INTERNATIONAL STANDARD

NORME INTERNATIONALE

ISO/IEC 2382-8

Second edition
Deuxième édition
1998-11-01

Information technology — Vocabulary —

Part 8:
Security

Technologies de l'information — Vocabulaire —

Partie 8:
Sécurité

Reference number
Numéro de référence
ISO/IEC 2382-8:1998(E/F)

Contents

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland/Imprimé en Suisse

Sommaire

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 2382-8 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 1, *Vocabulary*.

This second edition cancels and replaces the first edition (ISO 2382-08:1986), which has been technically revised.

ISO/IEC 2382 will consist of some 37 parts, under the general title *Information technology – Vocabulary*.

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment ensemble un système consacré à la normalisation internationale considérée comme un tout. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des différents domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux.

Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour approbation, avant leur acceptation comme Normes internationales. Les Normes internationales sont approuvées conformément aux procédures qui requièrent l'approbation de 75 % au moins des organismes nationaux votants.

La Norme internationale ISO/CEI 2382-8 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 1, *Vocabulaire*.

Cette deuxième édition annule et remplace la première édition (ISO 2382-08:1986), dont elle constitue une révision technique.

L'ISO/CEI 2382 comprendra environ 37 parties, présentées sous le titre général *Technologies de l'information – Vocabulaire*.

Introduction

Information technology gives rise to numerous international exchanges of both an intellectual and a material nature. These exchanges often become difficult, either because of the great variety of terms used in various fields or languages to express the same concept, or because of the absence or imprecision of the definitions of useful concepts.

To avoid misunderstandings and to facilitate such exchanges it is essential to clarify the concepts, to select terms to be used in various languages or in various countries to express the same concept, and to establish definitions providing satisfactory equivalents for the various terms in different languages.

ISO 2382 was initially based mainly on the usage to be found in the *Vocabulary of Information Processing* which was established and published by the International Federation for Information Processing and the International Computation Centre, and in the *American National Dictionary for Information Processing Systems* and its earlier editions published by the American National Standards Institute (formerly known as the American Standards Association). Published and Draft International Standards relating to information technology of other international organizations (such as the International Telecommunication Union and the International Electrotechnical Commission) as well as published and draft national standards have also been considered.

The purpose of ISO/IEC 2382 is to provide definitions that are rigorous, uncomplicated and which can be understood by all concerned. The scope of each concept defined has been chosen to provide a definition that is suitable for general application. In those circumstances, where a restricted application is concerned, the definition may need to be more specific.

However, while it is possible to maintain the self-consistency of individual parts, the reader is warned that the dynamics of language and the problems associated with the standardization and maintenance of vocabularies may introduce duplications and inconsistencies among parts.

Introduction

Les technologies de l'information sont à l'origine de multiples échanges intellectuels et matériels sur le plan international. Ceux-ci souffrent souvent de difficultés provoquées par la diversité des termes utilisés pour exprimer la même notion dans des langues ou des domaines différents, ou encore de l'absence ou de l'imprécision des définitions pour les notions les plus utiles.

Pour éviter des malentendus et faciliter de tels échanges, il paraît essentiel de préciser les notions, de choisir les termes à employer dans les différentes langues et dans les divers pays pour exprimer la même notion, et d'établir pour ces termes des définitions équivalentes dans chaque langue.

L'ISO 2382 a été basée à l'origine principalement sur l'usage tel qu'il a été relevé, d'une part, dans le *Vocabulary of Information Processing* établi et publié par l'International Federation for Information Processing et le Centre international de calcul et, d'autre part, dans l'*American National Dictionary for Information Processing Systems* y compris ses éditions précédentes publiées par l'American National Standards Institute (connu auparavant sous l'appellation d'American Standards Association). Les Normes internationales publiées ou au stade de projets concernant les technologies de l'information émanant d'autres organisations internationales (telles que l'Union internationale des télécommunications et la Commission électrotechnique internationale) ainsi que les normes nationales publiées ou au stade de projets, ont également été prises en compte.

Le but de l'ISO/CEI 2382 est de procurer des définitions rigoureuses, simples et compréhensibles pour tous les intéressés. La portée de chaque notion a été choisie de façon que sa définition puisse avoir la valeur la plus générale. Cependant, il est parfois nécessaire de restreindre une notion à un domaine plus étroit et de lui donner alors une définition plus spécifique.

D'autre part, si l'on peut assurer la cohérence interne de chaque partie prise individuellement, la cohérence des diverses parties entre elles est plus difficile à atteindre. Le lecteur ne doit pas s'en étonner: la dynamique des langues et les problèmes de l'établissement et de la révision des normes de vocabulaire peuvent être à l'origine de quelques répétitions ou contradictions entre des parties qui ne sont pas toutes préparées et publiées simultanément.

Information technology — Vocabulary —

Part 8: Security

Section 1: General

1.1 Scope

This part of ISO/IEC 2382 is intended to facilitate international communication in information technology. It presents, in two languages, terms and definitions of selected concepts relevant to the field of information technology and identifies relationships among the entries.

In order to facilitate their translation into other languages, the definitions are drafted so as to avoid, as far as possible, any peculiarity attached to a language.

This part of ISO/IEC 2382 defines concepts related to protection of data and information, including, cryptography, information classification and access control, recovery of data and information, and security violation.

1.2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 2382. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 2382 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 1087:1990, *Terminology – Vocabulary.*

ISO 3166-1:1997, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes.*

ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*

Technologies de l'information — Vocabulaire —

Partie 8: Sécurité

Section 1: Généralités

1.1 Domaine d'application

La présente partie de l'ISO/CEI 2382 a pour objet de faciliter les échanges internationaux dans le domaine des technologies de l'information. À cet effet, elle présente un ensemble bilingue de termes et de définitions ayant trait à des notions choisies dans ce domaine, et définit les relations pouvant exister entre les différentes notions.

Les définitions ont été établies de manière à éviter les particularismes propres à une langue donnée, en vue de faciliter leur transposition dans les langues autres que celles ayant servi à la rédaction initiale.

La présente partie de l'ISO/CEI 2382 définit les différentes notions relatives à la protection des données et des informations, y compris, la cryptographie, la classification des informations et le contrôle d'accès à ces informations, la récupération des données et des informations et les atteintes à la sécurité.

1.2 Références normatives

Les normes suivantes contiennent des dispositions qui, par suite de la référence qui en est faite, constituent des dispositions valables pour la présente partie de l'ISO/CEI 2382. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute norme est sujette à révision et les parties prenantes des accords fondés sur la présente partie de l'ISO/CEI 2382 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur à un moment donné.

ISO 1087:1990, *Terminologie – Vocabulaire.*

ISO 3166-1:1997, *Codes pour la représentation des noms de pays et de leurs subdivisions – Partie 1: Codes pays.*

ISO 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité.*

1.3 Principles and rules followed

1.3.1 Definition of an entry

Section 2 comprises a number of entries. Each entry consists of a set of essential elements that includes an index number, one term or several synonymous terms, and a phrase defining one concept. In addition, an entry may include examples, notes or illustrations to facilitate understanding of the concept.

Occasionally, the same term may be defined in different entries, or two or more concepts may be covered by one entry, as described in 1.3.5 and 1.3.8 respectively.

Other terms such as **vocabulary**, **concept**, **term**, and **definition** are used in this part of ISO/IEC 2382 with the meaning defined in ISO 1087.

1.3.2 Organization of an entry

Each entry contains the essential elements defined in 1.3.1 and, if necessary, additional elements. The entry may contain the following elements in the following order:

a) an index number (common for all languages in which this part of ISO/IEC 2382 is published);

b) the term or the generally preferred term in the language. The absence of a generally preferred term for the concept in the language is indicated by a symbol consisting of five dots (.....); a row of dots may be used to indicate, in a term, a word to be chosen in each particular case;

c) the preferred term in a particular country (identified according to the rules of ISO 3166);

d) the abbreviation for the term;

e) permitted synonymous term(s);

f) the text of the definition (see 1.3.4);

g) one or more examples with the heading "Example(s)";

h) one or more notes specifying particular cases in the field of application of the concepts with the heading "NOTE(S)";

i) a picture, a diagram, or a table which could be common to several entries.

1.3 Principes d'établissement et règles suivies

1.3.1 Définition de l'article

La section 2 est composée d'un certain nombre d'articles. Chaque article est composé d'un ensemble d'éléments essentiels comprenant le numéro de référence, le terme ou plusieurs termes synonymes et la définition de la notion couverte par ces termes. Cet ensemble peut être complété par des exemples, des notes, des schémas ou des tableaux destinés à faciliter la compréhension de la notion.

Parfois, le même terme peut être défini dans des articles différents, ou bien deux notions ou davantage peuvent être couvertes par un seul article: voir respectivement en 1.3.5 et 1.3.8.

D'autres termes tels que **vocabulaire**, **notion**, **terme**, **définition**, sont employés dans la présente partie de l'ISO/CEI 2382 avec le sens qui leur est donné dans l'ISO 1087.

1.3.2 Constitution d'un article

Chaque article contient des éléments essentiels définis en 1.3.1 et, si nécessaire, des éléments supplémentaires. L'article peut donc comprendre dans l'ordre les éléments suivants:

a) un numéro de référence (le même, quelle que soit la langue de publication de la présente partie de l'ISO/CEI 2382);

b) le terme, ou le terme préféré en général dans la langue. L'absence, dans une langue, de terme consacré ou à conseiller pour exprimer une notion est indiquée par un symbole consistant en cinq points de suspension (.....); les points de suspension peuvent être employés pour désigner, dans un terme, un mot à choisir dans un cas particulier;

c) le terme préféré dans un certain pays (identifié selon les règles de l'ISO 3166);

d) l'abréviation pouvant être employée à la place du terme;

e) le terme ou les termes admis comme synonymes;

f) le texte de la définition (voir 1.3.4);

g) un ou plusieurs exemples précédés du titre «Exemple(s)»;

h) une ou plusieurs notes précisant le domaine d'application de la notion, précédées du titre «NOTE(S)»;

i) une figure, un schéma ou un tableau, pouvant être communs à plusieurs articles.

