INP(J),2)
 30       CALL DES(0,INP,OUTP)
          CALL PACK(8,8,OUTP,MAC)
          RETURN
          END
```



```
          SUBROUTINE HEXKEY(PWLEN, STRING,HEXFLG)
C         CHECK WHETHER THE ENTERED STRING IS HEXADECIMAL WITH CORRECT PARITY
          TO SERVE AS A KEY
          INTEGER PWLEN, STRING( *) ,HEXFLG,TEMP(8) ,TEMPI(64)

C         TEST FOR HEXADECIMAL. RETURN IF NOT, ELSE CONVERT
          HEXFLG=0
          DO 5 1=1,8
 5        TEMP(I)=0
          DO 10 1=1,16

          TEMP(J)=16*TEMP(J)+STRING(I)
          IF((STRING(I).GE.48).AND.(STRING(I).LE.57)) THEN
                         TEMP(J)=TEMP(J)-48
                         ELSE IF((STRING(I).GE.65).AND.(STRING(I).LE.70)) THEN
                         TEMP(J)=TEMP(J)-55
                         ELSE IF((STRING(I).GE.97).AND.(STRING(I).LE.102)) THEN
                         TEMP(J)=TEMP(J)-'87
                         ELSE
                         RETURN
                         ENDIF
10        CONTINUE

          HEXFLG= 1
          PWLEN=8
          DO 30 I=1,8
 30       STRING(I)=TEMP(I)
          RETURN
          END


          SUBROUTINE TSTVAL( LEN, BUFFER, STATUS)
C         MASK CHARACTERS, CHECK FOR VALIDITY AND DETERMINE BUFFER LENGTH INTEGER
   LEN, BUFFER(*) , STATUS
          STATUS=0
          DO 10 I=LEN,1,-1
          BUFFER(I)=BUFFER(I)-(BUFFER(I)/128) *128
          IF((BUFFER(I).EQ.127).OR.(BUFFER(I).LT.32)) THEN
                         WRITE(6, 100) BUFFER(I)
100                      FORMAT(' UNACCEPTABLE ASCII CHARACTER: ,Z2.2)
                         DO 5 J=1,LEN
```

```
5                       BUFFER(J)='
                        STATUS=- 1
                        RETURN
                        ENDIF
          IF((STATUS.EQ.O).AND.(BUFFER(I).NE.32)) STATUS=I
10        CONTINUE
          RETURN
          END

          SUBROUTINE PACK(LEN, BPW, BINARY, PACKED)
C         SUBROUTINE TO PACK FROM BINARY VECTOR TO PACKED
C         VECTOR OF LENGTH LEN FILLING THE LEAST SIGNIFICANT BPW BITS. INTEGER
          BINARY( *) , PACKED( *)
          INTEGER LEN,BPW
          K=0
          DO 20 I=1,LEN
          ITEM=0
          DO 10 J=1,BPW
          K=K+1
10        ITEM=ITEM*2+MOD(BINARY(K) ,2)
20        PACKED(I)=ITEM
          END
```



```
          SUBROUTINE UNPBIN (LEN, BPW,PACKED, BINARY)
CO        SUBROUTINE TO UNPACK INTO BINARY VECTOR
CO        FROM PACKED VECTOR OF LENGTH N CONTAINING BPW BITS IN EACH WORD. INTEGER
         PACKED(*), BINARY(*)
          INTEGER LEN,BPW
          K=0
          DO 100 I=1,LEN
          ITEM=MOD(PACKED(I) ,2**BPW)
          DO 100 J-1,BPW
          IEX=2**(BPW-J)
          IBIT=ITEM/ IEX
          K-K+1
          BINARY(K)=IBIT
100       ITEM=ITEM-IBIT*IEX
          END


          SUBROUTINE PARITY (VECTOR)
C         COMPUTE ODD PARITY ON A 64-BIT UNPACKED VECTOR INTEGER VECTOR( 64)
          DO 10 1=8,64,8
          VECTOR(I)=1
          DO 10 J=1,7
10        VECTOR(I)=MOD(VECTOR(I)+VECTOR(I+J-8) ,2) RETURN
          END


C         PROGRAMS PRODUCED BY THE NATIONAL BUREAU OF STANDARDS
C         NOT SUPPORTED BY NBS AND NOT SUBJECT TO COPYRIGHT
C         SUBROUTINE TO PERFORM THE DATA ENCRYPTION STANDARD ALGORITHM SUBROUTINE
          DES ( SWITCH, INPUT , OUTPUT)
```

```
C          SWITCH = O CAUSES ENCRYPTION; SWITCH = 1 CAUSES DECRYPTION.
C          INPUT IS PLAINTEXT FOR ENCRYPTION, CIPHERTEXT FOR DECRYPTION.
C          OUTPUT IS CIPHERTEXT AFTER ENCRYPTION. PLAINTEXT AFTER DECRYPTION.

C          CALL DES(0,PT,CT) IS AN EXAMPLE OF CALL TO ENCRYPT PT INTO CT
C
C          CALL DES(1,CT,PT) IS AN EXAMPLE OF CALL TO DECRYPT CT INTO PT
C
C          THIS PROGRAM SHOULD NOT BE EXPORTED FROM THE UNITED STATES. IMPLICIT INTEGER (A-z)
           INTEGER INPUT(64) ,OUTPUT(64)
           INTEGER KS(48,16)
O          KS IS AN ARRAY TO HOLD THE 16 SUBKEYS FOR 16 ROUNDS OF DES
C          KS IS COMPUTED BY SETKEY SUBROUTINE WHICH MUST BE CALLED BEFORE
C          THE DES SUBROUTINE IS CALLED.  SETKEY IS CALLED ONCE TO SET THE
C          KEY AND THEN DOES NOT HAVE TO BE CALLED AGAIN UNTIL THE KEY IS
C          CHANGED.
C
           COMMON KS
           INTEGER LR(64),L(32),R(32)
           EQUIVALENCE (LR(1),L(1)), (LR(33),R(1))
           INTEGER TEMPL(32),EX(48),F(32)
C          IP IS THE INITIAL PERMUTATION FOR THE DATA INTEGER IP(64)/
          1 58,50,42,34,26,18,10,02.
          1 60,52,44.36.28.20.12,04,
          1 62,54,46,38,30,22,14,06,
          1 64,56,48,40,32,24,16,08,
          1 57,49,41,33,25,17,09,01,
          1 59,51,43,35,27,19,11,03,
          1 61,53,45,37,29,21,13,05,
          1 63,55,47,39,31,23,15,07/
```

