SECURITY ISSUES IN THE USE OF ELECTRONIC DATA INTERCHANGE

COMPUTER SYSTEMS LABORATORY BULLETIN
June 1991

CSL recognizes that the development of EDI standards is continuing. This CSL Bulletin provides initial information to federal agencies. Agencies should consider developments of supporting standards, particularly in the area of cryptography, and plan accordingly so that the integration of future technology developments is not precluded in the design of system architectures. As developments warrant, additional information from NIST will be issued.

Introduction

Electronic data interchange (EDI) is becoming an accepted business technology for participating in today's global market. Within the federal government, EDI holds great promise for improving the quality and efficiency of government programs and services. However, this technology will not be implemented in a risk-free environment. Federal agencies must assure that full consideration is given to the security issues inherent in the use of computers and telecommunications to accomplish traditional paper-based administrative functions. Such processes have traditionally been the targets of fraud and other criminal threats. The use of EDI technology also introduces new threats that can adversely effect the confidentiality and integrity of data and the continuity of critical administrative operations.

Purpose. The purpose of this document is to provide initial information to federal departments and agencies on security issues in the use of EDI. It also identifies existing computer security policies and standards applicable to federal EDI systems. This CSL Bulletin describes security controls that can be utilized in existing EDI applications and enumerates future technical security features that will provide additional levels of control in new EDI applications. The bulletin is not intended to serve as a comprehensive guide to the selection of security controls.

Background. EDI is the computer-to-computer interchange of messages representing business documents. The primary application of EDI in the federal government is procurement of goods or services, including such activities as the receipt of bids and the issuance of purchase orders. Vendor payments via electronic funds transfer (EFT) may be combined with notification of payment via EDI. Additional EDI applications that may be implemented are associated with agency responsibilities for data collection, or data interchange with other governments or private-sector organizations. Examples of other potential applications are in law enforcement, regulation of commercial activities, and tax collection.

EDI is an important component of continuing initiatives within the Executive Branch to improve the effectiveness and efficiency of government programs through the use of electronic information systems technology. However, introduction of this technology will be accompanied by a commensurate change in internal control and security risk environments. EDI applications are based upon the use of existing computer technology. The security problems inherent in the use of this technology are well documented in numerous studies, General Accounting Office reports, and criminal court proceedings.

Authority. The Computer Security Act of 1987 assigns to NIST responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive but unclassified information in federal computer systems.

Overview of Current EDI Security Policies and Standards

Activities

EDI is being implemented in an integrated government and voluntary industry standards policy framework. There are several existing government-wide computer security policies that apply to the full spectrum of sensitive federal government computer applications. In the voluntary industry standards world, there is an evolving set of technical standards that govern the formatting and transmission of electronic messages between data interchange partners. In the United States, the X12 standards committee, accredited by the American National Standards Institute, is

developing the X12 family of EDI standards. Internationally, the United Nations Economic Commission for Europe is developing the closely related family of standards called EDIFACT (for EDI for Administration, Commerce, and Trans-port). Both development groups are considering the need for security services in connection with transmissions based on the use of their standards. The X12 and EDIFACT standards recently have been adopted for federal use through FIPS PUB 161, Electronic Data Interchange (EDI).

Federal Computer Security and Related Policies Applicable to EDI.

Applicable security policies include:

- The Computer Security Act of 1987. This law requires federal departments and agencies to identify those computer systems that contain sensitive information and to develop a security plan for those systems. Requirements for agencies for EDI systems include:
  - Identification of those EDI systems that are "sensitive";
  - Preparation and maintenance of security plans for sensitive systems;
  - Conduct of security training for employees involved in the development and operation of EDI systems.
- Appendix III, OMB Circular A-130, "Security of Federal Automation Information Systems." Several elements of this omnibus government-wide computer security policy are directly applicable to EDI:
  - The applications security requirements that include definition of security specifications; security testing to assure proper implementation of security controls; and management certification of the adequacy of security safeguards;
  - The accomplishment of periodic security reviews or audits for sensitive applications;
  - The preparation of contingency plans to assure the continuity of essential information processing services.
- Federal Managers Fiscal Integrity Act and OMB Circular A-123. These documents require that periodic internal control reviews be accomplished over the management of information technology installations. Significant deficiencies identified by federal agencies are to be reported as material internal control weaknesses.
- Requirements for the Management of Electronic Records recently issued by the National Archives and Records Administration (NARA) as 36 CFR Part 1234. This regulation mandates an effective electronic records security program, and states that electronic records may be admitted in evidence in federal court proceedings if trustworthiness is established by thorough documentation of the recordkeeping system's operations and the controls imposed upon it.
- OMB Circular A-127. This circular prescribes policies and procedures to be followed by executive departments and agencies in developing, operating, evaluating, and reporting on financial management systems.