1.3.3 Classification of entries

A two-digit serial number is assigned to each part of ISO/IEC 2382, beginning with 01 for "Fundamental terms".

The entries are classified in groups to each of which is assigned a four-digit serial number; the first two digits being those of the part of ISO/IEC 2382.

Each entry is assigned a six-digit index number; the first four digits being those of the part of ISO/IEC 2382 and the group.

To show the relationship between versions of ISO/IEC 2382 in various languages, the numbers assigned to parts, groups, and entries are the same for all languages.

1.3.4 Selection of terms and wording of definitions

The selection of terms and the wording of definitions have, as far as possible, followed established usage. Where there were contradictions, solutions agreeable to the majority have been sought.

1.3.5 Multiple meanings

When, in one of the working languages, a given term has several meanings, each meaning is given a separate entry to facilitate translation into other languages.

1.3.6 Abbreviations

As indicated in 1.3.2, abbreviations in current use are given for some terms. Such abbreviations are not used in the texts of the definitions, examples or notes.

1.3.7 Use of parentheses

In some terms, one or more words printed in bold typeface are placed between parentheses. These words are part of the complete term, but they may be omitted when use of the abridged term in a technical context does not introduce ambiguity. In the text of another definition, example, or note of ISO/IEC 2382, such a term is used only in its complete form.

In some entries, the terms are followed by words in parentheses in normal typeface. These words are not a part of the term but indicate directives for the use of the term, its particular field of application, or its grammatical form.

1.3.3 Classification des articles

Chaque partie de l'ISO/CEI 2382 reçoit un numéro d'ordre à deux chiffres, en commençant par 01 pour la partie «Termes fondamentaux».

Les articles sont répartis en groupes qui reçoivent chacun un numéro d'ordre à quatre chiffres, les deux premiers chiffres étant ceux du numéro de la partie de l'ISO/CEI 2382.

Chaque article est repéré par un numéro de référence à six chiffres, les quatre premiers chiffres étant ceux du numéro de partie de l'ISO/CEI 2382 et de groupe.

Les numéros des parties, des groupes et des articles sont les mêmes pour toutes les langues, afin de mettre en évidence les correspondances des versions de l'ISO/CEI 2382.

1.3.4 Choix des termes et des définitions

Les choix qui ont été faits pour les termes et leurs définitions sont, dans toute la mesure du possible, compatibles avec les usages établis. Lorsque certains usages apparaissent contradictoires, des solutions de compromis ont été retenues.

1.3.5 Pluralité de sens ou polysémie

Lorsque, dans l'une des langues de travail, un même terme peut prendre plusieurs sens, ces sens sont définis dans des articles différents, pour faciliter l'adaptation du vocabulaire dans d'autres langues.

1.3.6 Abréviations

Comme indiqué en 1.3.2, des abréviations d'usage courant, au moins en anglais, sont indiquées pour certains termes. De telles abréviations ne sont pas employées dans le corps des définitions, exemples ou notes.

1.3.7 Emploi des parenthèses

Dans certains termes, un ou plusieurs mots imprimés en caractères gras sont placés entre parenthèses. Ces mots font partie intégrante du terme complet, mais peuvent être omis lorsque le terme ainsi abrégé peut être employé dans un contexte technique déterminé sans que cette omission ne crée d'ambiguïté. Un tel terme n'est employé dans le texte d'une autre définition, d'un exemple ou d'une note de l'ISO/CEI 2382, que sous sa forme complète.

Dans certains articles, les termes définis sont suivis par des expressions imprimées en caractères normaux et placées entre parenthèses. Ces expressions ne font pas partie du terme mais indiquent des prescriptions d'emploi, précisent un domaine d'application particulier ou indiquent une forme grammaticale.

1.3.8 Use of brackets

When several closely related terms can be defined by texts that differ only in a few words, the terms and their definitions are grouped in a single entry. The words to be substituted in order to obtain the different meanings are placed in brackets, i.e. [ ], in the same order in the term and in the definition. To clearly identify the words to be substituted, the last word that according to the above rule could be placed in front of the opening bracket is, wherever possible, placed inside the bracket and repeated for each alternative.

1.3.9 Use of terms printed in italic typeface in definitions and the use of an asterisk

A term printed in italic typeface in a definition, an example, or a note is defined in another entry in ISO/IEC 2382, which may be in another part. However, the term is printed in italic typeface only the first time it occurs in each entry.

Italic typeface is also used for other grammatical forms of a term, for example, plurals of nouns and participles of verbs.

The basic forms of all terms printed in italic typeface which are defined in this part of ISO/IEC 2382 are listed in the index at the end of the part (see 1.3.11).

An asterisk is used to separate terms printed in italic typeface when two such terms are referred to in separate entries and directly follow each other (or are separated only by a punctuation mark).

Words or terms that are printed in normal typeface are to be understood as defined in current dictionaries or authoritative technical vocabularies.

1.3.10 Spelling

In the English language version of this part of ISO/IEC 2382, terms, definitions, examples, and notes are given in the spelling preferred in the USA. Other correct spellings may be used without violating this part of ISO/IEC 2382.

1.3.11 Organization of the alphabetical index

For each language used, an alphabetical index is provided at the end of each part. The index includes all terms defined in the part. Multiple-word terms appear in alphabetical order under each of their key words.

1.3.8 Emploi des crochets

Lorsque plusieurs termes étroitement apparentés peuvent être définis par des textes presque identiques, à quelques mots près, les termes et leurs définitions ont été groupés en un seul article. Les mots à substituer à ceux qui les précèdent pour obtenir les différents sens sont placés entre crochets (c'est-à-dire [ ]) dans le même ordre dans le terme et la définition. En vue d'éviter toute incertitude sur les mots à remplacer, le dernier mot qui, suivant la règle ci-dessus, pourrait être placé devant le crochet d'ouverture, est placé, si possible, à l'intérieur des crochets et répété à chaque occasion.

1.3.9 Emploi dans les définitions de termes imprimés en caractères italiques et de l'astérisque

Dans le texte d'une définition, d'un exemple ou d'une note, tout terme imprimé en caractères italiques a le sens défini dans un autre article de l'ISO/CEI 2382, qui peut se trouver dans une autre partie. Cependant le terme est imprimé en caractères italiques uniquement la première fois qu'il apparaît dans chaque article.

Les caractères italiques sont également utilisés pour les autres formes grammaticales du terme, par exemple, les noms au pluriel et les verbes au participe.

La liste des formes de base des termes imprimés en caractères italiques qui sont définis dans cette partie de l'ISO/CEI 2382 est fournie dans l'index à la fin de la partie (voir 1.3.11).

L'astérisque sert à séparer les termes imprimés en caractères italiques quand deux termes se rapportent à des articles séparés et se suivent directement (ou bien sont séparés simplement par un signe de ponctuation).

Les mots ou termes imprimés en caractères normaux doivent être compris dans le sens qui leur est donné dans les dictionnaires courants ou vocabulaires techniques faisant autorité.

1.3.10 Mode d'écriture et orthographe

Dans la version anglaise de la présente partie de l'ISO/CEI 2382, les termes, définitions, exemples et notes sont écrits suivant l'orthographe prévalant aux États-Unis. D'autres orthographes correctes peuvent être utilisées sans violer la présente partie de l'ISO/CEI 2382.

1.3.11 Constitution de l'index alphabétique

Pour chaque langue de travail, un index alphabétique est fourni à la fin de chaque partie. L'index comprend tous les termes définis dans la partie. Les termes composés de plusieurs mots sont répertoriés alphabétiquement suivant chacun des mots clés.

Section 2: Terms and definitions

08 Security

08.01 General concepts

08.01.01
computer security
COMPUSEC (abbreviation) /US/
The protection of *data* and *resources* from accidental or malicious acts, usually by taking appropriate actions.

NOTE – These acts may be modification, destruction, access, *disclosure*, or acquisition, if not authorized.

08.01.02
administrative security
procedural security
Administrative measures for *computer security.*

NOTE – These measures may be operational and *accountability* procedures, procedures of investigating *breaches* in security, and reviewing *audit trails*.

08.01.03
communications security
COMSEC (abbreviation)
Computer security applied to *data communication*.

08.01.04
data security
Computer security applied to *data.*

08.01.05
security audit
An independent review and examination of *data processing system* records and activities to test for adequacy of system controls, to ensure compliance with established *security policy* and operational procedures, to detect *breaches* in security, and to recommend any indicated changes in control, security policy, and procedures.

08.01.06
security policy
A plan or course of action adopted for providing *computer security.*

08.01.07
data integrity
The property of *data* whose accuracy and consistency are preserved regardless of changes made.

08.01.08
file protection
The implementation of appropriate administrative, technical, or physical means to guard against the unauthorized access to, modification of, or deletion of a *file*.

Section 2: Termes et définitions

08 Sécurité

08.01 Notions générales

08.01.01
sécurité informatique
Protection des *données* et des *ressources* contre des actes accidentels ou malveillants, habituellement en prenant les mesures appropriées.

NOTE – Ces actes peuvent être la modification, la destruction, l'accès, la diffusion ou l'acquisition non autorisés.

08.01.02
sécurité administrative
Ensemble des mesures administratives de *sécurité informatique*.

NOTE – Ces mesures peuvent être des procédures opérationnelles ou d'*imputabilité* permettant de vérifier les *intrusions* dans la sécurité et l'étude d'*historiques d'expertise*.

08.01.03
sécurité des communications
Sécurité informatique appliquée aux *communications de données.*

08.01.04
sécurité des données
Sécurité informatique appliquée aux *données.*

08.01.05
audit de sécurité
Revue indépendante et examen des enregistrements et de l'activité du système afin de vérifier l'exactitude des contrôles du système pour s'assurer de leur concordance avec la *politique de sécurité* établie et les procédures d'exploitation, pour détecter les infractions à la sécurité et pour recommander les modifications appropriées des contrôles, de la politique et des procédures.

08.01.06
politique de sécurité
Plan ou programme d'action adopté pour assurer la *sécurité informatique*.

