IS 15256 (Part 1) : 2002
ISO 11568-1 : 1994

भारतीय मानक

बैंकिंग — कुंजी प्रबंधन (खुदरा)

भाग 1 कुंजी प्रबंधन का परिचय

Indian Standard

BANKING — KEY MANAGEMENT (RETAIL)

PART 1 INTRODUCTION TO KEY MANAGEMENT

ICS 35.240.40

© BIS 2002

BUREAU OF INDIAN STANDARDS
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI 110002

December 2002

Price Group 6

NATIONAL FOREWORD

This Indian Standard (Part 1) which is identical with ISO 11568-1:1994 'Banking — Key management (retail) — Part 1 : Introduction to key management' issued by the International Organization for Standardization (ISO) was adopted by the Bureau of Indian Standards on the recommendation of the Banking and Financial Services Sectional Committee (MSD 7) and approval of the Management and Systems Division Council.

The text of the International Standard has been approved as suitable for publication as an Indian Standard without deviations. Certain conventions are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

Wherever the words 'International Standard' appear referring to this standard, they should be read as 'Indian Standard'.

In this adopted standard, normative reference appears to the following International Standard for which no Indian Standard exists:

ISO 8908 : 1993 Banking and related financial services — Vocabulary and data elements

This International Standard has since been withdrawn by the International Organization for Standardization (ISO).

In this adopted standard, informative references appear to certain International Standards for which Indian Standards also exist. The corresponding Indian Standards which are to be substituted in their place are listed below along with their degree of equivalence for the editions indicated:

International Standard	*Corresponding Indian Standard*	*Degree of Equivalence*
ISO 7498-2:1989 : Information processing systems — Open systems interconnection — Basic reference model — Part 2: Security architecture	IS 12373 (Part 2):1992/ISO 7498-2:1989 Basic reference model of open systems interconnection for information processing systems : Part 2 Security architecture	Identical
ISO 9564-1:1991 : Banking — Personal identification number management and security — Part 1: PIN protection principles and techniques	IS 15042 (Part 1):2001/ISO 9564-1:1991 Banking — Personal identification number management and security : Part 1 PIN protection principles and techniques	do
ISO 9564-2:1991 : Banking — Personal identification number management and security — Part 2: Approved algorithm(s) for PIN encipherment	IS 15042 (Part 2):2001/ISO 9564-2:1991 Banking — Personal identification number management and security : Part 2 Approved algorithm(s) for PIN encipherment	do

(*Continued on third cover*)

Introduction

ISO 11568 describes procedures for the secure management of the cryptographic keys used to protect messages in a retail banking environment, for instance, messages between an acquirer and a card acceptor, or an acquirer and a card issuer. Key management of keys used in an Integrated Circuit Card (ICC) environment is not covered by ISO 11568 but will be addressed in another ISO standard.

Whereas key management in a wholesale banking environment is characterized by the exchange of keys in a relatively high-security environment, this standard addresses the key management requirements that are applicable in the accessible domain of retail banking services. Typical of such services are point-of-sale/point-of-service (POS) debit and credit authorizations and automated teller machine (ATM) transactions.

Key management is the process whereby cryptographic keys are provided for use between authorized communicating parties and those keys continue to be subject to secure procedures until they have been destroyed. The security of the enciphered data is dependent upon the prevention of disclosure and unauthorized modification, substitution, insertion, or termination of keys. Thus, key management is concerned with the generation, storage, distribution, use, and destruction procedures for keys. Also, by the formalization of such procedures, provision is made for audit trails to be established.

This part of ISO 11568 does not provide a means to distinguish between parties who share common keys. The final details of the key management procedures need to be agreed upon between the communicating parties concerned and will thus remain the responsibility of the communicating parties. One aspect of the details to be agreed upon will be the identity and duties of particular individuals. ISO 11568 does not concern itself with allocation of individual responsibilities; this needs to be considered for each key management implementation.

