June 1990

NCSL Bulletin

Advising users on computer systems technology

This *NCSL Bulletin* initiates a new publication series at the National Computer Systems Laboratory (NCSL). Each bulletin will present an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins will be issued on an as-needed basis and are available from NCSL Publications, National Institute of Standards and Technology, Room B151, Technology Building, Gaithersburg, MD 20899, telephone (301) 975-2821 or FTS 879-2821.

DATA ENCRYPTION STANDARD

Introduction

The National Computer Systems Laboratory (NCSL) of the National Institute of Standards and Technology (NIST) has received many inquiries related to the Data Encryption Standard (DES). This *NCSL Bulletin* addresses those frequently asked questions and provides sources of additional information. This document does not issue new policy; rather, it summarizes and clarifies existing policies.

Background

NIST (formerly the National Bureau of Standards) issued Federal Information Processing Standard (FIPS) 46 in 1977 to provide a system for the cryptographic protection of the confidentiality and integrity of federal sensitive unclassified computer information. DES has been reviewed and reaffirmed twice, most recently in 1988. The current standard, which was issued as FIPS 46-1, reaffirms the standard until 1993. The DES algorithm is based on work of the International Business Machines Corporation and has been adopted as American National Standard X3.92-1981/R1987.

Technical Overview

The Data Encryption Standard specifies a cryptographic algorithm that converts plaintext to ciphertext using a 56-bit key. The same algorithm is used with the same key to convert ciphertext back to plaintext, a process called decryption. The DES algorithm consists of 16 "rounds" of operations that mix the data and key together in a prescribed manner using the fundamental operations of permutation and substitution. The goal is to completely scramble the data and key so that every bit of the ciphertext depends on every bit of the data plus every bit of the key (a 56-bit quantity for DES).

Security Provided by DES

The security provided by a cryptographic system depends on several factors: mathematical soundness of the algorithm, length of the keys, key management, mode of operation, and implementation.

DES was developed to protect unclassified computer data in federal computer systems against a number of passive and active attacks in communications and computer systems. It was assumed that a knowledgeable person might seek to compromise the security system by employing resources commensurate with the value of the protected information. Appropriate applications of DES include Electronic Funds Transfer, privacy protection of personal information, personal authentication, password protection, access control, etc.

DES has been evaluated by several organizations and has been determined to be mathematically sound. Some individuals have analyzed the DES algorithm and have concluded that the algorithm would not be secure if a particular change were made (e.g., if fewer "rounds" were used). Modifications of this sort are not in accordance with the standard and, therefore, may provide significantly less security.

NIST believes that DES provides more than adequate security for its intended unclassified applications and plans to continue its support of the standard. It is currently the only cryptographic standard approved in the federal government to protect unclassified computer information (except for a special category of information described below). The next review of DES is scheduled for 1993. NIST plans to augment DES with other cryptographic algorithms to form a family of standards that will provide new types of protection in special applications.

Applicability

Subject to agency waivers as discussed below, **use of DES is mandatory for all federal agencies**, including defense agencies, for the protection of sensitive unclassified information **when the**

agency or department determines that cryptographic protection is required.

The National Security Agency (NSA) of the U.S. Department of Defense develops and promulgates requirements for telecommunications and automated information systems operated by the U.S. government, its contractors, or agents, that contain classified information or, as delineated in 10 U.S.C. Section 2315, the function, operation, or use of which:

—involves intelligence activities;

—involves cryptologic activities —related to national security;

—involves the direct command and control of military forces;

—involves equipment which is an integral part of a weapon or weapon systems; or

—is critical to the direct fulfillment of a military or intelligence mission.

Who we are

NCSL is one of five major science and engineering research components of the National Institute of Standards and Technology (NIST) of the Department of Commerce. We develop standards and test methods, conduct research on computer and related telecommunications systems, and provide technical assistance to government and industry. We seek to overcome barriers to the efficient use of computer systems, to the cost-effective exchange of information, and to the protection of valuable information resources in computer systems from threats of all kinds.

James H. Burrows, Director

Note that the term unclassified information as used in this document excludes information covered by 10 U.S.C. 2315.

DES may be used by private-sector individuals or organizations at their discretion.