```
C   IPINV IS THE INVERSE OF THE INITIAL PERMUTATION
C   INTEGER IPINV(64)/
C   1 40,08,48,16,56,24,64,32,
C   1 39,07,47,15,55,23,63,31,
C   1 38,06,46,14,54,22,62.30,
C   1 37,05,45,13,53,21,61,29,
C   1 36,04,44,12,52,20,60,28,
C   1 35,03,43,11,51,19,59,27,
C   1 34,02,42,10,50,18,58,26,
C   1 33,01,41,09,49,17,57,25/
C   NOTE:  THE REVERSED 1P INVERSE TABLE -REVIPI- IS USED BECAUSE
C   IT SAVES THE TIME OF REVERSING THE L AND R REGISTERS.
      INTEGER REVIPI (64)/
C   1 08,40,16,48,24,56,32,64,
     1 07,39,15,47,23,55,31,63,
    1 06,38,14,46,22,54,30,62,
    1 05,37,13,45,21,53,29,61,
    1 04,36,12,44,20,52,28,60,
    1 03,35,11,43,19,51,27,59,
    1 02,34,10,42,18,50,26,58,
    1 01,33,09,41,17,49,25,57/
C   E IS THE EXPANSION OPERATION WHICH EXPANDS 32 BITS TO 48 BITS
      INTEGER E(48)/
    1 32,01,02,03,04,05,
    1 04,05,06,07,08,09,
    1 08,09,10,11,12,13,
    1 12,13,14,15,16,17,
    1 16,17,18,19,20,21,
    1 20,21,22,23,24,25,
    1 24,25,26,27,28,29,
    1 28,29,30,31,32,01/
C   P IS THE PERMUTATION USED IN THE MAIN DES FUNCTION
      INTEGER P(32)/
    1 16,07,20,21,
    1 29,12,28,17,
    1 01,15,23,26,
    1 05,18,31,10,
    1 02,08,24,14,
    1 32,27,03,09,
    1 19,13,30,06,
    1 22,11,04,25/
C   THE EIGHT SUBSTITUTION TABLES ARE USED IN THE DES TO SUBSTITUTE 4 BITS
C    FOR SIX BITS.  ONE S TABLE IS USED FOR EACH 6 BIT TO 4 BIT TRANSFORMATION. INTEGER
     5(64,8)
      EQUIVALENCE (S(1,1),S1(1)), (S(1,2),S2(1))
      EQUIVALENCE (S(1,3),S3(1)), (S(1,4),S4(1))
      EQUIVALENCE (S(1,5),S5(1)), (S(1,6),S6(1))
      EQUIVALENCE (S(1,7),S7(1)), (S(1,8),S8(1))
      INTEGER SI(64)/
    1 14,04,13,01,02,15,11,08,03,10,06,12,05,09,00,07,
    1 00,15,07,04,14,02,13,01,10,06,12,11,09,05,03,08,
    1 04,01,14,08,13,06,02,11,15,12,09,07,03,10,05,00,
```

```
    1 15,12,08,02,04,09,01,07,05,11,03,14,1O,00,06,13/
      INTEGER S2(64)/
    1 15,01,08,14,06,11,03,04,09,07,02,13,12,00,05,10,
    1 03,13,04,07,15,02,08,14,12,00,01,10,06,09,11,05,
    1 00,14,07,11,10,04,13,01,05,08,12,06,09,03,02,15,
    1 13,08,10,01,03,15,04,02,11,06,07,12,00,05,14,09/
      INTEGER S3(64)/
    1 10,00,09,14,06,03,15,05,01,13,12,07,11,04,02,06,
    1 13,07,00,09,03,04,06,10,02,08,05,14,12,11,15,01,
    1 13,06,04,09,08,15,03,00,11,01,02,12,05,10,14,07,
    1 01,10,13,00,06,09,08,07,04,15,14,03,11,05,02,12/
```



```
          INTEGER S4(64)/
         1 07,13,14,03,00,06,09,10,01,02,08,05,11,12,04,15,
         1 13,08,11,05,06,15,00,03,04,07,02,12,01,10,14,09,
         1 10,06,09,00,12,11,07,13,15,01,03,14,05,02,08,04,
         1 03,15,00,06,10,01,13,08,09,04,05,11,12,07,02,14/
          INTEGER SS(64)/
         1 02,12,04,01,07,10,11,06,08,05,03,15,13,00,14,09.
         1 14,11,02,12,04,07,13,01,05,00,15,10,03,09,08,06.
         1 04,02,01,11,10,13,07,08,15,09,12,05,06,03,00,14,
         1 11,08,12.07,01,14,02,13,06,15,00,09,10,04,05,03/
          INTEGER S6(64)/
         1 12,01,10,15,09,02.06,08,00, 13,03,04,14,07,05,11,
         1 10,15,04,02,07.12,09,05,06,01, 13,14,00,11,03,08,
         1 09,14,15,05,02,08,12,03.07,00,04,10,01,13,11,06,
         1 04,03,02,12,09,05,15,10,11,14,01,07,06,00,08,13/
          INTEGER S7(64)/
         1 04,11,02, 14,15,00,08,13,03,12,09,07,05,10,08,01,
         1 13,00,11,07,04,09,01,10, 14,03,05,12,02,15,08,06.
         1 01,04,11,13,12,03,07,14,10, 15,06,08,00,05,09.02.
         1 06. 11,13,08,01,04,10.07,09,05,00,15,14,02,03,12/
          INTEGER S8(64)/
         1 13,02,08,04,06,15,11,01,10,09,03,14,05,00,12,07,
         1 01,15,13,08,10,03,07,04,12.05,06.11,00, 14,09,02,
         1 07,11,04,01,09,12,14,02,00,08,10,13,15,03,05,08,
         1 02,01.14.07,04.10,08,13,15,12,09.00,03,05.06,11/


C
C*** SWITCH=0 IS ENCRYPTION; SWITCH=1 IS DECRYPTION MODE
C
         N1=1
         N2=16
         N3=1
          IF (SWITCH .EQ. 0)GO TO 20
         N1=16
         N2=1
```

```
         N3=-1
C         LOOP WHICH DOES THE INITIAL PERMUTATION OF THE INPUT
20        DO 50 1=1,64
50        LR(I)=INPUT(IP(I))
C         MAIN LOOP WHICH ENCRYPTS OR DECRYPTS FOR 16 ROUNDS
          DO 500 N=N1,N2,N3
C         LOOP WHICH SAVES THE R REGISTER DO 75 1=1,32
75        TEMPL(I)=R(I)
C         LOOP WHICH EXPANDS THE R REGISTER USING THE E FUNCTION
C         AND DOES THE XOR OF THE KEY SCHEDULE SUBKEY AND THE EXPANDED R. DO 100
          1=1,48
          EX(I)=1
100       IF(R(E(I)) .EQ. KS(I.N)) EX(I)=0
C         LOOP WHICH DOES THE SUBSTITUTIONS USING THE 8 S TABLES.
         DO 200 J=0,7
          K=J*6+1
          IN=EX(K) *32+EX(K+5) * 16+EX(K+1 ) *8+EX(K+2) *4+EX(K+3) *2+EX(K+4)
          SUB=S(IN+1 .J+1)
          K=J*4
          F(K+1) = SUB/8
          F(K+2) = MOD(SUB,8)/4
          F(K+3) = MOD(SUB,4)/2
     200 F(K+4) - MOD(SUB,2)
C         LOOP WHICH DOES THE P PERMUTATION OPERATION TO THE 32-BIT RESULT
C         AND ALSO DOES THE XOR OF THE OLD L AND THE NEW RESULT OF THE F FUNCTION.
          DO 300 J=1,32
         R(J)-1
300       IF (L(J) .EQ. F(P(J))) R(J)-0
```