08.01.07
intégrité des données
Propriété des *données* dont l'*exactitude* et la cohérence sont préservées à travers toute modification licite.

08.01.08
protection des fichiers
Mise en œuvre de mesures administratives, techniques ou matérielles destinées à protéger des *fichiers* contre un accès, une modification ou une suppression non autorisés.

08.01.09
confidentiality
The property of *data* that indicates the extent to which these data have not been made available or disclosed to unauthorized individuals, processes, or other *entities*.

08.01.10
accountability
The property that ensures that the actions of an *entity* may be traced uniquely to that entity.

08.01.11
authentication
The act of verifying the claimed identity of an *entity*.

08.01.12
message authentication
Verification that a *message* was sent by the purported *originator* to the *intended recipient* and that the message was not changed in transit.

08.01.13
authentication information
Information used to establish the validity of a claimed identity of an *entity*.

08.01.14
credentials
Data that are *transferred* to establish the claimed identity of an *entity.*

08.01.15
authentication exchange
A mechanism intended to ensure the identity of an *entity* by means of an *information* exchange.

08.01.16
authorization
The granting of rights, which includes the granting of access based on *access rights*.

08.01.17
availability (in computer security)
The property of *data* or of *resources* being accessible and usable on demand by an authorized *entity*.

08.01.18
certification (in computer security)
The procedure by which a third party gives assurance that all or part of a *data processing system* conforms to security requirements.

08.01.19
security clearance
clearance
Permission granted to an individual to *access* * *data* or *information* at or below a particular *security level*.

08.01.09
confidentialité
Propriété des *données* qui indique dans quelle mesure elles n'ont pas été rendues accessibles ou divulguées à des personnes, des processus ou *entités* non autorisés.

08.01.10
imputabilité
Propriété d'une *unité fonctionnelle*, qui garantit que les actions de cette unité fonctionnelle ne peuvent être attribuées qu'à elle-même.

08.01.11
authentification
Action de vérifier l'identité déclarée d'une *entité*.

08.01.12
authentification de message
Vérification qu'un *message* a été émis par l'*émetteur* supposé au *destinataire* prévu et que ce méssage n'a pas été modifié au cours de sa transmission.

08.01.13
information d'authentification
Information utilisée pour établir la validité d'une identité déclarée d'une *entité*.

08.01.14
justificatif d'identité
authentifiant
*Données * transférées* pour établir l'identité déclarée d'une *entité*.

08.01.15
échange d'authentification
Mécanisme destiné à garantir l'identité d'une *entité* par échange *d'informations*.

08.01.16
autorisation
Attribution de droits comprenant la délivrance d'accès fondée sur des *droits d'accès*.

08.01.17
disponibilité (en sécurité informatique)
Propriété des *données* ou des *ressources* d'être accessibles et utilisables à la demande par une *entité* autorisée.

08.01.18
certification (en sécurité informatique)
Procédure par laquelle une tierce partie donne l'assurance écrite qu'un produit, un processus ou un service est conforme aux exigences de sécurité spécifiées.

08.01.19
habilitation
Droit accordé à un individu d'*accéder* à des *données* ou des *informations* dont le *niveau de sécurité* est inférieur ou égal à un niveau déterminé.

08.01.20
security level
The combination of a hierarchical *security classification* and a *security category* that represents the *sensitivity* of an *object* or the *security clearance* of an individual.

08.01.21
closed-security environment
An environment in which special attention is paid (in the form of *authorizations*, * *security clearances*, configuration controls, etc.) to protect *data* and *resources* from accidental or malicious acts.

08.01.22
open-security environment
An environment in which protection of *data* and *resources* from accidental or malicious acts is achieved through normal operational procedures.

08.01.23
privacy
Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of *data* about that individual.

08.01.24
risk analysis
risk assessment
A systematic method of identifying the assets of a *data processing system*, the *threats* to those assets, and the *vulnerability* of the system to those threats.

08.01.25
risk acceptance
A managerial decision to accept a certain degree of *risk*, usually for technical or cost reasons.

08.01.26
sensitivity
A measure of importance assigned to *information* by the information owner to denote its need for protection.

08.01.27
system integrity
The quality of a *data processing system* fulfilling its operational purpose while both preventing unauthorized users from making modifications to or use of *resources* and preventing authorized users from making improper modifications to or improper use of resources.

08.01.20
niveau de sécurité
Combinaison de la *classification de sécurité* hiérarchique et une *catégorie de sécurité*, qui représente la *sensibilité* d'un *objet* ou l'*habilitation* d'accès d'un individu.

08.01.21
environnement sécurisé
Environnement dans lequel une attention spéciale (sous la forme d'*autorisations*, de *permissions d'accès* et de la maîtrise de la configuration) est accordée à la protection des *données* et des *ressources* contre des actes accidentels ou malveillants.

08.01.22
environnement partiellement sécurisé
Environnement dans lequel la protection des *données* et des *ressources* contre des actes accidentels ou malveillants est assurée au moyen de procédures normales.

08.01.23
respect de la vie privée
Garantie de l'absence d'intrusion dans la vie privée ou les affaires d'un individu dans la mesure où cette intrusion résulte de la collecte et de l'utilisation illégales et non fondées de *données* relatives à cet individu.

08.01.24
analyse des risques
analyse de risque
Méthode systématique d'identification des éléments constitutifs d'un *système informatique*, des *menaces* pesant sur ces éléments et de la *vulnérabilité* du système à ces menaces.

08.01.25
acceptation des risques
acceptation de risque
Décision de gestion consistant à accepter un certain niveau de *risque informatique* généralement pour des raisons techniques ou financières.

08.01.26
sensibilité
Mesure de l'importance accordée à une *information*, par le propriétaire de cette information, afin de signaler son besoin de protection.

08.01.27
intégrité de système
intégrité du système
Aptitude d'un *système informatique* à accomplir la fonction prévue, en interdisant toute utilisation ou modification des *ressources* par des utilisateurs non autorisés, et en empêchant les utilisateurs autorisés d'effectuer des modifications inadéquates ou de faire un usage incorrect de ces ressources.

08.01.28
threat analysis
An examination of actions and events that might adversely affect a *data processing system*.

08.01.29
trusted computer system
A *data processing system* that provides sufficient *computer security* to allow for *concurrent* access to *data* by users with different *access rights* and to data with different *security classification* and *security categories.*

08.01.30
subject (in computer security)
An active *entity* that can *access * objects.*

Example: A *process* that involves *execution* of a *program*.

NOTE – A subject may cause *information* to flow among objects or may change the state of the *data processing system.*

08.01.31
object (in computer security)
An *entity* to which access is controlled.

Examples: A *file*, a *program*, an area of *main storage*; *data* collected and maintained about a person.

08.02 Classification of information

08.02.01
security classification
The determination of which specific degree of protection against access the *data* or *information* requires, together with a designation of that degree of protection.

Examples: "Top secret", "secret", "confidential".

08.02.02
sensitive information
Information that, as determined by a competent authority, must be protected because its *disclosure,* modification, destruction, or *loss* will cause perceivable damage to someone or something.

08.02.03
security category
A nonhierarchical grouping of *sensitive information* used to control access to *data* more finely than with hierarchical *security classification* alone.

08.01.28
analyse des menaces
analyse de menace
Étude des événements et des actions qui peuvent nuire au fonctionnement d'un *système informatique*.

08.01.29
système informatique fiable
système informatique éprouvé
Système informatique qui procure une sécurité informatique suffisante pour permettre un accès *concurrent* aux *données* par des utilisateurs disposant de *droits d'accès* différents et un accès à des données appartenant à des *classifications de sécurité* et à des *catégories de sécurité* différentes.

08.01.30
sujet (en sécurité informatique)
Entité active qui peut *accéder* à des *objets*.

Exemple: *processus* qui comprend l'*exécution* d'un *programme*.

NOTE – Un sujet provoque une circulation d'*informations* entre des objets ou un changement d'état du *système informatique*.

08.01.31
objet (en sécurité informatique)
Entité dont l'accès est protégé.

Exemples: *fichier*, * *programme*, zone de *mémoire principale; données* collectées et mises à jour sur une personne.

08.02 Classification de l'information

08.02.01
classification de sécurité
Détermination du degré spécifique de protection nécessaire pour éviter l'accès à des *données* ou des *informations*, assortie d'une mention qualifiant ce niveau.

Exemples: «très secret», «secret», «confidentiel».

08.02.02
information sensible
Information qui, par décision d'une autorité compétente, doit être protégée car sa *divulgation*, sa modification, sa destruction non autorisées ou sa perte, provoquerait un dommage notable aux biens ou aux personnes.

08.02.03
catégorie de sécurité
Regroupement non hiérarchique d'*informations sensibles* permettant un *contrôle d'accès* aux données plus fin qu'avec seulement une *classification de sécurité*.

08.02.04
compartmentalization
A division of *data* into isolated blocks with separate security controls for the purpose of reducing *risk*.

Example: The division of data relative to a major project into blocks corresponding to subprojects, each with its own security protection, in order to limit *exposure* of the overall project.

08.02.05
multilevel device
A *functional unit* that can simultaneously process *data* of two or more *security levels* without risking to compromise *computer security*.

08.02.06
single-level device
A *functional unit* that can only process *data* of a single *security level* at a particular time.

08.03 Cryptographic techniques

08.03.01
cryptography
The discipline that embodies the principles, means, and methods for the transformation of *data* in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.

08.03.02
encryption
encipherment
The cryptographic transformation of *data*.

NOTES
1 – The result of encryption is *ciphertext*.
2 – The reverse process is called *decryption*.
3 – See also *public-key cryptography, * symmetric cryptography, * irreversible encryption.*

08.03.03
irreversible encryption
irreversible encipherment
one-way encryption
Encryption that produces *ciphertext* from which the original *data* cannot be reproduced.

NOTE – Irreversible encryption is useful in *authentication*. For example, a *password* might be irreversibly encrypted and the resulting ciphertext *stored*. A password presented later would be irreversibly encrypted identically and the two *strings* of ciphertext compared. If they are identical, the presented password is correct.