ISO 9564 and ISO 9807 specify the use of cryptographic operations within retail financial transactions for personal identification number (PIN) encipherment and message authentication, respectively. ISO 11568 is applicable to the management of the keys introduced by those standards. Additionally, the key management procedures may themselves require the introduction of further keys, e.g. key encipherment keys. The key management procedures are equally applicable to those keys.

Indian Standard

BANKING — KEY MANAGEMENT (RETAIL)

PART 1 INTRODUCTION TO KEY MANAGEMENT

1 Scope

This part of ISO 11568 specifies the principles for the management of keys used in cipher systems implemented within the retail banking environment. The retail banking environment involves the interface between a card accepting device and an acquirer and between an acquirer and a card issuer. An example of this environment is described in annex B, and threats associated with the implementation of this standard in the retail banking environment are elaborated in annex C.

This part of ISO 11568 applies both to the keys of symmetric cipher systems, where both originator and recipient use the same secret key(s), and to the secret and public keys of asymmetric cipher systems, unless otherwise stated. The procedure for the approval of cryptographic algorithms used for key management is specified in annex A.

The use of ciphers often involves control information other than keys, e.g., initialization vectors and key identifiers. This other information is collectively called "keying material". Although this part of ISO 11568 specifically addresses the management of keys, the principles, services, and techniques applicable to keys may also be applied to keying material.

This part of ISO 11568 is appropriate for use by financial institutions and other organizations engaged in the area of retail financial services, where the interchange of information requires confidentiality, integrity, or authentication. Retail financial services include but are not limited to such processes as POS debit and credit authorizations, automated dispensing machine and ATM transactions, etc.

2 Normative reference

The following standard contains part of ISO 11568 provisions that, through reference in this text, constitute provisions of this part of ISO 11568. At the time of publication, the edition indicated was valid. All standards are subject to revision, and parties to agreements based upon this part of ISO 11568 are encouraged to investigate the possibility of applying the most recent edition of the standard indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 8908:1993, *Banking and related financial services — Vocabulary and data elements.*

3 Definitions

For the purposes of this part of ISO 11568, the definitions given in ISO 8908 and the following definitions apply.

3.1 cryptographic algorithm : A set of rules specifying the procedures required to perform encipherment and decipherment of data. The algorithm is designed so that it is not possible to determine the control parameters (e.g. keys) except by exhaustive search.

3.2 cryptographic key; key : The control parameter of a cryptographic algorithm that cannot be deduced from the input and output data except by exhaustive search.

3.3 dictionary attack : Attack in which an adversary builds a dictionary of plaintext and corresponding ciphertext. When a match is able to be made between intercepted ciphertext and dictionary-stored ciphertext, the corresponding plaintext is immediately available from the dictionary.

4 Introduction to key management

4.1 Purpose of security

Messages and transactions in a retail banking system contain both cardholder sensitive data and related financial information. The use of cryptography to protect this data reduces the risk of financial loss by fraud, maintains the integrity and confidentiality of the systems, and instills user confidence in business provider/retailer relationships. To this end, system security shall be incorporated into the total system design. The maintenance of security and system procedures over the keys in such systems is called key management.

4.2 Level of security

The level of security to be achieved needs to be related to a number of factors, including the sensitivity of the data concerned and the likelihood that it will be intercepted; the practicality of any envisaged encipherment process; and the cost of providing (and breaking) a particular means of security. It is therefore necessary for communicating parties to agree on the extent and detail of security and key management procedures.

4.3 Key management objectives

The primary objective of key management is to provide the users with those keys that they need to perform the required cryptographic operations and to control the use of those keys. Key management also ensures that those keys are protected adequately during their life cycle. The security objectives of key management are to minimize the opportunity for a breach of security, to minimize the consequences or damages of a security breach, and to maximize the probability of detection of any illicit access or change to keys that may occur, despite preventive measures. This applies to all stages of the generation, distribution, storage, use and archiving of keys, including those processes that occur in cryptographic equipment and those related to communication of cryptographic keys between communicating parties.