Waivers for the Mandatory Use of DES

The head of a federal department or agency may waive the use of DES for the protection of unclassified information in accordance with the provisions of FIPS 46-1, section 17, page 4, as discussed below:

"A waiver is necessary if cryptographic devices performing an algorithm other than that which is specified in this standard are to be used by a federal agency for data subject to cryptographic protection under this standard. No waiver is necessary if classified communications security equipment is to be used. Software implementations of this algorithm for operational use in general purpose computer systems do not comply with this standard and each such implementation must also receive a waiver. Implementation of the algorithm in software for testing or evaluation does not require waiver approval. Implementation of other special purpose cryptographic algorithms in software for limited use within a computer system (e.g., encrypting password files) or implementation of cryptographic algorithms in software which were being utilized in computer systems before the effective date of this standard do not require a waiver. However, these limited uses should be converted to the use of the standard when the system or equipment involved is upgraded or redesigned to include general cryptographic protection of computer data. Waivers will be considered for devices certified by the National Security Agency as complying with the Commercial COMSEC Endorsement Program (CCEP) when such devices offer equivalent cost/performance features when compared with devices conforming to this standard."

Waiver Procedures

As mentioned above, the heads of federal departments or agencies may waive the mandatory use of DES. This authority may be redelegated only to a senior official designated pursuant to 44 U.S.C. section 3506(b). Waivers shall be granted only when:

-compliance with the standard would adversely affect the accomplishment of the mission of an operator of a federal computer system; or

-compliance would cause a major adverse financial impact on the operator which is not offset by governmentwide 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
Attention: FIPS Waiver Decisions
Technology Building, Room B-154
Gaithersburg, MD 20899

In addition, notice of each waiver granted and each delegation of authority shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental 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 or accompanying documents, with such deletions as the agency is authorized and decides to make under 5 U.S.C. Section 552(b), shall be part of the procurement documentation and retained by the agency.

Endorsement of DES Products

DES products for use in telecommunications equipment and systems are no longer being endorsed by NSA for conformance to FIPS 140, General Security Requirements for Equipment Using the Data Encryption Standard, (formerly Federal Standard 1027). Federal agencies may purchase FIPS 140 products that have not been validated under the NSA endorsement program without processing a waiver. To do so, agencies must require written affirmation from vendors that their products are in conformance with the provisions of the current standard.

Also, NIST has notified the heads of federal departments that they may wish to consider waiving certain requirements of FIPS 140 in order to buy equipment which may not meet all of the criteria in the standard. This action will enable agencies to procure cost-effective equipment that meets their needs, but has not been endorsed by NSA.

FIPS 140 is currently under revision to be reissued as FIPS 140-1. All issues contained within the scope of the original standard are being readdressed. NIST is also examining various methods for conducting conformance testing against the requirements of FIPS 140-1.

DES Cryptographic Keys

U.S. government users of DES products which have been endorsed by NSA under Federal Standard 1027 may obtain DES cryptographic keys for these products from NSA upon request at no cost. (Note that NSA is no longer endorsing products under Federal Standard 1027.) Contact your responsible Communications Security (COMSEC) officer for further information.

Alternatively, users of DES, including federal organizations, may generate their own cryptographic keys. DES keys must be properly generated and managed in order to assure a high level of protection to computer data. Key Management includes generation, distribution, storage, and destruction of cryptographic keys. Information on this subject may be obtained from the following documents: FIPS 74, FIPS 140-1 (future), and ANSI X9.17. (See reference list for availability of the documents.)

Exportability of DES Devices and Software Products

Hardware- and software-based implementations of DES are subject to federal export controls as specified in Title 22, Code of Federal Regulations (CFR), Parts 120 - 128, the International Traffic in Arms Regulations (ITAR). Specific information regarding export applications, application procedures, types of licenses, and necessary forms may be found in the CFR. Responsibility for granting export licenses (except for those DES implementations noted below) rests with:

Office of Munitions Control
Bureau of Politico-Military Affairs
U.S. Department of State
Washington, DC, 20250
Telephone: (202) 875-6650

The Office of Munitions Control, U.S. Department of State, issues either individual or distribution licenses. Under a distribution license, annual reports must be submitted by the distributor describing to whom the licensed products have been sold. License requests for products to be shipped to certain prohibited countries (see Section 126.1 of the ITAR) are denied for foreign policy reasons by the Department of State.