08.02.04
parcellisation
Division de *données* en blocs isolés les uns des autres et munis de contrôles de sécurité séparés afin de réduire le *risque informatique*.

Exemple: division de données relatives à un grand projet en blocs correspondant à des sous-projets dont chacun est protégé par son propre système de sécurité afin de limiter l'*exposition* du projet dans son intégralité.

08.02.05
unité à niveaux de sécurité multiples
Unité fonctionnelle capable de traiter simultanément des données relevant de plusieurs *niveaux de sécurité*, sans risque de compromettre la *sécurité informatique*.

08.02.06
unité à niveau de sécurité unique
Unité fonctionnelle ne pouvant traiter, à un instant déterminé, que des données relevant d'un seul *niveau de sécurité*.

08.03 Techniques cryptographiques

08.03.01
cryptographie
Discipline incluant les principes, moyens et méthodes de transformation des *données*, dans le but de cacher leur contenu sémantique, d'empêcher leur utilisation non autorisée ou de permettre la détection de modifications.

08.03.02
chiffrement
cryptage
Transformation cryptographique des *données.*

NOTES
1 – Le résultat du chiffrement est le *cryptogramme.*
2 – L'opération inverse est appelée *déchiffrement.*
3 – Voir aussi *cryptographie* à *clé publique*, * *cryptographie symétrique*, * *chiffrement irréversible.*

08.03.03
chiffrement irréversible
cryptage irréversible
Chiffrement produisant un *cryptogramme* à partir duquel les données originelles ne peuvent être reconstituées.

NOTE – Le chiffrement irréversible est utilisé en particulier au cours des procédures *d'authentification*. Par exemple, un *mot de passe* est chiffré de façon irréversible, et le cryptogramme ainsi obtenu est *stocké*. Un mot de passe introduit ultérieurement sera alors chiffré de façon identique, et les deux cryptogrammes seront comparés. S'ils sont identiques, le mot de passe introduit est correct.

08.03.04
decryption
decipherment
The process of obtaining, from a *ciphertext*, the original corresponding *data*.

NOTE – A ciphertext may be encrypted a second time, in which case a single decryption does not produce the original *plaintext.*

08.03.05
cryptographic system
ciphersystem
cryptosystem
The documents, devices, equipment, and associated techniques that are used together to provide a means of *encryption* or *decryption*.

08.03.06
cryptanalysis
The analysis of a *cryptographic system*, its *inputs* or *outputs*, or both, to derive *sensitive information*, such as *plaintext*.

08.03.07
plaintext
cleartext
Data, the semantic content of which is available without using cryptographic techniques.

08.03.08
ciphertext
Data produced through the use of *encryption,* the semantic content of which is not available without the use of cryptographic techniques.

08.03.09
key (in computer security)
A *bit string* that controls the operations of *encryption* or *decryption*.

08.03.10
private key
A *key* that is intended for *decryption* for the exclusive use by its owner.

08.03.11
public key
A *key* that is intended for use by any *entity* for encrypted communication with the owner of the corresponding *private key*.

08.03.04
déchiffrement
Reconstitution, à partir d'un *cryptogramme*, des *données* originales correpondantes.

NOTE – Un cryptogramme peut être chiffré une deuxième fois; dans ce cas, un déchiffrement unique ne restitue pas le *texte en clair* original.

08.03.05
système de chiffrement
système cryptographique
Ensemble de documents, de dispositifs, d'équipements et des techniques associées dont l'utilisation combinée constitue un moyen de *chiffrement* ou *déchiffrement*.

08.03.06
analyse cryptographique
décryptage
Analyse d'un *système cryptographique* ou de ses entrées et sorties, pour en déduire des *informations sensibles*, telles que du *texte en clair*.

08.03.07
texte en clair
Données dont le contenu sémantique est disponible sans recourir à des techniques cryptographiques.

08.03.08
cryptogramme
texte chiffré
Données résultant d'un *chiffrement* et dont le contenu sémantique n'est pas disponible sans recours à des techniques cryptographiques.

08.03.09
clé (en sécurité informatique)
Chaîne de bits qui commande les opérations de *chiffrement* ou de *déchiffrement*.

08.03.10
clé privée
Clé de *déchiffrement* à l'usage exclusif de son détenteur.

08.03.11
clé publique
clé révélée
Clé destinée à être utilisée par une *entité* quelconque pour une communication *chiffrée* avec le propriétaire de la *clé privée* correspondante.

08.03.12
public-key cryptography
asymmetric cryptography
Cryptography in which a *public key* and a corresponding *private key* are used for *encryption* and *decryption*.

NOTE – If a public key is used for encryption, the corresponding private key must be used for decryption, and vice versa.

08.03.13
symmetric cryptography
Cryptography in which the same *key* is used for *encryption* and *decryption*.

08.03.14
secret key
A *key* that is intended for use by a limited number of correspondents for *encryption* and *decryption*.

08.03.15
transposition
Encryption that rearranges *bits* or *characters* according to some scheme.

NOTE – The resulting *ciphertext* is called transposition cipher.

08.03.16
substitution
Encryption that replaces *bit strings* or *character strings* with other bit strings or character strings.

NOTE – The resulting *ciphertext* is called substitution cipher.

08.04 Access control

08.04.01
access control
A means of ensuring that the *resources* of a *data processing system* can be *accessed* only by authorized *entities* in authorized ways.

08.04.02
access control list
access list
A list of *entities*, together with their *access rights*, that are authorized to *access* a *resource*.

08.04.03
access category
A category to which *entities* may be assigned, based on the *resources* that the entity is authorized to use.

08.03.12
cryptographie à clé publique
cryptographie asymétrique
Cryptographie dans laquelle on utilise une *clé publique* et une *clé privée* correspondante pour le *chiffrement* et le *déchiffrement*.

NOTE – Si une clé publique est utilisée pour le chiffrement, la clé privée correspondante doit être utilisée pour le déchiffrement, et vice versa.

08.03.13
cryptographie symétrique
Cryptographie dans laquelle on utilise la même *clé* pour le *chiffrement* et le *déchiffrement*.

08.03.14
clé secrète
En *cryptographie, clé* de *chiffrement* et de *déchiffrement* réservée à l'usage exclusif d'un nombre limité de correspondants.

08.03.15
permutation
transposition
chiffrement de transposition
Chiffrement qui change l'ordre des *caractères* ou des *bits* selon une logique donnée.

NOTE – Les termes transposition et permutation peuvent désigner aussi le *cryptogramme* résultant.

08.03.16
substitution
chiffrement de substitution
Chiffrement de *données* ou de messages effectué en remplaçant des *chaînes* de *caractères* ou de *bits* par d'autres suites de caractères ou de bits.

NOTE – Le terme substitution peut désigner le *cryptogramme* résultant.

08.04 Contrôle d'accès

08.04.01
contrôle d'accès
Ensemble des moyens garantissant que seules les *entités* autorisées peuvent *accéder* aux ressources d'un *système informatique*, et seulement d'une manière autorisée.

08.04.02
liste de contrôle d'accès
Liste d'*entités* autorisées à *accéder* à une *ressource*, ainsi que de leurs *droits d'accès*.

08.04.03
catégorie d'accès
Catégorie à laquelle on peut affecter des *entités* en fonction des *ressources* qu'elles ont le droit d'utiliser.

08.04.04
access level
The level of authority required from an *entity* to *access* a protected *resource*.

Example: The authority to access *data* or *information* at a particular *security level*.

08.04.05
access right
Permission for a *subject* to *access* a particular *object* for a specific type of *operation*.

Example: Permission for a *process* to *read* a *file* but not *write* to it.

08.04.06
access permission
All of a *subject*'s * *access rights* with respect to some *object*.

08.04.07
access period
A period of time during which specified *access rights* prevail.

08.04.08
access type (in computer security)
A type of *operation* specified by an *access right*.

Examples: *Read, * write, * execute*, append, modify, delete, create.

08.04.09
ticket (in computer security)
A representation of one or more *access rights* that a possessor has to an *object*.

NOTE – The ticket represents an *access permission.*

08.04.10
capability (in computer security)
A representation of the identification of an *object*, or of a class of objects, and of a set of authorized *access types* for these objects.

NOTE – A capability can be implemented in the form of a *ticket.*

08.04.11
capability list
A list associated with a *subject* that identifies all of the subject's *access types* for all *objects*.

Example: A list associated with a process that identifies all of its access types for all *files* and other protected *resources.*

08.04.04
niveau d'accès
Niveau d'autorisation requis d'une *entité* pour pouvoir accéder à une *ressource* protégée.

Exemple: autorisation d'accéder aux *données* ou aux *informations* d'un certain niveau de sécurité.

08.04.05
droit d'accès
Autorisation donnée à un *sujet* d'*accéder* à un *objet* particulier, pour un type donné d'*opération*.

Exemple: autorisation pour un *processus* de *lire* un *fichier* mais non d'y *écrire.*

08.04.06
permis d'accès
permission d'accès
Ensemble des *droits d'accès* d'un *sujet* à un *objet* déterminé.

08.04.07
période d'accès
Intervalle de temps pendant lequel les *droits d'accès* d'une entité sont valides.

08.04.08
type d'accès (en sécurité informatique)
Type d'*opération* spécifiée par un *droit d'accès*.

Exemples: *lire, * écrire, * exécuter*, ajouter, modifier, supprimer, créer.

08.04.09
ticket (en sécurité informatique)
Représentation du ou des droits d'accès à un *objet* possédés par un détenteur.

NOTE – Le ticket représente un *permis d'accès.*

08.04.10
capacité (en sécurité informatique)
Représentation de l'identité d'un *objet* ou d'une classe d'objets et d'un jeu de *types d'accès* autorisés applicable à ces objets.

NOTE – Une capacité peut être mise en œuvre sous la forme d'un *ticket.*

08.04.11
profil d'accès
liste d'habilitation
Liste associée à un *sujet* et qui identifie tous les types d'*accès* de ce *sujet* pour tous les *objets*.