EDI Security Exposures and Issues

Risks in EDI. EDI is typically used to convey information electronically between computers of different organizations. With EDI, information concerning predetermined subject matter that could be conveyed on paper is transferred as a set of electronic messages in standardized formats. The information may remain in electronic form and never be printed. The lack of hard-copy records and manual signatures creates new risks that must be carefully considered in any EDI implementation.

Specific Vulnerabilities of EDI. In the use of EDI, many paper documents are eliminated. As a result, original hard-copy evidence of obligation or commitment by the government, its bidders or contractors, or its other data interchange partners, may not be available. Instead, electronic records must be used. EDI messages become electronic records as they are prepared for transmission and when they are received. Specific activities must be undertaken to assure that EDI messages, as electronic records, are authentic, are properly authorized, and are completely and accurately retained with audit trails for purposes of accountability. Additionally, EDI messages, while being communicated or stored as records, must be protected from loss, modification, or unauthorized disclosure.

EDI Security Requirements

Message Integrity. Both parties to a data interchange want reasonable assurance that the critical information included in a message when composed is unchanged when received. The concern for potential loss requires that, if an action is to be taken as the result of a message, the action is taken on the basis of correct data. In addition, if a message that will cause an action to be taken is sent just once, it may be important that the message be recorded as being received just once (unless a repeat for clarity is understood), in order to prevent an incorrect, duplicate action.

Confidentiality. EDI messages, even if unclassified, may contain personal data, trade-secret data, sensitive financial data, or other data whose dissemination must be restricted. Technological and/or procedural methods may be employed to achieve the desired limitations on access.

Originator Authentication. A message recipient will want reasonable assurance that the source of the message is the named originator and not some other entity, as the recipient may intend to commit resources as a result of the message. Additionally, certainty of the source is particularly important if the purpose of the message is to bind the originator to the data presented in the message or to obligate the originator to undertake an action.

Non-Repudiation. This stronger form of authentication, when in use, assures that one of the two parties to a data interchange cannot falsely deny involvement, due to proof that can be offered to a third party. For example, the recipient of a purchase order requiring a significant resource outlay may desire originator non-repudiation. Similarly, a prospective vendor may desire recipient non-repudiation of its bid proposal sent to meet a deadline.

Availability. Contingency plans should be implementable in the case of system failure or degradation, in order to assure timely receipt and processing of data interchanges on a prioritized basis.

Computer Security Planning for EDI

Risk-Based Implementations. In the development of computer security plans for EDI, agencies should allocate resources according to the risk and magnitude of potential harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained or transmitted by the EDI system. In EDI, certain types of messages may be more inherently sensitive than other types. There must be assurance that each price quotation or purchase order is accurate and has been sent from the named originator. Less care would need to be taken with an invoice sent to an agency, if the agency's internal control system were sufficiently robust so that it would reject all non-authentic invoices.

Maintenance of Electronic Records. EDI messages that are transmitted, and those that are received from vendors or bidders, must be included in an agency's system of electronic records. Consistent with and in support of the previously referenced NARA regulation, agencies should ensure that (1) records of EDI interchanges are complete, (2) unauthorized modifications or alterations to records are prevented, (3) all modifications or alterations are automatically recorded in an electronic audit trail, and (4) dates and times of relevant activities are recorded, and are correct and precise.

Audit Trail for Message Authorization. With paper documents that are sent to a recipient, the handwritten signature (or acceptable substitute) of an authorizing officer is usually used to obligate the originator; a notation that the original was signed is often seen on a retained copy. An equivalent must be provided for each EDI message (called a "transaction set" in X12 terminology) used as a replacement. An electronic copy of each transmitted EDI message, together with the proof of approval, should be retained for audit purposes.

Agreements Prior to the Commencement of EDI. Before EDI can begin, certain arrangements may have to be completed with communications carriers and interchange partners. If an organization expects to interchange EDI messages with several different partners, the use of an independently operated value-added network (VAN) may be valuable as a switching mechanism. The VAN receives originators' messages and distributes them to the various recipients. The VAN may also provide store-and-forward services, retaining messages until each recipient's computer is able to receive the messages directed to it. The extensiveness of security procedures and audit trails provided by the VAN should be among the considerations used for VAN selection.