NOTE 1 This part of ISO 11568 covers the above issues. Total system security also includes such issues as protecting communications, data processing systems, equipment and facilities.

5 Principles of key management

Compliance with the following principles is required in order to protect keys from threats to subvert a retail banking system :

a) keys shall exist only in those forms permitted by ISO 11568 ;

b) no one person shall have the capability to access or ascertain any plaintext secret key ;

c) systems shall prevent the disclosure of any secret key that has been used to encipher any still-secret data ;

d) systems shall detect the disclosure of any secret key ;

e) systems shall prevent or detect the use of a secret key for other than its intended purpose, and the accidental or unauthorized modification, substitution, deletion or insertion of any key ;

f) secret keys shall be generated using a process such that it is not possible to predict any secret value or to determine that certain values are more probable than others from the total set of all the possible values ;

g) systems should detect the attempted disclosure of any secret key, the attempted use of a secret key for other than its intended purpose, and the unauthorized modification, substitution, deletion or insertion of any key ;

h) a key shall be replaced with a new key within the time deemed feasible to determine the old key ;

i) a key shall be replaced with a new key within the time deemed feasible to perform a successful dictionary attack on the data enciphered under the old key ;

j) a key shall cease to be used when its compromise is known or suspected ;

k) a compromise of a key shared among one group of parties shall not compromise keys shared among any other group of parties ;

l) a compromised key shall not provide any information to enable the determination of its replacement ;

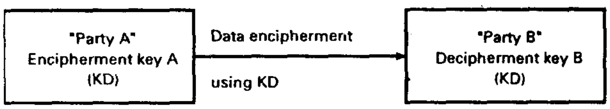
m) a key shall only be loaded into a device when it may be reasonably assured that the device is secure and has not been subjected to unauthorized modification or substitution.

6 Cipher systems

A cipher system comprises an encipherment operation and the inverse decipherment operation. Encipherment transforms plaintext to ciphertext using an encipherment key; decipherment transforms the ciphertext back to plaintext using a decipherment key. Retail banking applications employ cipher systems to protect sensitive cardholder and financial transaction data. The data to be protected is enciphered by the originator and subsequently deciphered by the receiver. There are two types of cipher systems: symmetric and asymmetric.

6.1 Symmetric ciphers

A symmetric cipher is one in which the encipherment key and decipherment key are equal or may be easily deduced from one another. The keys are kept secret at both the originator and recipient locations. Possession of the secret key(s) permits secure communications between the originator and recipient. An example of a symmetric cipher system is shown in figure 1.



NOTE — Encipherment key A = Decipherment key B.

Figure 1 — Example of a symmetric cipher system

A symmetric cipher system itself does not distinguish either end in the system. However, if a symmetric cipher system is implemented with appropriate key management techniques coupled with secure cryptographic devices, it may distinguish each end and support unidirectional key services. If the same set of keys provides protection (e.g. encipherment, authentication, etc.) of secret data transmitted in both directions, it is known as bidirectional keying. When a different set of keys is used for protection of secret data transmitted in each direction, it is known as unidirectional keying.

The key management principles shall be properly applied to ensure the confidentiality, integrity and authenticity of the secret keys.

6.2 Asymmetric ciphers

An asymmetric cipher is one in which the encipherment key and decipherment key are different, and it is computationally infeasible to deduce the decipherment key from the encipherment key. The encipherment key of an asymmetric cipher may be made public while the corresponding decipherment key is kept secret. The keys are then referred to as the public key and the secret key. An example of an asymmetric cipher system is shown in figure 2.