```
C         SETS THE NEW L TO BE THE OLD R THAT HAD BEEN SAVED.
          DO 400 J=1,32
400       L(J)=TEMPL(J)
500       CONTINUE
C         DOES THE INVERSE PERMUTATION AFTER THE 16 ROUNDS TO COMPLETE THE DES. DO
          600 J=1,64
600       OUTPUT(J)=LR(REVIPI(J))
          END
          SUBROUTINE SETKEY (KEY)
C         SUBROUTINE TO PERFORM DES KEY SCHEDULE
C         PRODUCED BY THE NATIONAL BUREAU OF STANDARDS
C         NOT SUBJECT TO COPYRIGHT - NOT SUPPORTED BY NBS
          IMPLICIT INTEGER (A-Z)
          INTEGER KEY(64)
C         KS IS THE COMMON AREA WITH THE DES SUBROUTINE.  SETKEY MUST SET KS
C         BEFORE THE DES IS CALLED OR GARBAGE WILL RESULT FROM THE DES. INTEGER
          KS(48.16).CD(56).C(28).D(28)
          COMMON KS
          EQUIVALENCE (CD(1), C(1)), (CD(29),D(1))
C         PCI IS THE PERMUTED CHOICE 1 DEFINED IN THE DES
```

```
           INTEGER PCI(56)/
          1 57,49,41,33,25,17,09,
          1 01,58,50,42,34,26,18,
          1 10,02,59,51,43,35,27,
          1 19,11,03,60.52,44,36,
          1 63,55,47,39,31,23,15,
          1 07,62,54,46,38,30,22,
          1 14,06,61,53,45,37,29,
          1 21,13,05,28,20,12,04/
C          PC2 IS THE PERMUTED CHOICE 2 DEFINED IN THE DES.
           INTEGER PC2(48)/
           1 14,17,11,24,01,05,
          1 03,28,15,06,21,10,
          1 23,19,12,04,26,08,
          1 16,07,27,20,13,02,
          1 41,52,31,37,47,55,
          1 30,40,51,45,33,48,
          1 44,49,39,56,34,53,
          1 46,42,50,36,29,32/
C          KSFT IS THE KEY SHIFT VECTOR DEFINED IN THE DES.
          INTEGER KSFT(16)/1.1,2,2,2,2,2.2,1,2,2,2,2,2,2,1/
C          LOOP WHICH PERFORMS THE FIRST PERMUTATION ON THE KEY, REMOVING THE
C          PARITY BITS AND SETTING UP THE C AND D REGISTERS.
          DO 100 1=1,56
100        OD(I)=KEY(PCI(I))
C          LOOP WHICH COMPUTES THE KS ARRAY FOR THE DES.  THIS TECHNIQUE USES
C          LOTS OF MEMORY BUT RUNS FAST.  THE KS NEED ONLY BE COMPUTED ONCE
C          FOR ALL THE ENCRYPT AND DECRYPT OPERATIONS WHICH USE THIS KEY.  DO 500
           1=1,16
           DO 300 J=1,KSFT(I)
           CT=C(1)
           DT=D(1)