A written agreement with an interchange partner (for example, a contract with a supplier) can be used to establish which specific EDI transaction sets (identifying versions, releases, and options) are to be interchanged. The agreement also may establish the specific security and authentication mechanisms to be used, and the legal acceptability, to the recipient, of the originator's electronic messages. A subset of a complete trading partner

agreement may be used to provide a bidder who is not yet a trading partner with the procedures for electronically responding with an offer to an office that has issued a request for quote. For small purchases, these procedures could be arranged verbally.

Computer Security Techniques for EDI

Security Technology and Internal Control. Technology is just one of the methods for assuring security, which is a major internal control element. Internal controls are the methods and procedures adopted by management to ensure that (a) resource use is consistent with laws, regulations, and policies; (b) resources are safeguarded against waste, loss, and misuse; and © reliable data are obtained, maintained, and fairly disclosed in reports. Requirements for internal control are spelled out in OMB Circular Nos. A-123, A-127, and A-130, and include organizational arrangements such as separation of duties. The cost and complexity of a selected mix of technical and procedural controls should be commensurate with the risk and potential harm.

Physical Security. Physical security includes the people, procedures, and products used to protect the physical aspects of an EDI system against accidental and intentional destruction and unauthorized access to physical resources. Such protection is fundamental to assure the proper performance of internal controls and technical protection features.

Techniques for Message Authorization. A system designed to transmit an EDI message may be programmed so as not to act unless the authorizing individual presents data that matches equivalent data stored in the system. The system should be designed also to prevent any changes to the message after the authorizer has acted. The presented data for authorization may be something known only to the authorizer (e.g., a password), something possessed (for example, an electronically readable key card), or something unique to the individual (such as the configuration of a fingerprint).

General Control Procedures for Authentication and Integrity. The following techniques may be used to assist in assurance of authentication: (1) An acknowledgement may be returned for each message sent. Then, failure of the originator to receive an acknowledgement within a specified time period, or the receipt of an acknowledgement when no message was sent, must be investigated. (2) If both parties use the same VAN (and therefore no VAN interconnection is required), the VAN's message status reports may provide, to the recipient, originator identity and date and time sent, and to the originator, notice of date and time of receipt. Future X12 standards, (i.e., mailbag interconnect, X12.56) or the use of the international message handling system protocol (X.400) extended to EDI (X.435), may provide the basis for the extension of this capability to situations in which a VAN interconnect is required for message delivery. (3) Log-on techniques, both local and VAN, could be reviewed for potential security improvements. See, for example, the techniques described in FIPS PUBS 48, 83, and 112, and NIST Special Publications 500-137 and 500-157. (4) The parties may agree, beforehand, to include certain reference numbers or passwords, known only to themselves, in the bodies of their messages.

The following techniques may be used to assist in assurance of message integrity: (1) The recipient may recalculate and verify real totals and hash totals to protect against altered values of essential parameters such as part numbers, quantities, unit prices, and total prices. (A hash total is a summation for checking purposes of similar fields of a file, such as fields containing part numbers, that would otherwise not be summed.) (2) The parties may agree to repeat back full messages, or the critical parts of messages, instead of just providing functional acknowledgements. (3) To prevent the replay of a message from being treated as another distinct message, and to prevent confusion between similar but different messages, a unique identification code may be included with each message.

For authentication and integrity protection against an active modification of message data, the following section provides applicable information.

Secret-Key Cryptographic Techniques.

Cryptographic techniques for confidentiality, integrity, and authentication should be carefully considered by users of EDI systems, particularly for higher-risk applications. Secret-key techniques are available at this time in approved FIPS for both confidentiality and message integrity. Agencies should determine if cryptographic techniques can be used to provide cost-effective integrity in their specific applications.

The data encryption standard, FIPS PUB 46-1, may be used directly for purposes of confidentiality. The keys used for confidentiality must be different than those used for message integrity. In a network of users desiring

confidentiality, each pair of data interchange partners uses a different key, and no using organization should have knowledge of a key of an interchange pair in which it is not a participant.