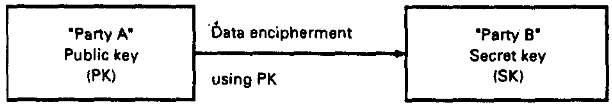


Figure 2 — Example of an asymmetric cipher system

The characteristics of asymmetric cipher systems require that the recipient hold a secret key with which the secret data may be deciphered. A different, non-secret (public) key is used by the originator to encipher the secret data. Thus, asymmetric cipher systems are unidirectional in nature, i.e. a pair of public and secret keys provides protection for data transmitted in one direction only. Public knowledge of the public key does not compromise the cipher system. When protection for data transmitted is required in both directions, two sets of public and secret key pairs are required. One common use for asymmetric ciphers is the secure distribution of initial keys for symmetric cipher systems.

The key management principles shall be properly applied to ensure the confidentiality of the secret key and the integrity and authenticity of both the public and secret keys.

7 Cryptographic environments

For both symmetric and asymmetric cipher systems, the confidentiality of the secret keys and the integrity of both public and secret keys during storage and use depends upon a combination of the following two factors :

a) the security of the hardware device performing the cryptographic processing and storage of the keys and other secret data (as described in 7.1) ; and

b) the security of the environment in which the cryptographic processing and storage of the keys and other secret data occurs (as described in 7.2).

Absolute security is not practically achievable; therefore, key management procedures should implement preventive measures to reduce the opportunity for a breach in security and aim for a "high" probability of detection of any illicit access to secret or confidential data should these preventive measures fail.

7.1 Secure cryptographic device

A secure cryptographic device is a device that provides secure storage for secret information such as keys and provides security services based on this secret information. The characteristics and management of such devices will be addressed in another ISO standard.

7.2 Physically secure environment

A physically secure environment is one that is equipped with access controls or other mechanisms designed to prevent any unauthorized access that would result in the disclosure of all or part of any key or other secret data stored within the environment.

Examples of a physically secure environment are a safe or a purpose-built room with continuous access control, physical security protection, and monitoring.

A physically secure environment shall remain such until all keys or other secret data and useful residue from such secret data have been removed from the environment or destroyed.

7.3 Security considerations for secret keys

Plaintext secret keys shall exist only within a secure cryptographic device or within a physically secure environment.

Plaintext secret key(s) whose compromise would affect multiple parties shall exist only within a secure cryptographic device. Plaintext secret key(s) whose compromise would affect only one party shall exist only within a secure cryptographic device or a physically secure environment operated by, or on behalf of, that party.

7.4 Security considerations for public keys

In principle, there is no need to provide protection to prevent disclosure of public keys. However, physical or logical protection shall be provided to prevent the unauthorized substitution of a public key. In addition to protecting against public key substitution, protection shall be provided to prevent the unauthorized disclosure of any secret data to be enciphered under a public key.

7.5 Protection against counterfeit devices

Protection shall be provided to prevent or detect the legitimate device from being replaced with a counterfeit having, in addition to its legitimate capabilities, unauthorized abilities that might result in the disclosure of secret data prior to encipherment.

8 Key management services for symmetric ciphers

Key management services are employed with symmetric cipher systems to ensure compliance with the key management principles listed in clause 5. These services are briefly described below. (Techniques used to provide these services are addressed in ISO 11568-2).

8.1 Separation

Key separation ensures that cryptographic processing may operate only with the specific functional key types, e.g. message authentication code (MAC) key, for which it was designed. Since keys are input to cryptographic functions in enciphered form, or recalled in clear form from secure storage within the cryptographic device, key separation may be achieved by varying the process under which they are enciphered or stored.

8.2 Substitution prevention

Key substitution prevention prohibits keys that are appropriate for use in a specific function from being used by parties, or at times, other than those for which they are intended, e.g. keys may not be used by an unauthorized party or after the keys have expired.

8.3 Identification

Key identification enables the transaction recipient to determine the appropriate key(s) associated with the transaction.

8.4 Synchronization (availability)

Cryptographic synchronization enables an originator and a recipient to ensure that the appropriate key is used when a key change occurs.

8.5 Integrity

Key integrity is ensured by verifying that the key has not been altered.