Licenses are normally granted if the end users are either financial institutions or American subsidiaries abroad. In general, either individual or distribution licenses may be used for financial institutions while only individual licenses may be used for subsidiaries of U.S. corporations.

Specific Cryptographic Implementations under Jurisdiction of the Department of Commerce

The Bureau of Export Administration, U.S. Department of Commerce, is responsible for the granting of export licenses for the following categories of cryptographic products (including DES):

Authentication. Software or hardware which calculates a Message Authentication Code (MAC) or similar result to assure no alteration of text has taken place, or to authenticate users, but does not allow for encryption of data, text, or other media other than that needed for the authentication.

Access Control. Software or hardware which protects passwords or Personal Identification Numbers (PIN) or similar data to prevent unauthorized access to computing facilities, but does not allow for encryption of files or text, except as directly related to password or PIN protection.

Proprietary Software Protection. Decryption-only routines for encrypted proprietary software, fonts, or other computer-related proprietary information for the purpose of maintaining vendor control over said information when such decryption routines are not accessible to users of said software, font, or other information, and cannot be used for any other purpose.

Automatic Teller Devices. Devices limited to the issuance of cash or traveler's checks, acceptance of deposits, or account balance reporting.

Vendors of products in the above four categories should contact the following for a product classification determination:

Bureau of Export Administration
U.S. Department of Commerce
P.O. Box 273
Washington, DC 20044
Telephone: (202) 377-0708

Following this determination, the vendor will be informed whether an export license from the U.S. Department of Commerce is necessary. The Bureau of Export Administration will provide vendors with license procedures and further information as appropriate.

Please note that vendors whose products do not fall clearly into the above categories should follow procedures set forth in the ITAR, 22 CFR 120-130.

Validation of Devices for Compliance with FIPS 46 and 113

NIST performs validations of products for compliance with FIPS 46 and 113. For further information about submitting products for validation or to obtain a list of devices validated under either standard, please contact:

Manager, Security Technology Group
Computer Security Division
National Computer Systems Laboratory
Building 225, Room A216
National Institute of Standards and Technology
Gaithersburg, MD 20899
Telephone (301) 975-2920

Reference Documents

NIST Documents

NIST has issued FIPS and other publications regarding DES, its implementation, and modes of operation.

FIPS 46-1, *Data Encryption Standard*

This standard provides the technical specifications for DES.

FIPS 74, *Guidelines for Implementing and Using the NBS Data Encryption Standard*

This guideline on DES discusses how and when data encryption should be used, various encryption methods, the reduction of security threats, implementation of DES, and key management.

FIPS 81, *DES Modes of Operation*

FIPS 81 defines four modes of operation for DES which may be used in a wide variety of applications. The modes specify how data will be encrypted and decrypted. The four modes are: (1) Electronic Codebook (ECB), (2) Cipher Block Chaining (CBC), (3) Cipher Feedback (CFB), and (4) Output Feedback (OFB).

FIPS 113, *Computer Data Authentication*

This standard specifies a Data Authentication Algorithm, based upon DES, which may be used to detect unauthorized modifications, both intentional and accidental, to data. The Message Authentication Code as specified in ANSI X9.9 is computed in the same manner as the Data Authentication Code as specified in this standard.

FIPS 139, *Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical Layer of Data Communications*

This standard specifies interoperability and security-related requirements for using encryption at the Physical Layer of the ISO Open Systems Interconnection (OSI) Reference Model in telecommunications systems conveying digital information. FIPS 139 was previously issued by the

General Services Administration as *Federal Standard 1026*.

FIPS 140, *General Security Requirements for Equipment Using the Data Encryption Standard*

This document establishes the physical and logical security requirements for the design and manufacture of DES equipment. FIPS 140 was previously issued by the General Services Administration as *Federal Standard 1027*.

FIPS 141, *Interoperability and Security Requirements for Use of the Data Encryption Standard With CCITT Group 3 Facsimile Equipment*

This document specifies interoperability and security related requirements for use of encryption with the International Telegraph and Telephone Consultative Committee (CCITT), Group 3-type facsimile equipment.

NBS Special Publication 500-20, *Validating the Correctness of Hardware Implementations of the NBS Data Encryption Standard*

This publication describes the design and operation of the testbed that is used for the validation of hardware implementations of DES. A particular implementation is verified if it correctly performs a set of 291 test cases that have been defined to exercise every basic element of the algorithm.