The use of a cryptographic technique for message integrity is described in FIPS PUB 113. The publication describes a message authentication code (MAC) that is calculated by the originator from all bits in the message and transmitted with the message. The recipient recalculates the MAC from the received message and compares the calculated MAC against the received MAC. If the calculated and received MACs are the same, then the transmitted and received messages are the same, with an extremely high probability. The use of the MAC is based on both originator and recipient having possession of a secret encryption/decryption key. The technique is derived from FIPS PUB 46-1.

Communication Security Implementations in EDI. Methods for communicating cryptographic operations that have been implemented for message integrity and confidentiality have been developed by accredited standards committee X12. One standard, X12.58, Security Structures, permits the addition of data to a message that informs the recipient whether or not cryptographic techniques for message integrity and/or confidentiality are in use in the message. If a MAC has been calculated by the originator, the value of the MAC is transmitted with the message. A second standard, X12.42, Cryptographic Service Message, provides the basis for the distribution of secret keys among data interchange partners.

Future Cryptographic Techniques. In the future, message confidentiality, integrity, and authentication may be protected with public-key encryption (PKE) or related techniques. With PKE, each party to an interchange has a pair of cryptographic keys, a public key and a private key. The public key is known to all interchange partners, but the private key is known only to its owner. To assure confidentiality, the originator encrypts the message with the recipient's public key, while the recipient's private key is used to decrypt the message. For integrity and authentication, the originator's private key is used to encrypt the message, while the recipient decrypts the message with the originator's public key. A related technique for integrity and authentication requires the originator to calculate and transmit a "digital signature" with the message; the signature, which is unique to the message is verifiable by the recipient. Digital signature techniques are being studied by NIST.

References

Federal Information Processing Standards (FIPS PUB) and Special Publications (Spec. Pub.)

FIPS PUB 46-1, Data Encryption Standard, January 1988.

FIPS PUB 65, Guideline for Automated Data Processing Risk Analysis, August 1979.

FIPS PUB 83, Guideline on User Authentication Techniques for Computer Network Access Control, September 1980.

FIPS PUB 112, Password Usage, May 1985.

FIPS PUB 113, Computer Data Authentication, May 1985.

FIPS PUB 146-1, Government Open Systems Interconnection Profile (GOSIP), April 1991.

FIPS PUB 161, Electronic Data Interchange, March 1991.

NBS Spec. Pub. 500-137, Security for Dial-up Lines, May 1986.

NIST Spec. Pub. 500-157, Smart Card Technology: New Methods for Computer Access Control, September 1988.

Copies of FIPS PUBS and Spec. Pubs. may be ordered from the National Technical Information Service (NTIS), U.S. Department of Commerce, Springfield, VA 22161; (703) 487-4650. When ordering, refer to the specific FIPS PUB number(s) and title(s). Payment may be made by check, money order, or NTIS deposit account.

Consultative Committee on International Telephone and Telegraph (CCITT) Documents CCITT Recommendation X.400 - 1984, Message Handling Systems:

System Model - Service Elements, and related documents in this series.

CCITT Recommendation X.400 - 1988, Message Handling, System, and Service Overview, and related documents in this series.

CCITT Recommendation X.435 - 1991, Message Handling Systems: EDI Messaging System.

The CCITT Recommendations are available from Omnicom, 115 Park Street, SE, Vienna, VA, 22180; (703) 281-1135.

EDI for Administration, Commerce, and Transport (EDIFACT)

Documents

Underlying standards for EDIFACT include:

International Standard ISO 9735: Electronic Data Interchange for

Administration, Commerce and Transport (EDIFACT) - Application

Level Syntax Rules

UN/TDID Trade Data Interchange Directory, which consists of eight components; see FIPS PUB 161 for a complete listing.

Documents defining both X12 and EDIFACT families of standards are available from the Data Interchange Standards Association (DISA) or from a contractor named by DISA. DISA serves as the secretariat for Accredited Standards Committee X12 on EDI and the North American EDIFACT Board (NAEB); the address is 1800 Diagonal Road, Suite 355, Alexandria, VA 22314; (703) 548-7005.

X12 Documents

These documents are developed by the Accredited Standards Committee (X12) on Electronic Data Interchange (ASC X12), accredited by the American National Standards Institute (ANSI).

They include (not a complete list):

X12.22 Data Segment Directory
X12.3 Data Element Dictionary
X12.42 Cryptographic Service Message
X12.5 Interchange Control Structure
X12.56 Interconnect Mailbag Control Structures
X12.58 Security Structures
X12.6 Application Control Structure

For information on availability of X12 documents, see ordering information for EDIFACT documents.