Exemple: liste associée à un processus et qui identifie tous ses types d'accès à tous les *fichiers* et autres *ressources* protégées.

08.04.12
identity authentication
identity validation
The performance of tests to enable a *data processing system* to recognize *entities*.

Example: The checking of a *password* or of an *identity token*.

08.04.13
identity token
A device used for *identity authentication.*

Examples: Smart card, metal key.

08.04.14
password
A *character string* that is used as *authentication information.*

08.04.15
minimum privilege
Restriction of the *access rights* of a *subject* to only those rights that are necessary for the execution of authorized tasks.

08.04.16
need-to-know
A legitimate requirement of a prospective *recipient* of *data* to know, to *access*, or to possess any *sensitive information* represented by these data.

08.04.17
logical access control
The use of mechanisms related to *data* or *information* to provide *access control*.

Example: The use of a *password*.

08.04.18
physical access control
The use of physical mechanisms to provide *access control*.

Example: Keeping a *computer* in a locked room.

08.04.19
controlled access system
CAS (abbreviation)
A means of *automating * physical access control.*

Example: The use of magnetic-striped badges, smart cards, *biometric* readers.

08.04.20
read access
An *access right* that gives permission to *read * data*.

08.04.12
validation d'identité
Exécution de tests permettant à un *système informatique* de reconnaître des *entités*.

Exemple: vérification d'un *mot de passe* ou d'une *preuve d'identité.*

08.04.13
jeton d'identité
Dispositif utilisé pour une *validation d'identité.*

Exemples: carte à puce, clé métallique.

08.04.14
mot de passe
Chaîne de caractères utilisée comme *information d'authentification.*

08.04.15
privilège minimal
droit minimal
Ensemble des *droits d'accès* strictement nécessaires à un *sujet* pour l'exécution de tâches autorisées.

08.04.16
besoin d'en connaître
Besoin légitime qu'a un *destinataire* potentiel d'une *information sensible* d'en connaître l'existence, d'y *accéder* ou de la détenir.

08.04.17
contrôle d'accès logique
Utilisation de mécanismes relatifs à des *données* ou des *informations* pour assurer un *contrôle d'accès*.

Exemple: utilisation d'un *mot de passe*.

08.04.18
contrôle d'accès physique
Contrôle d'accès reposant sur des moyens matériels.

Exemple: conserver un ordinateur dans une salle fermée à clé.

08.04.19
système de contrôle d'accès
Système permettant un *contrôle d'accès physique* automatique.

Exemple: utilisation de badges à piste magnétique, de cartes à puce, de capteurs *biométriques.*

08.04.20
accès en lecture
Droit d'accès autorisant à lire des *données.*

08.04.21
write access
An *access right* that gives permission to *write * data*.

NOTE – Write access may grant permission to append, modify, delete, or create data.

08.04.22
user ID
user identification
A *character string* or *pattern* that is used by a *data processing system* to identify a user.

08.04.23
user profile (1)
A description of a user, typically used for *access control*.

NOTE – A user profile may include *data* such as *user ID*, user name, *password*, * *access rights*, and other attributes.

08.04.24
user profile (2)
A *pattern* of a user's activity that can be used to detect changes in the activity.

08.05 Security violations

08.05.01
computer abuse
A willful or negligent unauthorized activity that affects or involves the *computer security* of a *data processing system*.

08.05.02
computer crime
A crime committed with the aid of, or directly involving, a *data processing system* or *computer network*.

NOTE – This is an revised version of the definition in ISO/IEC 2382-1:1993.

08.05.03
computer fraud
A fraud committed with the aid of, or directly involving, a *data processing system* or *computer network*.

08.05.04
threat
A potential violation of *computer security*.

NOTE – See figure 1.

08.05.05
active threat
Any *threat* of a deliberate unauthorized change to the state of a *data processing system*.

Example: A threat that would result in modification of *messages*, insertion of spurious messages, *masquerade*, or *denial of service*.

08.04.21
accès en écriture
Droit d'accès autorisant à écrire des *données.*

NOTE – L'accès en écriture peut autoriser à ajouter, modifier, supprimer ou créer des données.

08.04.22
identificateur d'utilisateur
ID utilisateur
Chaîne de caractères ou modèle utilisé par un *système informatique* pour identifier sans ambiguïté un utilisateur.

08.04.23
profil d'utilisateur
Description d'un utilisateur, notamment utilisée pour le *contrôle d'accès*.

NOTE – Un profil d'utilisateur peut inclure des données telles qu'*identité d'utilisateur,* nom *d'utilisateur, mot de passe*, *droits d'accès*, et autres attributs.

08.04.24
modèle de comportement
Description de l'activité d'un utilisateur, qui peut servir de référence pour détecter des changements.

08.05 Atteintes à la sécurité

08.05.01
malveillance informatique
Action non autorisée, délibérée ou due à la négligence, et qui affecte ou met en cause la *sécurité informatique* d'un *système informatique.*

08.05.02
délit informatique
Délit commis à l'aide d'un *système informatique* ou d'un *réseau d'ordinateurs* ou les impliquant directement.

NOTE – Cette définition est une version révisée de celle contenue dans l'ISO/CEI 2382-1:1993.

08.05.03
fraude informatique
Fraude commise à l'aide d'un *système informatique* ou d'un *réseau d'ordinateurs* ou les impliquant directement.

08.05.04
menace
Violation potentielle de la *sécurité informatique*.

NOTE – Voir figure 1.

08.05.05
menace active
Menace de changement non autorisé de l'état d'un *système informatique*.

Exemple: une menace qui aurait pour résultat la modification de *messages*, l'insertion de faux messages, le *déguisement* et le *déni de service*.

08.05.06
passive threat
A *threat* of *disclosure* of *information* without changing the state of a *data processing system.*

Example: A threat that would result in the recovery of *sensitive information* through the interception of *data * transmitted*.

08.05.07
flaw (in computer security)
loophole
An error of commission, an omission, or an oversight that allows protection mechanisms to be bypassed or disabled.

08.05.08
vulnerability
A weakness or *flaw* in a *data processing system.*

NOTES
1 – If a vulnerability corresponds to a *threat*, a *risk* exists.
2 – See figure 1.

08.05.09
risk
The possibility that a particular *threat* will exploit a particular *vulnerability* of a *data processing system*.

NOTE – See figure 1.

08.05.10
denial of service
The prevention of authorized access to *resources* or the delaying of time-critical *operations*.

08.05.11
compromise
A violation of *computer security* whereby *programs* or *data* may have been modified, destroyed, or made available to unauthorized *entities*.

NOTE – See figure 1.

08.05.12
loss
A quantitative measure of harm or deprivation resulting from a *compromise*.

NOTE – See figure 1.

08.05.13
exposure
The possibility that a particular *attack* will exploit a particular *vulnerability* of a *data processing system.*

NOTE – See figure 1.

08.05.06
menace passive
Menace de *divulgation* d'*informations* sans changement de l'état du *système informatique.*

Exemple: menace qui aurait pour résultat l'obtention d'*informations sensibles* par l'interception de *données* en cours de transmission.

08.05.07
faille (en sécurité informatique)
brèche
échappatoire
Erreur dans l'exécution d'un ordre, omission ou manquement qui neutralise les mécanismes de protection ou permet de les contourner.

08.05.08
vulnérabilité
Toute faiblesse ou *faille* d'un *système informatique*.

NOTES
1 – Si une vulnérabilité correspond à une *menace,* il existe un risque.
2 – Voir figure 1.

08.05.09
risque informatique
Possibilité qu'une *menace* particulière tire parti d'une *vulnérabilité* particulière d'un *système informatique.*

NOTE – Voir figure 1.

08.05.10
déni de service
refus de service
Impossibilité d'accès à des *ressources* pour des utilisateurs autorisés ou introduction d'un retard préjudiciable dans les *opérations*.

08.05.11
compromission
Violation de la *politique de sécurité* d'un *système informatique* au cours de laquelle des *programmes* ou des *données* ont pu être modifiés, détruits ou rendus accessibles à des *entités* non autorisées.

NOTE – Voir figure 1.

08.05.12
perte
Mesure quantitative des dommages et des privations résultant d'une *compromission*.

NOTE – Voir figure 1.

08.05.13
exposition
Possibilité qu'une *attaque* particulière exploite une *vulnérabilité* particulière d'un *système informatique*.

NOTE – Voir figure 1.

08.05.14
compromising emanation
Signals that are unintentionally emitted and that, if intercepted and analyzed, may reveal *sensitive information* being processed or *transmitted*.

Examples: Acoustic emanation, electromagnetic emanation.

08.05.15
disclosure
A violation of *computer security* whereby *data* have been made available to unauthorized *entities*.

08.05.16
penetration
Unauthorized access to a *data processing system.*

NOTE – See figure 1.

08.05.17
breach
The circumvention or disablement of some element of *computer security*, with or without detection, which could result in a *penetration* of the *data processing system*.

NOTE – See figure 1.

08.05.18
network weaving
A *penetration* technique in which different communication *networks* are used to gain access to a *data processing system* to avoid detection and trace-back.

08.05.19
attack
An attempt to violate *computer security*.

Examples: *Malicious logic*, * *wiretapping*.

NOTE – See figure 1.

08.05.20
analytical attack
cryptanalytical attack
An attempt to break a *code* or to find a *key* using analytical methods.

Examples: A statistical analysis of *patterns*; a search for *flaws* in an *encryption* * *algorithm*.

NOTE – Contrast with *exhaustive attack.*

08.05.14
émission compromettante
Émission non intentionnelle qui, si elle est interceptée et analysée, peut révéler des informations sensibles en cours de traitement ou de *transmission*.

Exemples: émission acoustique, émission électro-magnétique.

08.05.15
divulgation
Violation de la *politique de sécurité* d'un *système informatique* au cours de laquelle des *données* ont été mises à la disposition d'*entités* non autorisées.

08.05.16
pénétration
Accès non autorisé à un *système informatique.*

NOTE – Voir figure 1.