          DO 200 K=1,27
           C(K)=C(K+1)
200        D(K)=D(K+1)
          C(28)=DT
300       D(28)=DT
          DO 400 J=1,48
400        KS(J,I)=CD(PC2(J))
500        CONTINUE
END
```

APPENDIX E

PASSWORD MANAGEMENT GUIDELINE

This appendix contains the complete Department of Defense Password Management Guideline issued by the DoD Computer Security Center. It is included as a part of the Password Usage Standard as additional information and guidance that may be used when implementing a password security system. This guideline was not available for coordination with the Password Usage Standard but it, like the other appendices, is not a required part of the Standard.

This guideline provides a set of good practices related to the use of password-based user authentication mechanisms in automatic data processing systems. While it was originally issued for systems processing classified and national security related information, it is also useful for application in systems processing sensitive, fragile or critical information (i.e., information that must be protected from unauthorized disclosure, modification or destruction). Comments on this guideline should be directed to the Office of Standards and Products, DoD Computer Security Center, Fort George G. Meade, Maryland 20755.

This guideline is the result of the work of numerous individuals. Sheila L. Brand, DoD Computer Security Center (DoDCSC) and Jeffrey D. Makey, formerly DoDCSC, are recognized as principal authors. Additional contributions were made by: Daniel J. Edwards, Mary B. Flaherty, Steven J. Padilla, all of the DoDCSC; John J. Stasak III, Gregory Wessel and Bernard Peters, all of the DoD; Roger R. Schell, formerly DoDCSC; and James P. Anderson. These people contributed to the formulation and review of the guideline.

1. Introduction

In August 1983, the DoD Computer Security Center published CSC-STD-001-83, Department of Defense Trusted Computer System Evaluation Criteria. That publication defines and describes feature and assurance requirements for six hierarchical classes of enhanced security protection for computer systems that are to be used for processing classified or other sensitive information. A major requirement common to all six classes is accountability:

> "Individual accountability is the key to securing and controlling any system that processes information on behalf of individuals or groups of individuals. A number of requirements must be met in order to satisfy this objective."
>
> "The first requirement is for individual user identification. Second, there is a need for authentication. Without authentication, user identification has no credibility. Without a credible identity (no) ... security policies can be properly invoked because there is no assurance that proper authorizations can be made." [2]

This guideline has been developed to assist in providing that much needed credibility of user identity by presenting a set of good practices related to the design, implementation and use of password-based user authentication mechanisms. It is intended that features and practices described in this guideline be incorporated into DoD automatic data processing (ADP) systems used for processing classified or other sensitive information.

2. Scope

The security provided by a password system depends on the passwords being kept secret at all times. Thus, a password is vulnerable to compromise whenever it is used, stored, or even known. In a password-based authentication mechanism implemented on an ADP system, passwords are vulnerable to compromise due to five essential aspects of the password system: 1) a password must be initially assigned to a user when enrolled on the ADP system; 2) a user's password must be changed periodically; 3) the ADP system must maintain a "password database"; 4) users must remember their passwords; and 5) users must enter their passwords into the

ADP system at authentication time. This guideline prescribes steps to be taken to minimize the vulnerability of passwords in each of these circumstances.

Specific areas addressed in this guideline include the responsibilities of the system security officer and of users, the functionality of the authentication mechanism, and password generation. The major features advocated in this guideline are:

- Users should be able to change their own passwords
- Passwords should be machine-generated rather than user-created
- Certain audit reports (e.g., date and time of last login) should be provided by the system directly to the user

For certain sensitive applications such as Command and Control Systems, pertinent DoD directives should be referenced in order to assess the need for additional identification and authentication features.

3. Control Objectives

The CSC-STD-001-83 gives the following as the Accountability Control Objective:

> "Systems that are used to process or handle classified or other sensitive information must assure individual accountability whenever either a mandatory or discretionary security policy is invoked. Furthermore, to assure accountability, the capability must exist for an authorized and competent agent to access and evaluate accountability information by a secure means, within a reasonable amount of time, and without undue difficulty." [2]

In order to attain the individual accountability required, it is necessary for the ADP system to be able to uniquely identify each person who uses it. In many cases, a password scheme will be used to achieve this. The Accountability Control Objective, applied to password systems, leads to the following control objectives for password systems.

Personal Identification. Password systems used to control access to ADP systems that process or handle classified or other sensitive information must assure the capability to uniquely identify each individual user of the system.

Authentication. Password systems used to control access to ADP systems that process or handle classified or other sensitive information must assure unequivocal authentication of the user's claimed identity.

Password Privacy. Password systems must assure, to the extent possible, protection of the password database consistent with the protection afforded the classified or other sensitive information processed or handled by the ADP system in which the

password systems operate.

Auditing. Password systems used to control access to ADP systems that process or handle classified or other sensitive information must be able to assist in the detection of password compromise.

4. Definitions

Access Port-A logical or physical identifier that a computer uses to distinguish different terminal input/ output data streams.

Expired Password-A password that must be changed by the user before login may be completed.

Password-A character string used to authenticate an identity. Knowledge of the password that is associated with an ID is considered proof of authorization to use the capabilities associated with that ID.

Password System -A part of an ADP system that is used to authenticate a user's identity. Assurance of unequivocal identification is based on the user's ability to enter a private password that no one else should know.

System Security Officer (550)-The person responsible for the security of an ADP system. The 550 is authorized to act in the "security administrator" role defined in CSC-STD-001-83. Functions that the 550 is expected to perform include auditing and changing security characteristics of a user.

Trusted Identification Forwarding-An identification method used in networks where the sending host can verify that an authorized user on its system is attempting a connection to another host The sending host transmits the required user authentication information to the receiving host. The receiving host can then verify that the user is validated for access to its system. This operation may be transparent to the user.

User ID-A unique symbol or character string that is used by an ADP system to uniquely identify a user. The security provided by a password system should not rely on secrecy of the user's ID.

5. Guidelines

In the remainder of this document, guidelines for good practice are presented in bold print, while amplifications, examples, and rationale are presented in normal print. The guidelines are given with two degrees of emphasis. Those that are most important to the security of a password system are presented with such wording as "The 550 should ..." (the word "should" is the key), while less critical functions are presented with such wording as "It is recommended that ..." ("recommended" is the key). Because it is anticipated that diverse user communities will adopt this guideline, all recommendations are presented in general rather than specific terminology, divorced from vendor-specific hardware or system software. Where features require the setting of a specific value (e.g., password maximum lifetime), it is suggested that these be designed as parametric settings leaving the determination of exact values to local security management who understand the particular security requirements of their user environment.

It is recommended that, whenever possible, the mechanisms discussed in this guide he automated. Automation will result in a minimal burden on the system administration and on the users, and thus in greater effectiveness of the mechanisms by eliminating situations where passwords might be exposed to people.

5.1 SSO Responsibilities

5.1.1 Initial System Passwords

Many ADP systems come from the vendor with a few standard user IDs (e.g., SYSTEM, TEST, MASTER, etc.) already enrolled in the system. The System Security Officer (550) should change the passwords for all standard user IDs before allowing the general user population to access the system. This can be easily assured if the standard user IDs are initially identified by the system as having "expired" passwords. (See sec. 3.2.2. 1 for discussion of expired passwords.)

5.1.2 Initial Password Assignment

The 550 is responsible for generating and assigning the initial password for each user ID. The user must then be informed of this password. In some areas, it may be necessary to prevent exposure of the password to the 550. In other cases, the user can easily nullify

this exposure.

5.1.2.1Preventing Exposure

There are methods that can be implemented to prevent exposure of a password to the 550 after it has been generated.