8.6 Confidentiality

Key confidentiality ensures that secret keys are never disclosed.

8.7 Compromise detection

In some situations it is not possible or feasible to prevent a security compromise, but adverse results from the compromise may be avoided or limited if the compromise is detected. Security compromises are detected by means of controls and audits.

9 Key life cycle for symmetric ciphers

Key management involves the generation of suitable keys, their distribution to and use by authorized recipients, and their termination once they are no longer required. To protect keys during their lifetime in a manner necessary to comply with the key management principles listed in clause 5, keys are processed through a series of stages, which are briefly described below. This entire procedure is called the key life cycle. (More detailed information on the key life cycle for symmetric ciphers is provided in ISO 11568-3).

9.1 Generation

Key generation involves the creation of a new key for subsequent use.

9.2 Storage

Key storage involves the holding of a key in one of the permissible forms.

9.3 Backup

Key backup occurs when a protected copy of a key is kept in storage during its operational use.

9.4 Distribution and loading

Key distribution and loading is the process by which a key is manually or electronically transferred into a secure cryptographic device.

9.5 Use

Key use occurs when a key is employed for the cryptographic purpose for which it was intended.

9.6 Replacement

Key replacement occurs when one key is substituted for another when the original key is known or suspected to be compromised or the end of its operational life is reached.

9.7 Destruction

Key destruction ensures that an instance of a key in one of the permissible key forms no longer exists at a specific location. Information may still exist at the location from which the key may be feasibly reconstructed for subsequent use.

9.8 Deletion

Key deletion is the process by which an unwanted key, and information from which the key may be reconstructed, is destroyed at its operational storage/ use location. A key may be deleted from one location and continue to exist at another, e.g. for archival purposes.

9.9 Archive

Key archive is the process by which a key that is no longer in operational use at any location is stored.

9.10 Termination

Key termination occurs when a key is no longer required for any purpose and all copies of the key and information required to regenerate or reconstruct the key have been deleted from all locations where they ever existed.

Annex A

(normative)

Procedure for approval of a cryptographic algorithm

The following procedure for approval of a cryptographic algorithm for use with ISO 11568 shall be used by ISO/TC 68.

A.1 Justification of proposal

ISO/TC 68 shall require the originator of the proposed algorithm to justify its proposal by describing :

a) the purpose the proposal is to serve ;

b) how this purpose is equally or better achieved by the proposal than the algorithms already in the standard (the approved algorithms are located in the parts of this standard to which they apply) ;

c) Additional merits not described elsewhere ; and

d) Experience with the new algorithm.

A.2 Documentation

The proposed algorithm shall be completely documented when submitted for consideration. The documentation shall include :

a) a full description of the algorithm proposed ;

b) a clear acknowledgment that the algorithm satisfies, or is compatible with, all the requirements contained in this part of ISO 11568 ;

c) a definition and explanation of any new terms, factors or variables introduced ;

d) a step-by-step example illustrating the encipherment and decipherment computations ; and

e) details of any prior testing to which the proposed algorithm has been subjected, particularly concerning its security, reliability, and stability. Such information should include an outline of the testing procedures used, the results of the tests, and the identity of the agency or group performing the tests and certifying the results (i.e. sufficient information should be provided to enable an independent agency to conduct the same tests and to compare the results achieved).

A.3 Public disclosure

Any algorithm submitted for consideration shall be free of security classification. If copyright or patent application has been made on the algorithm, the originator shall submit the appropriate letter stating that the originator is willing to grant a licence under these copyrights and patents on reasonable and non discriminatory terms and conditions to anyone wishing to obtain such a licence to allow free and unconditional use by testers, users, and suppliers of supporting equipment and material. All documentation and information submitted with the request for consideration of the algorithm shall be considered public information available to any individual, organization or agency for review, testing and usage.