08.05.17
intrusion
effraction
Action de contourner ou de neutraliser avec succès un élément de la *sécurité informatique*, avec ou sans détection, action qui, si elle est menée à son terme, peut entraîner une *pénétration* du *système informatique*.

NOTE – Voir figure 1.

08.05.18
chemin furtif
réseautage illicite
louvoiement
faufilement
Technique de *pénétration* dans laquelle on utilise différents *réseaux* de communication pour *accéder* à un *système informatique* pour éviter d'être détecté et pisté.

08.05.19
attaque
Tentative de violation de la *sécurité informatique.*

Exemples: *logiciel malveillant*, * *branchement clandestin*.

NOTE – Voir figure 1.

08.05.20
attaque analytique
attaque cryptanalytique
Tentative pour briser un *code* ou trouver une clé par des moyens systématiques.

Exemples: analyse statistique de modèles, recherche de *failles* dans un *algorithme* de *chiffrement*.

NOTE – Différent d'*attaque exhaustive.*

08.05.21
ciphertext-only attack
An *analytical attack* in which a cryptanalyst possesses only *ciphertext*.

08.05.22
known-plaintext attack
An *analytical attack* in which a cryptanalyst possesses a substantial quantity of corresponding *plaintext* and *ciphertext*.

08.05.23
chosen-plaintext attack
An *analytical attack* in which a cryptanalyst can submit an unlimited number of *plaintext * messages* and examine the corresponding *ciphertext*.

08.05.24
exhaustive attack
brute-force attack
A trial-and-error attempt to violate *computer security* by trying possible values of *passwords* or *keys*.

NOTE – Contrast with *analytical attack.*

08.05.25
eavesdropping
The unauthorized interception of *information*-bearing emanations.

08.05.26
wiretapping
Surreptitious access to some part of a *data circuit* to obtain, modify, or insert *data*.

08.05.27
active wiretapping
Wiretapping with the purpose to modify or insert *data*.

08.05.28
passive wiretapping
Wiretapping limited to obtaining *data*.

08.05.29
masquerade
The pretense by an *entity* to be a different entity in order to gain unauthorized access.

08.05.30
piggyback entry
Unauthorized access to a *data processing system* via an authorized user's legitimate connection.

08.05.21
attaque par cryptogramme
Attaque analytique dans laquelle le cryptanalyste ne dispose que du *cryptogramme.*

08.05.22
attaque par texte en clair connu
Attaque analytique dans laquelle le cryptanalyste dispose d'une quantité importante de *texte en clair* et du *cryptogramme* correspondant.

08.05.23
attaque par texte en clair choisi
Attaque analytique dans laquelle le cryptanalyste peut soumettre un nombre illimité de *textes en clair* et examiner les *cryptogrammes* correspondants.

08.05.24
attaque exhaustive
attaque en force
Tentative de violation de la *sécurité informatique* par une technique d'essais et erreurs consistant à essayer des valeurs possibles de *mots de passe* ou de *clés.*

NOTE – Différent d'*attaque analytique.*

08.05.25
écoute clandestine
interception illicite
Interception non autorisée d'émissions porteuses d'*informations.*

08.05.26
branchement clandestin
Accès clandestin à une partie d'un *circuit de données* pour obtenir, modifier ou insérer des *données.*

08.05.27
branchement clandestin actif
Branchement clandestin destiné à modifier ou insérer des *données.*

08.05.28
branchement clandestin passif
Branchement clandestin limité à l'obtention de *données.*

08.05.29
déguisement
usurpation d'identité
Fait de prétendre, pour une *entité*, être une autre entité pour obtenir un accès non autorisé.

08.05.30
accès à califourchon
accès à dada
accès superposé
Accès non autorisé à un *système informatique* via la connexion légitime d'un utilisateur autorisé.

08.05.31
to **tailgate**
To gain unauthorized physical access by following an authorized person through a controlled door.

08.05.32
to **scavenge**
To search, without *authorization*, through *residual data* to acquire *sensitive information.*

08.05.33
to **spoof**
To take action intended to deceive a user, an observer (such as an eavesdropper), or a *resource*.

08.05.34
aborted connection
A disconnection that does not follow established procedures.

NOTE – An aborted connection may enable other *entities* to gain unauthorized access.

08.05.35
failure access
An unauthorized and usually inadvertent access to *data* in a *data processing system*, resulting from a *failure* of *hardware* or *software*.

08.05.36
between-the-lines entry
Access obtained through *active wiretapping* by an unauthorized user to a momentarily inactive *transmission channel* connected to a legitimate user *resource*.

08.05.37
trapdoor
A hidden *software* or *hardware* mechanism, usually created for testing and troubleshooting, that may be used to circumvent *computer security*.

08.05.38
maintenance hook
A *trapdoor* in *software* that allows easy *maintenance* and development of additional features and that may allow entry into the *program* at unusual points or without the usual checks.

08.05.31
faufilement
talonnage
Obtenir un accès physique non autorisé en suivant une autre personne à travers une porte contrôlée.

08.05.32
récupération illicite
cannibalisation
Recherche sans *autorisation* dans des *données résiduelles* pour obtenir des *informations sensibles.*

08.05.33
bluff
incitation à la faute
mystification
arnaque
Action de prendre des mesures destinées à tromper un utilisateur, un observateur (qui effectue par exemple un *branchement clandestin*) ou une *ressource.*

08.05.34
abandon de connexion
Déconnexion ne suivant pas les procédures établies.

NOTE – Une déconnexion peut permettre à d'autres entités d'obtenir un accès non autorisé.

08.05.35
accès sur défaillance
accès par défaillance
Accès non autorisé et généralement accidentel à des *données* dans un *système informatique*, par suite d'un dysfonctionnement du *logiciel* ou du *matériel*.

08.05.36
accès par infiltration
faufilage
Accès obtenu par une *entité* non autorisée qui effectue un *branchement clandestin actif* sur une *voie de communication de données* temporairement inactive, reliée à une *ressource* d'une entité légitime.

08.05.37
trappe
porte dissimulée
Mécanisme *logiciel* ou *matériel* dissimulé, habituellement conçu pour les tests et la détection des erreurs, utilisé pour contourner la *sécurité informatique*.

08.05.38
entrée de service
porte secrète
Porte dissimulée dans un logiciel, pour faciliter la *maintenance* et le développement de fonctions supplémentaires, et qui peut permettre d'accéder au *programme* en des endroits imprévus, ou sans les contrôles habituels.

08.05.39
aggregation
Acquisition of *sensitive information* by collecting and correlating *information* of lesser *sensitivity*.

08.05.40
linkage (in computer security)
fusion
The purposeful combination of *data* or *information* from one *data processing system* with data or information from another system to derive protected information.

08.05.41
traffic analysis
The inference of *information* from observation of traffic flow.

Example: Analysis of the presence, absence, amount, direction, and frequency of traffic.

08.05.42
data corruption
An accidental or intentional violation of *data integrity*.

08.05.43
flooding
Accidental or intentional insertion of a large volume of *data* resulting in *denial of service*.

08.05.44
contamination
The introduction of *data* of one *security classification* or *security category* into data of a lower security classification or different security category.

08.05.45
covert channel
A *transmission channel* that may be used to *transfer * data* in a manner that violates *security policy.*

08.05.46
malicious logic
A *program* implemented in *hardware*, * *firmware*, or *software*, and whose purpose is to perform some unauthorized or harmful action.

Examples: A *logic bomb*, a *Trojan horse*, a *virus*, a *worm*.

08.05.39
recoupement
Acquisition d'*informations sensibles* par le rassemblement et la mise en relation d'*informations* d'une *sensibilité* inférieure.

08.05.40
recoupement (en sécurité informatique)
corrélation
Combinaison volontaire de *données* ou *d'informations* provenant d'un système informatique avec des données ou informations provenant d'un autre système afin d'en déduire de l'information protégée.

08.05.41
analyse du trafic
Déduction *d'informations* à partir de l'observation des flux de *données*.

Exemple: analyse de la présence, de l'absence, de la quantité, de la direction et de la fréquence des flux.

08.05.42
altération des données
Violation accidentelle ou intentionnelle de *l'intégrité des données*.

08.05.43
inondation
Ajout acccidentel ou intentionnel d'un important volume de données entraînant un *déni de service*.

08.05.44
pollution
contamination des données
Introduction de *données* relevant d'une *classification de sécurité* ou d'une *catégorie de sécurité* donnée dans des données relevant d'une classification de sécurité inférieure ou d'une catégorie de sécurité différente.

08.05.45
voie clandestine
Voie de transmission qui permet à un processus de *transférer des données* d'une manière qui viole la *politique de sécurité.*

08.05.46
logiciel malveillant
programme malveillant
antiprogramme
Programme implanté au niveau du *matériel,* du *microprogramme* ou du *logiciel* et dont le but est d'accomplir un acte non autorisé ou dangereux.

Exemples: *bombe logique*, * *cheval de Troie*, * *virus*, * *ver*.

08.05.47
virus
A *program* that propagates itself by modifying other programs to include a possibly changed copy of itself and that is *executed* when the infected program is invoked.

NOTE – A virus often causes damage or annoyance and may be triggered by some event such as the occurrence of a predetermined date.

08.05.48
worm
A self-contained *program* that can propagate itself through *data processing systems* or *computer networks*.

NOTE – Worms are often designed to use up available *resources* such as *storage* space or processing time.

08.05.49
Trojan horse
An apparently harmless *program* containing *malicious logic* that allows the unauthorized collection, falsification, or destruction of *data.*

08.05.50
bacterium
chain letter
A *program* that propagates itself by *electronic mail* to everyone in each *recipient's * distribution list*.

08.05.51
logic bomb
Malicious logic that causes damage to a *data processing system* when triggered by some specific system condition.

08.05.52
time bomb
A *logic bomb* to be activated at a predetermined time.

08.06 Protection of sensitive information

08.06.01
verification
Comparing an activity, a process, or a product with the corresponding requirements or specifications.

Examples: Comparing a specification with a *security policy* model or comparing *object code* with *source code*.

