FIPS PUB 181 - Announcing the Standard for Automated Password Generator

Federal Information Processing Standards Publication 181

1993 October 5

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100-235.

- 1. Name of Standard. Automated Password Generator.
- 2. Category of Standard. Computer Security.
- 3. Explanation. A password is a protected character string used to authenticate the identity of a computer system user or to authorize access to system resources. When users are allowed to select their own passwords they often select passwords that are easily compromised. An automated password generator creates random passwords that have no association with a particular user.
- This Automated Password Generator Standard specifies an algorithm to generate passwords for the protection of computer resources. This standard is for use in conjunction with FIPS PUB 112, Password Usage Standard, which provides basic security criteria for the design, implementation, and use of passwords. The algorithm uses random numbers to select the characters that form the random pronounceable passwords. The random numbers are generated by a random number subroutine based on the Electronic Codebook mode of the Data Encryption Standard (DES) (FIPS PUB 46-1). The random number subroutine uses a pseudorandom DES key generated in accordance with the procedure described in Appendix C of ANSI X9.17.
- Similar to DES, the FIPS for Automated Password Generator is an interoperability standard. Interoperability standards specify functions and formats so that data transmitted can be properly acted upon when received by another computer. This type of standard is independent of physical implementation. Implementors are required to use the algorithm defined in the FIPS, however, they are not constrained in how they package it. For discussion purposes a NIST implementation of the Automated Password Generator is provided. It is expected that commercial implementations will be based on the latest technologies and differ from NIST's, however the results should be logically equivalent to that of this FIPS.
- 4. Approving Authority. Secretary of Commerce.5. Maintenance Agency. U.S.

Department of Commerce, National Institute of Standards and Technology (NIST), Computer Systems Laboratory (CSL).

- 6. Cross Index.
- a. American National Standards Institute (ANSI) X9.28, Financial Institution Multiple Center Key Management (Wholesale) Draft. b. Department of Defense CSC-STD-002-85, Password Management Guideline. c. Federal Information Processing Standards Publication (FIPS PUB) 48, Guidelines on Evaluation of Techniques for Automated Personal Identification. d. Federal Information Processing Standards Publication (FIPS PUB) 46-1, Data Encryption Standard. e. Federal Information Processing Standards Publication (FIPS PUB) 81, DES Modes of Operation. f. Federal Information Processing Standards Publication (FIPS PUB) 83, Guideline on User Authentication Techniques for Computer Network Access Control. g. Federal Information Processing Standards Publication (FIPS PUB) 112, Password Usage. h. Federal Information Processing Standards Publication (FIPS PUB) 171, Key Management Using ANSI X9.17. i. National Technical Information Service (NTIS) AD A 017676, A Random Word Generator for Pronounceable Passwords.
- 7. Objectives. The objectives of this standard are to:
- a. improve the administration of password systems that are used for authenticating the identity of individuals accessing computer resources or files;
- b. provide a standard automated method for producing pronounceable passwords that have no association with a particular user;
- c. produce passwords that are easily remembered, stored, and entered into computer systems, yet not readily susceptible to automated techniques that have been developed to search for and disclose passwords.
- 8. Applicability. This standard is applicable to the development of procurement or design specifications for implementing an automatic password generation algorithm within a computer system. It shall be used by all Federal departments and agencies when there is a requirement for computer generated pronounceable passwords for authenticating users of computer systems, or for authorizing access to resources in those systems.
- This standard does not require the use of passwords in a computer system, but establishes an automatic password generation algorithm for use in systems where an agency's computer security policy requires computer generated pronounceable passwords. It should be used in conjunction with FIPS PUB 112, Password Usage Standard, which specifies basic security criteria for the design, implementation, and use of passwords.
- 9. Export Control. The Bureau of Export Administration, U.S. Department of Commerce, is responsible for administering export controls on cryptographic products used for authentication and access control, which categories would include implementations of the Automated Password Generator. Vendors should contact the following for a product classification:
- Bureau of Export Administration U.S. Department of Commerce P.O. Box 273 Washington, DC 20044 Telephone: (202) 482-0708
- Following this determination, the vendor will be informed whether an export license is required and will be provided further information as appropriate.