One technique is to print the user's password on a sealed multipart form in such a way that it is not visible on the top page of the form. The 550 would then protect the sealed password appropriately until it could be delivered to the user. In this case, the password is generated randomly by the ADP system and is not known by the 550. The password should he sealed so it is not visible and cannot he made visible without breaking the seal. Delivery of the password in this manner could require several days.

Another method of preventing exposure is to have the user present at password generation. The 550 must initiate the procedure and the user must shield the generated password and then remove or erase it from the display. This method cannot be used when user terminals are at remote locations.

It is recommended that a technique comparable to one of the above he used to prevent exposing a user's initial password to the 550.

Whatever method is used to distribute passwords, the 550 must receive an acknowledgment of receipt of the password within a specified time period.

5.1.2.2Nullifying Exposure

When a user's initial password must be exposed to the 550, this exposure may be nullified by having the user immediately change the password by the normal procedure. (Presumably, this change procedure does not expose the new password to the 550).

When a user's initial password is not protected from exposure to the 550, the user ID should be identified by the system as having an "expired password" which will require the user to change the password by the usual procedure (see sec. 5.2.2.3) before receiving authorization to access the system.

5.1.2.3Classification Assignment

Where the password must be classified, the initial classification assignment should be entered by the 550 to designate the highest security level that may be associated with each user's initial password and its successors.

5.1.3 Password Change Authorization

Occasionally, a user will forget the password or the 550 may determine that a user's password may have been compromised. To be able to correct these problems, it is recommended that the 550 be permitted to change the password of any user by generating a new one. The 550 should not have to know the user's password in order to do this, but should follow the same rules for distributing the new password that apply to initial password assignment (see sec. 5. 1.2). Positive identification of the user by the 550 is required when a forgotten password must be replaced.

5.1.4 Group IDs

Throughout the lifetime of an ADP system, each user ID should be assigned to only one person. In other words, no two people may ever have the same user ID at the same time, or even at different times. It should be considered a security violation when two or more people know the password for a user ID (except in the case when the 550 is the other person and the user ID is identified by the system as having an "expired password"). Note that there is no intention of prohibiting alternate forms of user identification (e.g., group IDs, functional titles) for non-authentication purposes (e.g., data access control, mail). If alternate IDs are used, they must be based on user IDs.

5.1.5 User ID Revalidation

The 550 should be responsible for the development of a procedure whereby prompt notification is given to the 550 when a user ID and password must be removed from the ADP system (e.g., when an employee leaves the sponsoring organization). In addition, all user IDs should be revalidated periodically, and information such as sponsor and means of offline contact (e.g., phone number, mailing address) updated as necessary. It Is recommended that this revalidation be done at least once per year.

5.2 User Responsibilities

5.2.1 Security Awareness

Users should understand their responsibility to keep passwords private and to report changes in their user status, suspected security violations, etc. To assure security awareness among the user population, it is recommended that each user be required to sign a statement to acknowledge understanding these responsibilities.

5.2.2 Changing Passwords

The simplest way to recover from the compromise of a password is to change it. Therefore, passwords should be changed on a periodic basis to counter the possibility of undetected password compromise. They should

be changed often enough so that there is an acceptably low probability of compromise during a password's lifetime. To avoid needless exposure of users' passwords to the 550, users should be able to change their passwords without Intervention by the 550.

5.2.2.1Password Lifetime

The most obvious threat to the security provided by a password system is from the compromise of passwords. The greater the length of time during which a password is used for authentication purposes, the more opportunities there are for exposing it. In a useful password system, the probability of compromise of a password increases during its lifetime. For a period of time, this probability could be considered acceptably low while after a longer period of time, it would be considered unacceptably high. At this latter point, use of the password should be considered suspect rather than a reliable proof of identity. By appropriately limiting the length of time (called the password lifetime) during which a password can be used, the vulnerability of the password can remain acceptable.

There should be a maximum lifetime for all passwords. To protect against unknown threats, it is recommended that the maximum lifetime of a password be no greater than 1 year. The presence of known threats may indicate a need for a shorter maximum lifetime. Also, depending on the size of the password space and on how fast a penetrator can execute a login attempt, it may be necessary to change passwords even more frequently. See Appendix B.3 for a discussion of the relationship between password lifetime, password space, and the guess rate.

A password should be invalidated at the end of its maximum lifetime. It is recommended that, at a predetermined period of time prior to the expiration of a password's lifetime, the user ID it is associated with be notified by the system as having an "expired" password. A user who logs in with an ID having an expired password should be required to change the password for that user ID before further access to the system is permitted. If a password is not changed before the end of its maximum lifetime, it is recommended that the user ID it is associated with be

identified by the system as "locked." No login should be permitted to a locked user ID, but the 550 should be able to unlock the user ID by changing the password for that user ID, following the same rules that apply to Initial password entry (see sec. 5.1.2). After a password has been changed, the lifetime period for the password should be reset to the maximum value established by the system.

5.2.2.2Change Authorization

To be consistent with the Password Privacy control objective, users (other than the 550) should be permitted to change only their own passwords. To ensure this, it is recommended that the user enter the old password and the user ID/password combination be validated as part of the password changing procedure.

5.2.2.3Change Procedure

Changing a password in a secure manner involves several steps. The following procedure is recommended:

The procedure should be Invoked at the user's request or when a user logs in with an expired password. If the change is necessary due to an expired password, the user should be so informed. The user should be presented with a brief summary of the major steps in changing a password, including a caution that the user should ensure that no one else is watching what the user is doing. Except when the change procedure is part of the login procedure (e.g., logging in with an expired password), the user's current password should be entered to re-authenticate identity. The change procedure should display a new password for the user. The new password should be different from the old one and should be generated by an algorithm that satisfies the specifications In Appendix E.l. The user should then enter the new password twice so the procedure can verify that the user can consistently enter the password correctly. The new password should be obliterated by techniques such as overprinting or terminal screen erasing. If the two entered passwords are identical to the generated password, the password database should be updated (i.e., the old password deleted or invalidated and the new password associated with the user ID) and a message to this effect should be displayed. Failure by the user to correctly enter the current password or the generated password should result in a useful error message to the user and In the change procedure being aborted without changing the password. When the attempt to change an expired password is not successful, the password should be retained as expired and the user given the option to again change the password or logout. An audit record should be generated that indicates whether or not the change was successful.

5.2.3Login to a Connected System

Users should be required to authenticate their identities at "login" time by supplying their password along with their user ID. It is recommended that some form of trusted identification forwarding be used between hosts when users connect to other ADP systems through a network. When trusted identification forwarding is not used, a remote host should require the user's ID and password when logging in through a network connection. Note that user IDs on different hosts for the same user may be different, and that corresponding machine-generated passwords almost certainly will be different. Note also that a password required by a remote host is vulnerable to compromise by the local host or intermediate hosts.

5.2.4Remembering Passwords

Since users must supply their passwords to the ADP system at authentication time, it follows that they must know what their passwords are. It is recommended that users memorize their passwords and not write them on any medium. If passwords must be written, they should be protected in a manner that is consistent with the damage that could be caused by their compromise. See Appendix E.4 for guidance on the protection of passwords.

5.3 Authentication Mechanism Functionality

5.3.1Internal Storage of Passwords