A.4 Examination of proposals

ISO/TC 68 shall examine and prepare a report on each new proposal submitted. The report shall normally be sent to the ISO/TC 68 Secretariat within 180 days of receipt of the proposal. The report shall state if the proposal is adequately documented, if it has been properly tested and certified already, and if the proposed algorithm satisfies the conditions and requirements of this standard. The examination may also include submission of the proposal for public review.

ISO/TC 68 shall determine in each case whether such report and recommendations are best prepared by correspondence between members or by a meeting. If a meeting is to be held, at least 60 days notice of the date shall be given and of the papers to be dealt with at the meeting.

Where the majority of members of ISO/TC 68 recommends the rejection of the proposal, the secretariat shall notify the originator, in writing, advising of the rejection and the reasons for it.

A.5 Public review

ISO/TC68 shall forward proposals that it considers should be accepted (and that have not already been subjected to extensive testing or experience) to selected agencies or institutions with an international reputation in this field. These agencies and institutions will be requested to examine and report on the proposals within 90 days of receipt.

NOTE 2 This period of public review may extend to the 180 days allowed for ISO/TC 68 to prepare its overall report on the proposal.

A.6 Appeal procedure

Originators whose proposals are rejected by ISO/TC 68 may ask the Secretariat of ISO/TC 68 to have the proposals subjected to public review if this has not already been done. If, following the submission of the public review reports, ISO/TC 68 still recommends rejection, the originator may request the ISO/TC 68 Secretariat to circulate the proposal, together with copies of all relevant reports on it, for ballot by primary members of the subcommittee whose ruling in the matter shall be final.

A.7 Incorporation of the new cryptographic algorithm

The new algorithm recommended for acceptance by ISO/TC 68, together with relevant reports on them, shall be circulated for letter ballot by the Secretariat of ISO/TC 68 to all primary members of the subcommittee. Proposals approved as a result of this process shall be forwarded to the Secretariat of ISO/TC 68 for action under the abbreviated procedure to amend an existing standard. Once approval is given, the new algorithm shall be added to ISO 11568.

A.8 Maintenance

An algorithm approved by the method described in this part of ISO 11568 shall be reviewed at intervals not greater than five years.

Annex B

(informative)

Example of a retail banking environment

B.1 Introduction

This annex presents an example of the different parties involved in the retail banking environment. Transaction processing systems are composed of subsystems operated by one or more of these parties.

This example is included to provide additional insight into the key management principles and requirements discussed within this part of ISO 11568. The description has been simplified and may not apply to all national or international environments.

B.1.1 Cardholder and card issuer

The cardholder has a contractual relationship with the card issuer. The card issuer guarantees payment for transactions or services whenever the cardholder identifies himself. The card serves to identify the cardholder and the card issuer. In addition, the card may carry other information such as period of validity (e.g. expiration date) and security related information (e.g. PIN offset). The cardholder and card issuer may agree on the method of issuing the unique, secret PIN (see ISO 9564-1) to be used during transactions. The transaction processing system has an obligation to maintain the PIN secrecy while transporting the transaction of the cardholder between the card acceptor and the card issuer. The card issuer maintains the confidentiality of sensitive cardholder data (e.g. PINs). The card issuer may delegate responsibility for verification of the PIN to an agent.

B.1.2 Card acceptor

The card acceptor is the party that accepts cards as a means of payment for goods or services. In POS systems, this may be a retailer, services company, financial institution, etc. In ATM systems the card acceptor may be the same party as the acquirer. Rather than accepting the card as direct proof of payment, the card acceptor may forward transaction information to an acquirer. The card acceptor takes a transaction authorization from the acquirer as guarantee for payment. The security of the transaction information exchanged with the acquirer is important. Security features may include message authentication (see ISO 9807) and/or encipherment of the PIN.

B.1.3 Acquirer

The transaction acquirer provides transaction processing to card acceptors and card issuers. The acquirer takes responsibility for all or for part of the transaction content according to business arrangements with card issuers or their agents. Thus, for some transactions the acquirer may authorize a transaction acting as agent of a card issuer. In other cases (e.g. the transaction value exceeds a certain threshold), the transaction information is sent to a card issuer or its agent for authorization.