- 10. Specifications. Federal Information Processing Standard (FIPS) 181, Automated Password Generator (affixed);
- 11. Qualifications. The Automated Password Generator uses the Electronic Codebook (ECB) mode of the Data Encryption Standard (DES), Federal Information Processing Standard 46-1 (FIPS PUB 46- 1), as the random number generator. This mode of operation is specified in FIPS 81, DES Modes of Operation.
- The protection provided by the DES algorithm against potential threats has been reviewed every 5 years since its adoption in 1977 and has been reaffirmed during each of those reviews. The DES, and the possible threats reducing the security provided by the use of DES, will undergo continual review by NIST and other cognizant Federal organizations. The new technology available at review time will be evaluated to determine its impact on the DES. In addition, the awareness of any breakthrough in technology or any mathematical weakness of the algorithm will cause NIST to reevaluate the DES and provide necessary revisions.
- 12. Implementation Schedule. This Standard becomes effective March 25, 1994.
- 13. Waivers. Under certain exceptional circumstances, the heads of Federal departments and agencies may approve waivers to Federal Information Processing Standards (FIPS). The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of Title 44, U.S. Code. Waivers shall be granted only when compliance with a standard would:
- a. adversely affect the accomplishment of the mission of an operator of a Federal computer system, or
- b. cause a major adverse financial impact on the operator which is not offset by Government-wide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision which explains the basis on which the agency head made the required finding(s). A copy of each such decision, with procurement sensitive or classified portions clearly identified, shall be sent to: National Institute of Standards and Technology; ATTN: FIPS Waiver Decisions; Technology Building, Room B-154; Gaithersburg, MD 20899.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Government Affairs of the Senate and shall be published promptly in the Federal Register.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an

acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A copy of the waiver, any supporting documents, the document approving the waiver, and any supporting and accompanying documents, with such deletions as the agency is authorized and decides to make under 5 U.S.C Sec. 552(b), shall be part of the procurement documentation and retained by the agency.

- 14. Where to Obtain Copies. Copies of this publication are available 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 181 (FIPSPUB181), and identify the title. When microfiche is desired, this should be specified. Payment may be made by check, money order, credit card, or deposit account.Federal Information Processing Standards Publication 181

1993 October 5

Announcing the Standard for

Automated Password Generator

Contents

- 1.0 INTRODUCTION 6
- 2.0 TECHNICAL EXPLANATION 6
- 2.1 Unit Table 6
- 2.2 Digram Table 7
- 2.3 Random Number Generator Subroutine 7
- 2.4 Random Word Algorithm. 8
- 2.5 NIST Implementation. 9

Appendix A 10

1.0 INTRODUCTION

The Automated Password Generator standard is derived from a C-code version of the program described in "A Random Word Generator For Pronounceable Passwords," National Technical Information Service (NTIS) AD A 017676. The original program used Unix system functions to produce the random numbers needed by the password generator. These functions were replaced with a DES-based random number subroutine that uses DES in the Electronic Code Book (ECB) mode. As input, DES uses the old password or user supplied character string, and a pseudorandom key created in accordance with the procedure described in Appendix C of ANSI X9.17. Any change to either the key or input

data string causes DES to generate an entirely different random number. Every time this occurs the password generator creates a new random password.

2.0 TECHNICAL EXPLANATION

The Automated Password Generator standard is organized as a main procedure that references three major components: (1) the "unit table"; (2) the "digram table"; and (3) the "random number subroutine." The random password generator works by forming pronounceable syllables and concatenating them to form a word. Rules of pronounceability are stored in a table for every unit and every pair of units (digram). The rules are used to determine whether a given unit is legal or illegal, based on its position within the syllable and adjacent units. Most rules and checks are syllable oriented and do not depend on anything outside the current syllable. The main procedure (algorithm) defines the internal rules used to generate random words. The three components and the algorithm are described below.

Appendix A is the code for the NIST implementation of the Automated Password Generator standard. This code consists of the C-code version of the program described in "A Random Word Generator For Pronounceable Passwords," the code that comprises the DES random number subroutine, the actual DES subroutine, and the code for generating the pseudorandom key. Implementations in other programming languages are acceptable, however, the results obtained must be logically equivalent to those produced by this standard.

In the NIST implementation of the password generator, the values selected for the two DES keys and the seed for the random number generator are readable in the code (Appendix A). In an actual vendor or user developed implementation the values of the keys and the seed would be secret, randomly generated values set by the application.

2.1 Unit Table

The unit table defines the units (alphabetic characters) and specifies rules pertaining to the individual units used in a randomly generated word. For example, the location of vowels in the words generated is determined by these rules. The unit table used in the Automated Password Generator standard is identical to that furnished in the report "A Random Word Generator For Pronounceable Passwords" (item i in Cross Index).

2.2 Digram Table

The digram table specifies rules about all possible pairs of units and the juxtaposition of units. The table contains one entry for every pair of units (digram), whether that pair is allowed or not. The random word generator ensures that the rules specified in the digram table are satisfied for every two

consecutive units in the word being formed. The digram table is also from the original report.

2.3 Random Number Generator Subroutine

The random number generator uses a DES subroutine to produce double precision floating point values between 0 and (excluding) 1. These numbers are multiplied by a program variable n which is an integer value. This operation yields a random integer between 0 and (n-1) inclusive. The random numbers created by the DES routine serve as input to the random word generator. The subroutine to generate these numbers is called by the word generator each time a character (unit) is needed.