NBS Special Publication 500-27, *Computer Security and the Data Encryption Standard*

This publication contains the proceedings of the Conference on Computer Security and the Data Encryption Standard held at the National Bureau of Standards on February 15, 1977. Subjects of the papers and presentations include physical security, risk assessment, software security, computer network security, applications and implementation of the Data Encryption Standard.

NBS Special Publication 500-54, *A Key Notarization System for Computer Networks*

This document describes a system for key notarization, which can be used with an encryption device, to improve data security in computer networks. The key notarization system can be used to communicate securely between two users, communicate via encrypted mail, protect personal files, and provide a digital signature capability.

NBS Special Publication 500-61, *Maintenance Testing for the Data Encryption Standard*

This special publication describes the design of four maintenance tests for the Data Encryption Standard. The tests consist of an iterative procedure that tests the operation of DES devices using a small program and minimal data. The tests are defined as four specific stopping points in a general testing process and satisfy four testing requirements of increasing degree of completeness depending on the thoroughness of testing desired.

NBS Special Publication 500-156, *Message Authentication Code (MAC) Validation System: Requirements and Procedures*

This special publication describes a Message Authentication Code (MAC) Validation System (MVS) to test message authentication devices for conformance to two data authentication standards: FIPS 113 and ANSI X9.9-1986, *Financial Institution Message Authentication (Wholesale)*. The MVS is designed to perform automated testing on message authentication devices which are remote to NIST. This publication provides brief overviews of the two data authentication standards and introduces the basic design and configuration of the MVS. The requirements and administrative procedures to be followed by those seeking formal NIST validation of a message authentication device are presented.

Copies of these publications are for sale by the National Technical Information Service, at:

National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161
Telephone (703) 487-4650,
FTS: 737-4650

Other Documents

DES has been incorporated into a number of other standards, including:

"American national standard for financial institution key management (wholesale)," ANSI X9.17-1985, American Bankers Association, 10 Jay Gould Ct., Waldorf, MD 20602.

"American national standard for financial institution message authentication," ANSI X9.9-1986 (Revised), American Bankers Association, 10 Jay Gould Ct., Waldorf, MD 20602.

"American national standard for financial message encryption," ANSI X9.23-1988, American Bankers Association, 10 Jay Gould Ct., Waldorf, MD 20602.

"American national standard for information systems - Data encryption algorithm - Modes of operation," ANSI X3.106-1983, American National Standards Insti-

tute, 1430 Broadway, New York, NY 20018.

"American national standard for information systems - Data link encryption," ANSI X3.105-1983, American National Standards Institute, 1430 Broadway, New York, NY 20018

"American national standard for personal identification number (PIN) Management and Security," ANSI X9.8-1982, American Bankers Association, 10 Jay Gould Ct., Waldorf, MD 20602.

"American national standard for retail message authentication," ANSI X9.19-1985, American Bankers Association, 10 Jay Gould Ct., Waldorf, MD 20602.

"Banking - Key management (wholesale)," IS 8732, Association for Payment Clearing Services, London, England, Dec. 1987.

"Banking - Requirements for message authentication (wholesale)," IS 8730, Association for Payment Clearing Services, London, England, July 1987.

"Data encryption algorithm," ANSI X3.92-1981, American National Standards Institute, 1430 Broadway, New York, NY 20018.

"Draft American national standard for financial institution sign-on authentication for wholesale financial systems: Secure transmission of personal authenticating information and node authentication," ANSI X9-26-199_, American Bankers Association, 10 Jay Gould Ct., Waldorf, MD 20602.

Related Documents

"The Data Encryption Standard: Past and Future," Smid and Branstad, *Proceedings of the IEEE,* Vol. 76, No. 5, May 1988.

NIST's Computer Security Program

For further information regarding other aspects of NIST's computer security program, including NIST's federal agency assistance program, please contact:

Computer Security Division
National Computer Systems Laboratory
Building 225, Room A216
National Institute of Standards and Technology
Gaithersburg, MD 20899
Telephone (301) 975-2934

U.S. DEPARTMENT OF COMMERCE

National Institute of Standards and Technology
Bldg. 225/B151
Gaithersburg MD 20899

Official Business
Penalty for Private Use $300

BULK RATE
POSTAGE & FEES
PAID
NIST
PERMIT NO G195