It is normally necessary for the ADP system to store internally the user ID for each authorized system user as well as some representation of the password and, when required, the clearance and authorizations that at associated with each user ID. Without some form of access control over this information, it will be possible for unauthorized users to read and/or modify the password database. Unauthorized reading and writing of the password database are a concern. Reading it could result in disclosure of passwords to unauthorized users. Being able to write it could result, for example, in user A changing user B's password so user A could login under user

B's identity. Note that it is necessary for the login process to be able to read the password database and for the password changing process to be able to read and write the password database.

Stored passwords should be protected by access controls provided by the ADP system, by password encryption, or by both.

5.3.1.1Use of Access Control Mechanisms

Access control mechanisms (e.g., mandatory or discretionary controls as discussed in CSC-STD-001-83) should be used to protect the password database from unauthorized modification and disclosure.

5.3.1.2Use of Encryption

Encryption of stored passwords should be used whenever the access control mechanisms provided by the ADP system are not adequate to prevent exposure of the stored passwords. It is recommended that password encryption be used even when other access controls are considered adequate, as this helps protect against possible exposure when access controls are bypassed (e.g., system dumps). When encryption is used to protect stored passwords, it is recommended that the algorithm meet the specifications in Appendix E.2. It is recommended that encryption be done immediately after entry, that the memory containing the plaintext password be erased immediately after encryption, and that only the encrypted password be used in comparisons. There is no need to be able to decrypt passwords. Comparisons can be made by encrypting the password entered at login and comparing the encrypted form with the encrypted password stored in the password database.

5.3.2Entry

Passwords should be entered after providing a user ID to the system. If the entry is correct, the system should then display the date and time of the user's last login.

It is recommended that the system not echo passwords that users type in. When the system cannot prevent a password from being echoed (e.g., in a half-duplex connection), it is recommended that a random overprint mask be printed before or after the password is entered, as appropriate, to conceal the typed password.

The complete password as entered by the user should be an

exact match, character for character, with the user's current password.

5.3.3Transmission

During transmission of a password from a user's terminal to the computer In which the authentication is done, passwords should be protected In a manner that is consistent with the damage that could be caused by their compromise. Since passwords are no more sensitive than the data they provide access to, there is generally no reason to protect them, during transmission, to any greater degree (e.g., encryption) than regular data is protected. See Appendix B.4 for guidance on the protection of passwords.

5.3.4Login Attempt Rate

By controlling the rate at which login attempts can be made (where each attempt constitutes a guess of a password), the number of guesses a penetrator can make during a password's lifetime is limited to a known upper bound. To control attacks where a penetrator attempts many logins through a single access port, the password guess rate should be controlled on a per-access port basis. That is, each access port should be individually controlled to limit the rate at which logIn attempts can be made at each port. When a penetrator can easily switch among multiple access ports, it is recommended that the password guess rate also be controlled on a per-user ID basis.

It is recommended that maximum logIn attempt rates fall within the range of one per second to one per minute. This range provides reasonable user-friendliness without permitting so many login attempts that an extremely large password space or an extremely short password lifetime is necessary. See Appendix E.3 for a discussion of the relationship between the guess rate, password lifetime, and password space.

Note that it is not intended that login be an inherently slow procedure, for there is no reason to delay a successful login. However, in the event of an unsuccessful login attempt, it is quite reasonable to use an internal timer to enforce the desired delay before permitting the next login attempt. The user should not be able to bypass this procedure.

5.3.5Auditing

5.3.5.1 Audit Trails

The system should be able to create an audit trail of password usage and changes. Such an audit trail should not contain actual passwords or character strings that were incorrectly given

as passwords, since this could expose the password of a legitimate user who mistyped his user ID or password. Auditable events should include: successful login, unsuccessful login attempts, use of the password changing procedure, and the locking of a user ID due to its password reaching the end of its lifetime. For each recorded event, the audit record should include: date and time of the event, type of event, offered user ID for unsuccessful logins or actual user ID for other events, and origin of the event (e.g., terminal or access port ID). Audit records of password changes should also indicate whether or not the change was successful.

5.3.5.2 Real-time Notification to System Personnel

It is recommended that each accumulation of 5 consecutive unsuccessful login attempts from a single access port or against a single user ID results in immediate notification of the event to the ADP system operator or the 550. While there is no requirement for the 550 or operator to take any action upon receiving the notification, frequent notifications may indicate that a penetration attempt is in progress and may warrant investigation and possible corrective action.

5.3.5.3 Notification to the User

Upon successful logIn, the user should be notified of:

- The date and time of user's last login;
- The location of the user (as can best be determined) at last login; and
- Each unsuccessful login attempt to this user ID since the last successful login.

This provides a means for the user to determine if someone else is using or attempting to guess this user ID and password.

5.4 Password Protection

5.4.1Single Guess Probability

The probability that any single attempt at guessing a password will be successful is one of the most critical factors in a password system. This probability depends on the size of the password space and the statistical distribution within that space of passwords that are actually used. Since many user-created

passwords are particularly easy to guess, all passwords should be machine-generated using an algorithm that meets the specifications in Appendix E.l.

5.4.2Password Distribution

During distribution to the user, passwords should be protected to the same degree as the information to which they provide access. Machine-generated passwords should be displayed on the user's terminal at the time of change, along with appropriate cautions to the user to protect the password. At the completion of the change procedure, It Is recommended that displayed passwords be erased or overstrike as appropriate for the terminal type. Passwords changed by the 550 should be distributed in a manner that is consistent with the damage that could be caused by their compromise. See Appendix E.4 for guidance on the protection of passwords.

APPENDIX E.1

PASSWORD GENERATION ALGORITHM

This appendix describes the requirements to be met by an acceptable password generation algorithm. The issues involved relate to the specifications for password space, random seed generation, pseudo-random number generation and "user-friendly" passwords.

1. Password Space

The size of the password space is a function of the size of the alphabet and the number of characters from that alphabet that are used to create passwords. (The maximum size of the password space can be expressed as S=AM where S is the maximum password space, A is the alphabet size and M is the password length.) To determine the minimum size of the password space needed to satisfy the security requirements for an operating environment, equation (3) in Appendix B.3 can be used. The password generation algorithm selected should be able to generate at least that number of passwords. In addition, the generated passwords should be, at a minimum, 6 characters in length.

2. Random Seeds

When a pseudo-random number generator is used in a password generation algorithm, it should accept random data as input that would provide output which has a high degree of unpredictability. This random data (seed) can be derived from a number of available parameters such as a system clock, system registers, date, time, etc. The parameters should be selected to ensure that the number of unique seeds that can be generated from these inputs should be at least equal to the minimum number of passwords that must be generated. When passwords are used to protect classified information, the seed generator should be approved by the DoD Computer Security Center.

3. Pseudo-Random Number Generator

Using a random seed as input, the pseudo-random number generator

that drives a password generation algorithm should have the property that each bit in the pseudo-random number that it generates is a complex function of all the bits in the seed. The Federal Data Encryption Standard (DES), as specified in FIPS 46, is an example of a pseudo-random number generator with this property. If DES is used, it is suggested that the 64-bit Output Feedback (OFB) mode be used as specified in FIPS 81. In this case, the seed used as input could consist of:

- An initialization vector
- A cryptographic key
- Plain text

Factors that can be used as input to these parameters are:

For the initialization vector:

- System clock
- System ID
- User ID
- Date and time

For the cryptographic key:

- System interrupt registers
- System status registers
- System counters

The plain text can be an external randomly generated 64-bit value (8 characters input by the 550).

The resulting pseudo-random number that is output will be the 64 bits of cipher text generated in the 64-bit OFB mode. The password generation algorithm can either format this pseudo-random number into a password or use it as an index (or indices) into a table and use the contents from this table to form a password or a passphrase.

4. "User-Friendly" Passwords