Not all characters generated will be acceptable to the word generator in every position of the word. Each character is checked for appropriateness using the rules defined by the unit and digram tables. Therefore the random number generator subroutine will be repeatedly called until an acceptable character is returned. An upper limit of 100 calls is placed on generating any particular character. If that number is reached the whole word is discarded and the program starts over.

The actual distribution of legal units is different for every position in a particular word which, for any unit, depends on the units that precede it as well as the units and digram tables. The random number subroutine itself makes no tests for legal units.

As its input DES accepts two 64 bit data blocks. One consists of the old password or a data string; the other is a 64 bit (56 bits + 8 parity bits) pseudorandom key derived using the procedure described in Appendix C of ANSI X9.17. The old password is entered manually from the keyboard. An input array is created from the first eight bytes of the password or input string. The program will accept a null string (carriage return). All characters past the eighth are disregarded. If the input block is less than eight characters long the extra elements in the input array are filled with ASCII 0. The Electronic Codebook (ECB) mode of DES described in FIPS 81 ("DES Modes of Operation," December 2, 1980) is then used to encrypt the input data. The output is a 64-bit random number which is the encrypted form of the input. The first function in the DES structure is setkey(), which converts the pseudorandom key to a format used by DES for the encryption. The command-line options sent to setkey are (0, 0, key). The first 0 is set so that setkey() does not generate parity; the second 0 tells setkey() that encryption (rather than decryption) is required. Key is a pointer to the beginning of the key array. After setkey(), the des() function is called. For input it uses the addresses of the input and output arrays. Both input and output are defined as unsigned character arrays of length 8 bytes.

The output array, out, is sent to a function, answer(), which returns the final required number. The function answer() takes in the address of the output array as an unsigned char pointer and the integer n for which a value of 0 to (n-1) is needed by the random word program. This function creates a variable sum, defined as an unsigned integer. To obtain a numerical value from the output character array, it adds the ASCII values of the first three elements in the out array and stores the sum in the variable sum. Thus, sum = out[0] + out[1] + out[2], which is an integer. To obtain a number with the required range of 0 to n-1 from sum, the function takes the modulus of sum and n, (sum%n). This value is then returned to the calling function within the random word program.

2.4 Random Word Algorithm

The algorithm used to generate random words is fixed and cannot be modified without changing the logic of the program. The function of the algorithm is to determine whether a given unit, generated by the random unit subroutine, can be appended to the end of the partial word formed so far. Rules of pronounceability are stored in the unit and digram tables discussed above. The rules are used to check if a given unit is legal or illegal. If illegal, the unit is discarded and the random unit subroutine is called again. Once a unit is accepted, various state variables are updated and a unit for the next position in the word is tried. Most rules and checks are syllable oriented and do not depend on anything outside the current syllables. When the end of the word is reached, additional checks are made before the algorithm terminates.

Passwords created by this automated password generator are composed of the 26 characters of the English alphabet. Although numbers and special characters are not permitted, the password space, which is a function of the number of characters in the password, is very large. Approximately 18 million 6-character, 5.7 billion 8- character, and 1.6 trillion 10-character passwords can be created by the program. Users should select a password space commensurate with the level of security required for the information being protected.

The password algorithm does not preclude the generation of words found in a standard English dictionary. If required, a computerized dictionary could be used to check for English words, and the implementation could include software tests to prevent them from being offered to users as passwords.

2.5 NIST Implementation

Figure 1 is a block diagram of the NIST implementation of the automated password generation algorithm. Appendix A contains the C-code for the DES, random key generation, and random word generation routines that were used in the implementation (see shaded boxes in Fig. 1). The personal computer used by NIST to demonstrate the standard is implementation dependent. NIST replaced the Unix random number routine in the original version of the program with the

"DES Randomizer" and "Generate Random Key" function. The DES randomizer accepts an old password and a pseudorandom key created in accordance with Appendix C of ANSI X9.17 (FIPSPUB 171) and generates a random number. This number is used by the Random Word Generator to develop a password. As the password is being generated each group of letters is subjected to tests of grammar and semantics to determine if an acceptable word has been created. If all tests are passed, the new password is output to the PC.

In the NIST implementation, the values for minlen and maxlen, which define the minimun and maximum size of the password, were set at 5 and 8 respectively. A user needing a fixed length password word could set these variables to a specific value.

Appendix A

This section contained a listing of the source code referenced in the Automated Password Generator Standard. This section is not available in electronic form.

Complete copies of FIPS 181, including this appendix, may be purchased in hardcopy from the National Technical Information Service (NTIS) via mail or telephone.

National Technical Information Service U.S. Department of Commerce 5285 Port Royal Road Springfield, VA 22161 (703) 487-4650

Order by FIPSPUB181 Price: $22.50

(Same address and phone number for discount prices on quantity orders.)