08.05.47
virus informatique
virus
Programme qui se propage en modifiant d'autres programmes pour y inclure une copie éventuellement modifée de lui-même, et qui est *exécuté* quand le programme infecté est invoqué.

NOTE – Un virus contient cause souvent des dommages ou des ennuis et qui peut être déclenché par un événement donné comme l'arrivée d'une date prédéterminée.

08.05.48
ver
Programme indépendant qui peut se propager à travers des *systèmes informatiques* ou des *réseaux d'ordinateurs.*

NOTE – Les vers sont souvent conçus pour absorber la totalité des *ressources* disponibles, comme l'espace *mémoire* ou le temps de traitement.

08.05.49
cheval de Troie
Programme apparemment inoffensif contenant un *logiciel malveillant* qui permet la collecte, la falsification ou la destruction non autorisées de *données*.

08.05.50
bactérie
Programme qui se propage lui-même par *courrier électronique* à toutes les adresses de la *liste de distribution* de chaque *destinataire*.

08.05.51
bombe logique
Logiciel malveillant qui cause des dommages à un *système informatique* quand il est déclenché par des conditions spécifiques du système.

08.05.52
bombe à retardement
Bombe logique destinée à être activée à un instant prédéfini.

08.06 Protection des informations sensibles

08.06.01
vérification
Fait de comparer une activité, un processus our un produit avec des exigences ou des spécifications.

Exemples: comparaison d'une spécification avec un modèle de *politique de sécurité* ou comparaison d'un *code objet* avec un *code source*.

08.06.02
data protection
The implementation of administrative, technical, or physical measures to guard against the unauthorized access to *data*.

NOTE – This is an revised version of the definition in ISO/IEC 2382-1:1993.

08.06.03
countermeasure
An action, device, procedure, technique, or other measure that is designed to minimize *vulnerability*.

08.06.04
failsafe (in computer security)
Pertaining to avoidance of *compromise* in the event of a *failure*.

08.06.05
data validation
A process used to determine if *data* are accurate, complete, or meet specified criteria.

NOTE – Data validation may include *format* checks, completeness checks, check key tests, reasonableness checks, and limit checks.

08.06.06
keystroke verification
The determination of the accuracy of *data entry* by the re-entry of the same *data* through a keyboard.

08.06.07
audit trail (in computer security)
Data collected for the potential use in a *security audit*.

08.06.08
privacy protection
The measures taken to ensure *privacy*.

NOTE – The measures include *data protection* and limitations on the gathering, combining, and processing of *data* about individuals.

08.06.09
digital signature
Data appended to a *message*, that allow the *recipient* of the message to verify the source of the message.

08.06.10
digital envelope
Data appended to a *message,* that allow the *intended recipient* to verify the integrity of the content of the message.

08.06.02
protection des données
Mise en vigueur d'un ensemble de mesures administratives, techniques et physiques pour interdire tout accès non autorisé à des *données*.

NOTE – Cette définition est une version révisée de celle contenue dans l'ISO/CEI 2382-1:1993.

08.06.03
mesure de prévention
contre-mesure
Action, dispositif, procédure, technique ou autre mesure conçue pour réduire la *vulnérabilité*.

08.06.04
à sécurité intégrée (en sécurité informatique)
Qualifie le fait d'éviter la *compromission* dans le cas d'une *défaillance*.

08.06.05
validation de données
Processus servant à déterminer si des *données* sont exactes, complètes ou correspondent à des critères spécifiés.

NOTE – La validation de données peut comprendre notamment des contrôles de disposition, des contrôles de présence, des vérifications par clés de contrôle, des contrôles de vraisemblance et des contrôles de valeurs limites.

08.06.06
vérification au clavier
contrôle par double frappe
Vérification de l'exactitude de la saisie de *données* par la réintroduction au clavier de ces mêmes données.

08.06.07
historique d'expertise (en sécurité informatique)
piste de vérification
journal d'audit de sécurité
Données collectées permettant un *audit de sécurité*.

08.06.08
protection de la vie privée
Ensemble des mesures prises pour assurer le *respect de la vie privée*.

NOTE – Ces mesures incluent la *protection des données* et des restrictions sur la collecte, la combinaison et le traitement des *données* sur les individus.

08.06.09
signature numérique
Données ajoutées à un *message,* permettant au destinataire du message de vérifier la source de ce message.

08.06.10
enveloppe numérique
Données ajoutées à un *message*, qui permettent au *destinataire prévu* de vérifier l'intégrité du contenu du message.

08.06.11
biometric
Pertaining to the use of specific attributes that reflect unique personal characteristics, such as a fingerprint, an eye blood-vessel print, or a voice print, to validate the identity of a person.

08.06.12
call-back
dial-back
A procedure in which a *data processing system* identifies a *calling * terminal*, disconnects the *call*, and dials the calling terminal to authenticate the calling terminal.

08.06.13
clearing (in computer security)
Overwriting classified *data* on a *data medium* that has a particular *security classification* and *security category,* so that this data medium may be reused for *writing* at the same security classification and security category.

08.06.14
sanitizing
Removing *sensitive information* from a *document* to reduce its *sensitivity.*

08.06.15
residual data
Data left in a *data medium* after deletion of a *file* or a portion of a file.

NOTE – Residual data remain recoverable until *clearing* of the data medium has taken place.

08.06.16
separation of duties
Dividing responsibility for *sensitive information* so that an individual acting alone can compromise the security of only a limited portion of a *data processing system.*

08.06.17
entrapment
The deliberate planting of apparent *flaws* in a *data processing system* for the purpose of detecting attempted *penetrations* or for confusing an intruder about which flaws to exploit.

08.06.18
penetration testing
Examining the functions of a *data processing system* to find a means of circumventing *computer security.*

08.06.11
biométrique
Qualifie l'utilisation d'attributs spécifiques qui reflètent des caractéristiques personnelles uniques, telles que les empreintes digitales, l'empreinte des vaisseaux de l'œil ou une empreinte vocale, pour valider l'identité d'une personne.

08.06.12
rappel automatique
Procédure par laquelle un *système informatique* identifie un *terminal * appelant*, déconnecte l'*appel*, et appelle le terminal appelant pour vérifier son identité.

08.06.13
écrasement (en sécurité informatique)
Fait d'*écraser* des *données* classées sur un support de données qui a une *classification de sécurité* et une *catégorie de sécurité* particulières, afin que ce support de données puisse être réutilisé pour l'écriture au même niveau de classification et de catégorie de sécurité.

08.06.14
nettoyage
toilettage
assainissement
Fait de retrancher des *informations sensibles* d'un *document* pour en réduire la *sensibilité.*

08.06.15
données résiduelles
résidus
Données restant sur un *support de données* après suppression d'un *fichier* ou d'une portion de fichier.

NOTE – Les données résiduelles peuvent être récupérées jusqu'à l'*écrasement* du support de données.

08.06.16
séparation des responsabilités
Fait de diviser les responsabilités en matière d'*informations sensibles* afin qu'un individu agissant seul ne puisse compromettre la sécurité que d'une partie limitée d'un *système informatique.*

08.06.17
piégeage
Fait de placer de manière délibérée des *failles* apparentes dans un *système informatique* pour pouvoir détecter des essais de *pénétration* ou pour faire hésiter un intrus sur les failles à exploiter.

08.06.18
test de pénétration
essai de pénétration
Examen des fonctions d'un *système informatique* pour trouver les moyens de contourner la *sécurité informatique.*

08.06.19
computer-system audit
An examination of the procedures used in a *data processing system* to evaluate their effectiveness and correctness, and to recommend improvements.

08.06.20
contingency procedure
A procedure that is an alternative to the normal path of a process if an unusual but anticipated situation occurs.

08.06.21
data authentication
A process used to verify *data integrity*.

Examples: *Verification* that *data* received are identical to data sent, verification that a *program* is not infected by a *virus*.

NOTE – Not to be confused with *authentication*.

08.06.22
message authentication code
A *bit string* that is a function of both *data* (either *plaintext* or *ciphertext*) and a *secret key,* and that is attached to the data in order to allow *data authentication.*

NOTE – The function used to generate the message authentication code is typically a one-way function.

08.06.23
manipulation detection
modification detection
A procedure that is used to detect whether *data* have been modified, either accidentally or intentionally.

08.06.24
manipulation detection code
modification detection code
MDC (abbreviation)
A *bit string* that is a function of *data* to which it is attached to allow *manipulation detection*.

NOTES
1 – The resulting *message* (data plus MDC) may then be encrypted in order to achieve secrecy or *data authentication.*
2 – The function used to generate the MDC must be public.

08.06.19
vérification de système informatique
audit de système informatique
Examen des procédures utilisées dans un *système informatique* pour en évaluer l'efficacité et la conformité et proposer des améliorations.

08.06.20
procédure de substitution
procédure de repli
procédure d'urgence
Procédure utilisée à la place du cheminement normal d'un processus, s'il se produit durant son déroulement un événement inhabituel mais prévisible.

08.06.21
authentification des données
Processus servant à vérifier l'intégrité de *données* transmises, tout particulièrement dans un message.

Exemples: *vérification* que les données reçues sont identiques aux données envoyées, vérification qu'un programme n'est pas atteint par un *virus*.

NOTE – A ne pas confondre avec l'*authentification*.

08.06.22
code d'authentification de message
Chaîne de bits, qui est une fonction de *données* (*texte en clair* ou *cryptogramme*), et d'une *clé secrète,* et qui est attachée aux données afin de permettre l'*authentification des données*.

NOTE – La fonction utilisée pour générer le code d'authentification de message est généralement une fonction unilatérale.

08.06.23
détection de modification
Procédure utilisée pour détecter les modifications, accidentelles ou intentionnelles, de *données*.

08.06.24
code de détection de modification
Chaîne de bits qui est une fonction des *données* auxquelles elle est attachée afin de permettre la *détection de modification.*

NOTES
1 – Le *message* correspondant (données plus code de détection de modification) peut alors être chiffré pour garantir le secret de l'*authentification des données.*
2 – La fonction utilisée pour générer le code de détection de modification doit être publique.

08.06.25
repudiation
The denial by one of the *entities* involved in a communication of having participated in all or part of the communication.