To assist users in remembering their passwords, the password generation algorithm should generate pass-words or passphrases that are "easy" to remember. Passwords formed by randomly choosing characters are generally difficult to remember. Passwords that are pronounceable are often easy to remember, as are passphrases that are formed by concatenating real words into a phrase or sentence.

APPENDIX E.2

PASSWORD ENCRYPTION ALGORITHM

Password encryption is advocated as a password protection measure. The algorithm selected for this would be determined by the system environment. Some environments may require that a classified encryption algorithm be used, while for other environments an unclassified algorithm would be required.

1. Encryption Algorithm

A conventional or public key cryptographic algorithm which is configured as a "one-way" encryption algorithm may be used for password encryption, but whatever algorithm is used, the protection that the encryption algorithm provides should rely on its complexity. If there is a key that can be used with the algorithm to decrypt passwords, that key should not be stored In the ADP system.

2. Assurance for Unique Encrypted Passwords

If a password encryption system depends only on the password and other fixed information, there is a possibility that two different users will have identical encrypted passwords. A user who discovers another user with an identical encrypted password will then know that the same password will work for both user IDs even if they don't have identical plaintext passwords. To minimize this possibility, it is recommended that the encryption algorithm use the ADP system name (in network environments) and the user's ID as factors in the encryption. (This can be easily accomplished by concatenating the system ID, user ID and password, and then applying the encryption algorithm to the resulting string.)

APPENDIX E.3

DETERMINING PASSWORD LENGTH

The security afforded by passwords is determined by the probability that a password can be guessed during its lifetime. The smaller that probability, the greater the security provided by the password. All else being equal, the longer the password, the greater the security it provides. This appendix reviews the mathematics involved in establishing how long a password should be.

The basic parameters that affect the length of the password needed to provide a given degree of security are:

L=maximum lifetime that a password can be used to log into the system.

P = probability that a password can be guessed within its lifetime, assuming continuous guesses for this period.

R=number of guesses per unit of time that it is possible to make.

S =password space, i.e., the total number of unique passwords that the password generation algorithm can generate.

1. Relationship

Considering only the cases where S is greater than L X R and therefore P is less than 1, the relationship between these parameters is expressed by the equation:

$$P=\frac{LXR}{S}$$

A detailed explanation of the derivation of this basic equation is given in Appendix E.6.

2. Guess Rate

Several factors contribute to the rate at which attempts can be made to gain access to the data on a system when a valid password is not known. First and foremost is the protection given to the password data base itself. If the password data base is unprotected (i.e., can be read by anyone as ordinary data), then "guessing" may not be required.

If the password data base can be read, but the passwords are encrypted (see Appendix E.2), a very high guess rate may be possible by using a computer to try a dictionary of possible passwords to see if ciphertext can be generated that is the same as one in the password data base. A similar situation frequently occurs where only passwords are used to protect files.

Finally, if the password data base has effective access controls and the login procedure cannot be bypassed, the guess rate can be controlled by setting limits on the number of login or other attempts that can be made before terminating the connection or process.

3. Password Lifetime

All other things being equal, the shorter the lifetime of a password, the fewer the number of guesses that can be made and thus the greater the degree of password security. As stated in 5.2.2.1, the maximum password lifetime should not exceed 1 year.

4. Password Space

Password length and alphabet size are factors in computing the maximum password space requirements. Equation (2) expresses the relationship between S, A, and M where:

S =password space
A =number of alphabet symbols
M=password length

$$S=A^{M} \qquad (2)$$

To illustrate: If passwords consisting of 4 digits using an alphabet of 10 digits (e.g., 0-9) are to be generated:

$$S=10^{4}$$

That is, 10,000 unique 4-digit passwords could be generated. Likewise, to generate random 6-character passwords from an alphabet of 26 characters (e.g., A-Z):

$$5=26^{6}$$

That is, 3.089*108 unique 6-character passwords could be generated.

"User-friendly" passwords (sometimes referred to as passphrases) could be generated by using, for example, 3 symbols from an alphabet (dictionary) of 2000 symbols, where each symbol was a pronounceable word of 4, 5, or 6 characters. Using equation (2) and setting:

A =2000 symbols (words)

M=3

Then $S=2000^3$

That is, $8* 10^9$ unique passwords could be generated where each password was made up of 3 words taken from a dictionary of 2000 words.

5. A Procedure for Determining Password Length

What is important in using passwords is how long to make the password to resist exhaustive penetration attacks. We can do this by using the following procedure:

a. Establish an acceptable probability, P, that a password will be guessed during its lifetime. For example, when used as a login authenticator, the probability may be no more than 1 in 1,000,000. In another case, where very sensitive data is involved, the value for P may be set at 10^{-20}.

b. Solve for the size of the password space, S, with the equation derived from equation (1)

$$S=P^{\underline{G}} \qquad (3)$$

where G=L x R

c. Determine the length of the password, M, from the equation

$$M = \log (\text{number of symbols in the 'alphabet'})^{\log S}$$

M will generally be a real number that must be rounded up or down to the nearest whole number. Examples of calculating many of the values described above are given below.

6. Worked Examples

An example shown here is drawn from a real network case. The problem is to determine the needed password length to reduce to an acceptable level the probability that a password will be guessed during its lifetime.

The network to which this is applied supports both a 300-baud and a 1200-baud service. Experiments on the network have determined that it is possible to make about 8.5 guesses per minute on the 300-baud service and 14 guesses per minute on the 1200-baud service. (The reason that the 'guess rate' for the 1200-baud service is not 4 times that of the 300-baud service is that the system response time, which is not affected by the improved transmission speed, becomes the limiting factor in how many guesses can be accomplished in a given amount of time.)

In this example, the arbitrary value of 10^{-6} is used for the probability (P) of guessing the password in its lifetime. As we will see below, the password lifetime is not the critical factor here as long as the password is changed at least once per year.

The statement of the problem is to find a password length that will resist being guessed with a probability of 1 in 10^{-6} in 1 year of continuous guesses.

When three parameters in equation (1) are known, the fourth value can be found. To find the password space required by our examples, the following parameters are given:

L is set for 6 months and 12 months.

P is set for 1 in 1,000,000 (acceptable probability of guessing the password).

R is set at 8.5 guesses per minute (guess rate possible with 300-baud service).

At 8.5 guesses per minute, the number of guesses per day would be 12,240.

Substituting 183 days for 6 months then using equation (3),

$$S = \frac{G}{P} = \frac{183 \times 12240}{.000001} = 2.23992 \times 10^{12} \text{ passwords}$$

The 12-month value is twice that of the 6-month case.

With this data, and using equation (4), we can determine the length of the passwords as a function of the size of the alphabet from which they are drawn. We will assume two alphabet sizes: a 26-letter alphabet and a 36-letter-and-number alphabet.

$$M=\frac{\log(2.23992\times10^{12})}{\log 26}=8.72 \text{ (for 6-month lifetime)}$$

$$M=\frac{\log(4.4676\times10^{12})}{\log 26}=8.94 \text{ (for 12-month lifetime)}$$

$$M=\frac{\log(2.23992\times10^{12})}{\log 36}=793 \text{ (for 6-month lifetime)}$$

$$M=\frac{\log(4.4676X\ 10^{12})}{\log 36}=8.13 \text{ (for 12-month lifetime)}$$

Table 1 presents the results.

Table 1

Length of Password

MAXIMUM LIFETIME (months)	26-character alphabet	36character alphabet
6	9 (rounded up from 8.72)	8 (rounded up from 7.93)
12	9 (rounded up from 8,94)	8 (rounded down from 8.13)

7. Passphrases

A "passphrase" is a concatenation of words drawn from a dictionary. The dictionary is merely the collection of symbols making up the "alphabet" from which the password is generated. As an example, suppose the passphrase is made up of words drawn from a dictionary of 4-, 5- and 6-letter words. There are approximately 3,780 4-letter words, 7,500 5-letter words and 12,000 6-letter words in English. The "alphabet size"

for generating passphrases is approximately 23,300.
We can compute how many words, drawn at random from the dictionary of 23,300 words, are needed to produce a passphrase that will be resistant to exhaustive attack with the probability of 1 x 10-6.
We have to solve for S as before, and from that, solve for M, the length of the password (i.e., number of alphabet symbols or words).

For L= 12 months, 5=4.4676*1012, Log S= 12.6500

For L=6 months, 5=2.2399*1012, Log 5=12.3502

Log 23300=4.3669

Using equation (4) we obtain:

$$\text{For L=12 months} \quad M = \frac{12\ 6500}{4.3669} = 3 \text{ (rounded from 2.89)}$$

$$\text{For L=6 months} \quad M = \frac{12\ 3502}{4.'3669} = 3 \text{ (rounded from 2.82)}$$

Thus, for the passphrase algorithm described, namely selection at random from a dictionary of 23,300 words, only 3 words are needed in a passphrase to obtain the desired resistance to exhaustive enumeration. In using the algorithm, each word of the phrase is drawn independently from the dictionary. This may result in a word appearing more than once in the passphrase.

APPENDIX E.4

PROTECTION BASIS FOR PASSWORDS