For the acquisition function, the acquirer needs facilities that provide secure processing for translation of enciphered PINs in node-to-node systems, message authentication for transaction exchanges, etc. For combined acquisition and authorization functions, the acquirer needs security facilities to satisfy the requirements of the card issuer that they represent.

B.1.4 Communications provider

The communications provider delivers retail transactions sent from card acceptors to acquirers and card issuers. In some cases, the communication services are limited to data transmission, whereas in other cases more complex conversion facilities are needed. For example, the latter type of services may be offered by a switch in an interchange environment. Such a switch needs security facilities that complement and satisfy the requirements of all business parties involved in the electronic delivery of the transaction. These facilities may provide secure PIN translation, PIN verification, and message authentication.

Annex C

(informative)

Examples of threats in the retail banking environment

C.1 Introduction

This annex presents examples of threats to keys and other secret data in the retail banking environment. These examples are included to provide insight into the need to implement key management schemes to provide data security. The information presented in this annex is drawn from ISO 7498-2:1989, Annex A.

C.2 Threats

Threats to retail banking systems include the following :

a) destruction of information and/or other resources ;

b) corruption, modification or insertion of information ;

c) theft, removal or loss of information and/or other resources ;

d) disclosure of information ; and

e) interruption of services.

Threats may be classified as accidental or intentional and may be active or passive.

C.2.1 Accidental threats

Accidental threats are those that exist with no premeditated intent. Examples of realized accidental threats include system malfunctions, operational blunders and software bugs.

C.2.2 Intentional threats

Intentional threats may range from casual examination using easily available monitoring tools to sophisticated attacks using special system knowledge. An intentional threat, if realized, may be considered an "attack".

C.2.3 Passive threats

Passive threats are those that, if realized, would not result in any modification to any information contained in the system(s) and where neither the operation nor the state of the system is changed. Examples of passive threats that may be realized are the use of passive wiretapping to observe data being transmitted over a communications line, the unauthorized modification (or "bugging") of a device to disclose secret data in the clear, or the substitution of a counterfeit device for a legitimate device, where the counterfeit has the capability to disclose secret data.

C.2.4 Active threats

Active threats to a system involve the alteration of information in the system or changes to the state of operation of the system. Examples of active attacks are a malicious change to the routing tables of a system by an unauthorized user or the fraudulent modification of a "transaction declined" code to a "transaction approved" code.

C.2.4.1 Masquerade

A masquerade is where one party pretends to be a different party. A masquerade is usually used with some form of an active attack such as replay and modification of messages or data. For instance, authentication sequences may be captured and replayed after a valid authentication sequence has taken place. An authorized party with few privileges may use a masquerade to obtain extra privileges by impersonating a party that has those privileges.

C.2.4.2 Replay

A replay occurs when a message, or part of a message, is repeated to produce an unauthorized effect. For example, a valid message containing authentication information may be replayed by another party in order to authenticate itself (as something that it is not).

C.2.4.3 Modification of messages

Modification of a message occurs when the content of a data transmission is altered without detection and results in an unauthorized effect. For example, a message "Allow John Smith to read confidential file named accounts" is changed to "Allow Fred Brown to read confidential file named accounts".

C.2.4.4 Denial of service

Denial of service occurs when a party fails to perform its proper function or acts in a way that prevents other parties from performing their proper functions. The attack may be general, as when a party suppresses all messages directed to a particular destination, such as a security audit service or when a party generates extra traffic. It is also possible to generate messages intended to disrupt the operation of the network, especially if the network has relay parties that make routing decisions based upon status reports received from other relay parties

C.2.4.5 Insider attacks

Insider attacks occur when legitimate users of a system behave in unintended or unauthorized ways. Most known computer crime has involved insider attacks that compromised the security of the system.

C.2.4.6 Outsider attacks

Outsider attacks may use techniques such as :

a) wire tapping (active or passive) ;

b) intercepting emissions ;

c) masquerading as authorized users of the system or the components of the system ;

d) bypassing authentication or access control mechanisms ; and

e) penetrating a cryptographic device to determine the keys stored within it.

C.2.4.7 Trapdoor

A trapdoor is a hidden unauthorized software or hardware mechanism that may be triggered to allow the system security features to be bypassed. The trigger may be an external command (e.g. a special key sequence) or an internal predetermined event (e.g. a counter or date/time value). For example, a password validation program could be modified so that when a specific key sequence is entered, the attacker's password is validated.

C.2.4.8 Trojan horse

When a software program that performs a legitimate function contains a hidden unauthorized function that exploits the legitimate function, the unauthorized function is called a Trojan horse. For example, a program that legitimately copies secret data to a protected file could be modified to also copy the data to a file accessible by the attacker.

Annex D

(informative)

Bibliography

[1] ISO 7498-2:1990, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture.*

[2] ISO 9564-1:1991, *Banking — Personal Identification Number management and security — Part 1: PIN protection principles and techniques.*

[3] ISO 9564-2:1991, *Banking — Personal Identification Number management and security — Part 2: Approved algorithm(s) for PIN encipherment.*

[4] ISO 9807:1991, *Banking and related financial services — Requirements for message authentication (retail).*

[5] ISO 11568-2:1994, *Banking — Key management (retail) — Part 2: Key management techniques for symmetric ciphers.*

[6] ISO 11568-3:1994, *Banking — Key management (retail) — Part 3: Key life cycle for symmetric ciphers.*

(*Continued from second cover*)

In this adopted standard, informative references also appear to the following International Standards, for which no Indian Standards exist:

ISO 9807:1991	Banking and related financial services — Requirements for message authentication (retail)
ISO 11568-2:1994	Banking – Key management (retail) — Part 2: Key management techniques for symmetric ciphers
ISO 11568-3:1994	Banking – Key management (retail) — Part 3: Key life cycle for symmetric ciphers

The Sectional Committee responsible for the preparation of this standard has reviewed the provisions of the above referred standards and has decided that they are acceptable as such for use in conjunction with this standard.

Annex A forms an integral part of this standard. Annexes B, C and D of this standard are for information only.

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 1986 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

BIS has the copyright of all its publications. No part of these publications may be reprodued in any form without the prior permission in writing from BIS. This does not preclude the free use, in the course of implementing the standard, of necessary details, such as symbols and sizes, type or grade designations. Enquiries relating to copyright may be addressed to the Director (Publications), BIS.

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc : No. MSD 7 (244).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters :

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110 002
Telephones : 323 01 31, 323 33 75, 323 94 02

Telegrams : Manaksanstha
(Common to all offices)

Regional Offices :		Telephone
Central	: Manak Bhavan, 9 Bahadur Shah Zafar Marg NEW DELHI 110 002	323 76 17 323 38 41
Eastern	: 1/14 C.I.T. Scheme VI M, V. I. P. Road, Kankurgachi KOLKATA 700 054	337 84 99, 337 85 61 337 86 26, 337 91 20
Northern	: SCO 335-336, Sector 34-A, CHANDIGARH 160 022	60 38 43 60 20 25
Southern	: C.I.T. Campus, IV Cross Road, CHENNAI 600 113	254 12 16, 254 14 42 254 25 19, 254 13 15
Western	: Manakalaya, E9 MIDC, Marol, Andheri (East) MUMBAI 400 093	832 92 95, 832 78 58 832 78 91, 832 78 92
Branches	: AHMEDABAD. BANGALORE. BHOPAL. BHUBANESHWAR. COIMBATORE. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. KANPUR. LUCKNOW. NAGPUR. NALAGARH. PATNA. PUNE. RAJKOT. THIRUVANANTHAPURAM. VISAKHAPATNAM.	

Printed by Dee Kay Printers.