Passwords are used to prevent people who have physical access to an ADP system from gaining access to data belonging to another user. Thus, a password should be protected in a manner that is consistent with the damage that might be caused by its exposure to someone who has the opportunity to use it (i.e., has physical access to the ADP system terminals). Exposure of a password to someone who is physically prevented from attempting to use it is not a threat.

1. Systems Containing Only Unclassified Information

Although an ADP system may process only unclassified information, it still may require that the data be protected from unauthorized use. Although the password is unclassified, the obligation remains that the user protect this password so that only those with a need-to-know can access the data.

2. Systems Containing Classified Information

Passwords that are used in ADP systems that operate in the dedicated or system high security modes [3] should not be classified, but should be protected to the same degree as For Official Use Only information. In this case, there is no need to classify passwords since access to the area in which the system resides is restricted to those with a clearance as high as the highest classification level of the information processed. A person who obtained a password for a system running in dedicated or system high security mode but who did not possess the proper security clearance would be unable to gain physical access to the system and use the password.

For systems operating in the multilevel security mode [3], passwords may or may not have to be classified.

When the ability to access classified information is based on the physical protection of the terminal rather than on the identity of the user (i.e., when all terminals are single-level devices), passwords should not be classified. but should be protected to the same degree as For Official Use Only information. There is no need to classify passwords that can only be used on single-level terminals, since physical access to single-level terminals is controlled to the level associated with the terminal. When the ability to access classified information is based on the user's identity and is not restricted by the level of the terminal (i.e., multilevel terminals), each password must be classified to the highest level of the information to which it provides access.

When multilevel terminals are used, the system determines the user's access authorizations to classified material based on his identity, and authenticates the identity by requiring a password. Thus, the ADP system can protect the information it processes only to the extent that passwords are protected. For example, a user with a Secret clearance can access Secret information. Compromise of that user's password could result in the compromise of Secret information; therefore, the password would be classified Secret. In the case of a system with multilevel terminals, disclosure of a Top Secret user's password to a Secret user would allow the Secret user to login as the Top Secret user and thus gain access to Top Secret information. Disclosure of Top Secret information to someone with only a Secret clearance can cause exceptionally grave damage to the national security. Since disclosure of the Top Secret user's password could lead to this, the password must be classified Top Secret [5].

Note that classified passwords must not be used on terminals that are not authorized for data at the level of the password (e.g., a Top Secret password must not be used on a Secret terminal). The presence of both single-level and multilevel terminals on a system may indicate the need for passwords at each security level. At a minimum, an unclassified password should be available for use on terminals that are only authorized for unclassified data.

APPENDIX E.5

FEATURES FOR USE IN VERY SENSITIVE APPLICATIONS

The following features can be used to enhance the security provided by a password system. Because they are somewhat "user-unfriendly," they are recommended for environments only when there is a high threat of password compromise.

1. One-Time Passwords

One-time passwords (i.e., those that are changed after each use) are useful when the password is not adequately protected from compromise during login (e.g., the communication line is suspected of being tapped). The difficult part of using one-time passwords is in the distribution of the new passwords. If a one-time password is changed often because of frequent use, the distribution of new one-time passwords becomes a significant point of vulnerability. There are products on the market that generate such passwords through a cryptographic protocol between the destination host and a hand-held device the user can carry.

2. Failed Login Attempt Limits

In some instances, it may be desirable to count the number of unsuccessful login attempts for each user ID and to base password expiration and user ID locking on the actual number of failed attempts. (Changing a password would reset the count for that user ID to zero.) For example, the password could be identified as expired after 100 failed login attempts, and the user ID locked after 500.

APPENDIX E.6

ON THE PROBABILITY OF GUESSING A PASSWORD

Appendix B.3 discusses the techniques for finding a password

length that will resist exhaustive enumeration over the lifetime of the password with a given probability. This appendix derives the probability of guessing a password during its lifetime.

As in Appendix B.3, we use the parameters:

L = password lifetime R = guess rate S = size of the password space
P=probability of guessing a password during its lifetime.

The total number of guesses, (G), that can be made during a password's lifetime is:

$$G=R \times L \qquad (I)$$

At this point, we need to consider the relation of the size of the password space, S, to G. Clearly, if S is so small that one could try all possible passwords before the lifetime of the password expires, the probability of guessing the password is 1. As a result, we consider only cases where S is greater than G.

The probability question then is, "For the case where S is greater than G, what is the probability that in G guesses the password will be guessed?". This is the same as asking the question, "What is the probability that in the lifetime of the password, it will be guessed?". The probability sought is:

How many ways one can make G guesses (of S objects)

that include the password

How many different ways one can make G guesses of S objects

Note that the probability that is appealed to is of the simplest form. It is derived from the definition of probability that the probability of an event is given by the number of ways the event can happen divided by the number of ways an event can happen or fail.

We first observe that the total number of ways one can make G guesses of S things is given by sCg (the combinatorial notation that means the number of combinations of "s" things taken "g" at a time). (Lower case letters are used with the combinatorial notation in order to make the expressions more readable.) This is determined by:

$$\frac{s!}{}$$

g!(s-g)!

Thus, if S=A,B,C,D,E, one could make 3 guesses in 5C3 different ways, 5*4*3*2*1/3*2*1*2*1 = 10.

(Enumerating, they are ABC,ABD,ABE,ACD,ACE,ADE,BCD,BCE,BDE,CDE.)

The problem of finding the number of guesses of this total that include a specific password, e.g., an "A" is addressed by considering a reduced set without the specific password and asking how many ways one can make G guesses with the reduced set. Then, the total number of ways to make G guesses that include the specified password is the difference between the two values. This is given by:

sCg-(s-1)Cg (2)

That is, remove the designated password from the set S, compute the number of ways of making G guesses without the password, then consider the difference between the two values.

If we ask in our example how many ways to make 3 guesses that do NOT include a particular password from the set of 5 (say an "A"), this is given by:

4C3=4*3*2*1/3*2*1*1 =4

Enumerating for the specific case of an "A", they are BCD,BCE,BDE,CDE.

The number of ways to make 3 guesses that include the designated element is 10-4=6. Thus, the probability of guessing a designated password in 3 guesses is 6/10 or .6.

Simplification

It is indeed fortuitous that there is a theorem in any number of books on Probability Theory that states:

nCr=(n-1)C(r-1)+(n- 1)Cr

This may also be expressed as:

$$nCr-(n-1)Cr=(n-1)C(r-1)$$

Substituting s for n and g for r we obtain the expression:

$$(s-l)C(g-1)$$

for the number of ways of making G guesses that include a specific password. Then, the probability that a given password will be guessed during the lifetime of that password is given by:

$$\frac{P-(s-1)C(g-1)}{sCg} \qquad (6)$$

Evaluating this expression gives:

$$P=\frac{\frac{(s-1)!}{(g-1)!((s-1)-(g-1))!}}{\frac{s!}{g!(s-g)!}}=\frac{(g-1)!(s-g)!}{s!}=\frac{g!(s-1)!}{(g-1)s!}=\frac{g}{s}$$

This derivation of the probability of guessing a password during its lifetime, i.e.,

$$P=S^{G}$$

is important in that it allows us to derive the size of the password space

$$S=P^{\frac{G}{}} \qquad (9)$$

given an acceptable probability of not guessing the password during its lifetime.

APPENDIX E.7

REFERENCES

[1] Brown, R. L. Computer System Access Control Using Passwords, final draft, Aerospace Corporation, 16 January 1984.

[2] DoD Computer Security Center. Department of Defense Trusted Computer System Evaluation Criteria, CSC-STD-001-83, 15 August 1983.

[3] DoD Directive 5200.28, Security Requirements for Automatic Data Processing (ADP) Systems, revised April 1978.

[4] Downey, P. J. Multics Security Evaluation: Password and File Encryption Techniques, ESD-TR-74- 193, Vol. III, AD-A045279, AFSC Electronic Systems Division, Hanscom AFB, Mass., June 1977.

[5] Executive Order 12356, National Security Information, 6 April 1982.

[6] Gasser, M. A Random Word Generator for Pronounceable Passwords, MTR-3006, ESD-TR-75-97, ADA017676, MITRE Corp., Bedford, Mass., November 1975.

[7] Wood, H. M. The Use of Passwords for Controlled Access to Computer Resources, NBS Special Publication 500-9, U.S. Department of Commerce, National Bureau of Standards, May 1977.

[8] National Bureau of Standards. Federal Information Processing Standards Publication 46, Data Encryption Standard, 15 January 1977.

[9] National Bureau of Standards. Federal Information Processing Standards Publication 81, DES Modes of Operation, 2 December 1980.