NOTE – In the description of techniques and mechanisms the term "non-repudiation" is often used to mean that none of the entities involved in a communication can deny its participation in the communication.

08.06.26
security filter
A *trusted computer system* that enforces a *security policy* on the *data* that pass through the system.

08.06.27
guard (in computer security)
A *functional unit* that provides a *security filter* between two *data processing systems* operating at different *security levels* or between a *user terminal* and a *database* to filter out *data* that the user is not authorized to *access*.

08.06.28
mutual suspicion
The relationship between interacting *entities* in which neither entity relies upon the other entity to function correctly or securely with respect to some property.

08.06.29
notarization
The registration of *data* with a trusted third party that allows the later assurance of the accuracy of the data's characteristics such as content, origin, time, and delivery.

08.06.30
traffic padding
A *countermeasure* that generates spurious *data* in *transmission media* to make *traffic analysis* or *decryption* more difficult.

08.06.31
virus signature
A unique *bit string* that is common to each copy of a particular *virus* and that may be used by a *scanning* * *program* to detect the presence of the virus.

08.06.32
anti-virus program
vaccine program
A *program* designed to detect *viruses* and possibly to suggest or take corrective action.

08.06.25
répudiation
Le fait, pour une des *entités* impliquées dans une communication, de nier avoir participé à tout ou partie de cette communication.

NOTE – Dans la description des techniques et des mécanismes, le terme «non-répudiation» est souvent utilisé pour signifier qu'aucune des entités impliquées dans une communication ne peut nier sa participation à la communication.

08.06.26
filtre de sécurité
Système informatique fiable qui applique une *politique de sécurité* aux *données* qui passent par lui.

08.06.27
gardien (en sécurité informatique)
Unité fonctionnelle qui fournit un *filtre de sécurité* entre deux *systèmes informatiques* opérant à des *niveaux de sécurité* différents ou entre un *terminal d'utilisateur* et une *base de données* pour éliminer les *données* auxquelles l'utilisateur n'est pas autorisé à avoir accès.

08.06.28
méfiance réciproque
méfiance mutuelle
Relation entre deux *entités* agissant l'une sur l'autre, dans laquelle aucune des deux entités ne suppose que l'autre entité fonctionne correctement ou de manière sûre pour une propriété donnée.

08.06.29
notarisation
Enregistrement de *données* chez un tiers de confiance permettant de s'assurer ultérieurement de l'exactitude des caractéristiques des données telles que le contenu, l'origine, l'heure, et la remise.

08.06.30
bourrage
Mesure de prévention consistant à générer des *données* parasites dans des *supports de transmission* afin de rendre *l'analyse du trafic* et le *déchiffrement* plus difficiles.

08.06.31
signature (de virus)
Chaîne de bits qui est commune à chacune des copies d'un *virus* particulier et qui peut être utilisée par un *programme* de *balayage* pour détecter la présence du virus.

08.06.32
vaccin
détecteur de virus
antivirus
programme antivirus
Programme conçu pour détecter des *virus* et éventuellement pour suggérer ou appliquer des remèdes.

08.07 Recovery of data

08.07.01
data restoration
The act of regenerating *data* that have been lost or contaminated.

NOTE – Methods include *copying* data from archive, *data reconstruction* from source data, or *data reconstitution* from alternative sources.

08.07.02
data reconstruction
A method of *data restoration* by analyzing original sources.

08.07.03
data reconstitution
A method of *data restoration* by assembling *data* from components available in alternative sources.

08.07.04
backup procedure
A procedure to provide for *data restoration* in case of a *failure* or a disaster.

Example: Making *backup files*.

08.07.05
backup file
A *file* made for possible later *data restoration*.

Example: A copy of a file preserved at an alternate site.

08.07.06
backward recovery
The *data reconstitution* of an earlier version of *data* by using a later version and data recorded in a journal.

08.07.07
forward recovery
The *data reconstitution* of a later version of *data* by using an earlier version and data recorded in a journal.

08.07.08
to **archive**
To *store* * *backup files* and any associated journals, usually for a given period of time.

08.07 Récupération des données

08.07.01
restauration des données
Fait de régénérer des *données* qui ont été perdues ou contaminées.

NOTE – Les méthodes de restauration des données comprennent la *copie* à partir d'une archive, la *reconstruction des données* à partir de données sources ou la *reconstitution des données* à partir d'autres sources.

08.07.02
reconstruction des données
Méthode de *restauration des données* utilisant l'analyse des sources orginales.

08.07.03
reconstitution des données
Méthode de *restauration des données* par assemblage de données disponibles dans d'autres sources.

08.07.04
procédure de sauvegarde
Procédure destinée à permettre la *restauration des données* en cas de *défaillance* ou de désastre.

Exemple: créer des *fichiers de secours*.

08.07.05
fichier de sauvegarde
fichier de secours
Fichier créé pour une éventuelle *restauration de données* ultérieure.

Exemple: copie d'un fichier conservée dans un autre site.

08.07.06
restauration par régression
restauration par mise à jour en amont
restauration par annulation de mise à jour
Reconstitution des données d'une version antérieure de *données* en utilisant une version plus récente et des données enregistrées dans un journal.

08.07.07
restauration par progression
restauration par mise à jour en aval
Reconstitution des données d'une version récente de *données* en utilisant une version ancienne et des *données* enregistrées dans un journal.

08.07.08
archivage
Stockage de *fichiers de sauvegarde* et des journaux associés à ces fichiers, généralement pendant une période déterminée.

08.07.09
archive file
A *file* set aside for later research or *verification*, for security, or for any other purpose.

08.07.10
archived file
A *file* for which an *archive file* exists.

08.07.11
cold site
shell site
A facility with at least the equipment necessary to support the installation and operation of an alternative *data processing system*.

08.07.12
hot site
A fully equipped *computer center* that provides an immediate alternative *data processing* capability.

08.07.13
contingency plan
disaster recovery plan
A plan for *backup procedures*, emergency response, and post-disaster recovery.

08.08 Copy protection

08.08.01
copy protection
The use of special techniques to detect or prevent the unauthorized *copying* of *data*, * *software*, or *firmware*.

08.08.02
software piracy
The unauthorized use, *copying*, or distribution of *software* products.

NOTE – This is an revised version of the definition in ISO/IEC 2382-1:1993.

08.08.03
padlocking
The use of special techniques to protect *data* or *software* against unauthorized *copying*.

08.08.04
bad sectoring
A technique for *copy protection* in which bad *sectors* are intentionally *written* on a *disk*.

08.08.05
checking code
Machine instructions that *read* part of a *disk* to determine whether it is an unauthorized copy.

08.07.09
fichier d'archives
Fichier mis de côté pour des recherches ou des *vérifications* ultérieures, par mesure de sécurité ou pour tout autre besoin.

08.07.10
fichier archivé
Fichier pour lequel il existe un *fichier d'archives*.

08.07.11
salle blanche
Ensemble de moyens comportant au moins l'équipement nécessaire pour permettre l'installation et le fonctionnement d'un *système informatique* de remplacement.

08.07.12
centre de secours immédiat
site de secours
Centre de traitement de l'information totalement équipé, qui peut immédiatement prendre le relais d'un *traitement des données*.

08.07.13
plan de secours
plan de reprise après sinistre
Plan comportant des *procédures de sauvegardes*, des solutions d'urgence et une remise en ordre à la suite d'un désastre.

08.08 Protection contre la copie

08.08.01
protection contre la copie
Recours à des techniques spéciales pour détecter ou éviter la *copie* non autorisée de *données,* de *logiciels*, ou de *micrologiciels.*

08.08.02
piratage informatique
piratage logiciel
Utilisation, *copie* ou distribution non autorisées de *logiciels*.

NOTE – Cette définition est une version révisée de celle contenue dans l'ISO/CEI 2382-1:1993.

08.08.03
verrouillage logiciel
Utilisation de techniques spéciales pour protéger d'une copie illicite les *données* ou le *logiciel*.

08.08.04
sectorisation truquée
Technique de *protection contre la copie* selon laquelle de mauvais *secteurs* sont volontairement *écrits* sur une *disque.*

08.08.05
code de vérification
Instructions machine qui *lisent* une partie d'une *disque* pour vérifier s'il s'agit d'une copie non autorisée.

08.08.06
extra sector
A *sector* that is *written* on a *track* in excess of the standard number of sectors, as part of a method of *copy protection*.

08.08.07
extra track
A *track* that is *written* on a *disk* in excess of the standard number of *tracks*, as part of a method of *copy protection*.

08.08.08
fake sector
A *sector* consisting of a header but no *data*, used in large numbers on a *disk* to cause an unauthorized *copying * program* to fail to copy the disk.

08.08.09
offset track
A *track * written* at a nonstandard position on a *disk*, as part of a method of *copy protection*.

08.08.10
sector alignment
A technique for *copy protection* that determines whether a *disk* is an unauthorized copy by checking whether *sectors* are positioned properly from *track* to track.

08.08.11
spiral track
A *track* with a spiral shape on a *disk*, as part of a method of *copy protection*.

08.08.12
supersector
An oversized *sector * written* on a *disk*, as part of a method of *copy protection*.

08.08.13
weak bit
A *bit* intentionally *written* on a *disk* with a weak magnetic field strength that may be interpreted as zero or one and that is written as part of a method of *copy protection*.

08.08.14
wide track
A set of two or more adjacent *tracks* on a *disk* onto which the same *data* are *written*, as part of a method of *copy protection*.

08.08.06
secteur excédentaire
*Secteur * écrit* sur une *piste* en supplément du nombre normal de secteurs, en tant que technique de *protection contre la copie*.

08.08.07
piste excédentaire
*Piste * écrite* sur une *disque* en supplément du nombre normal de pistes, en tant que technique de *protection contre la copie*.

08.08.08
secteur leurre
Secteur comportant un *en-tête* mais pas de *données*, utilisé en grand nombre sur une *disque* pour faire en sorte qu'un *programme* de copie illicite manque de *mémoire* et ne puisse pas *copier* le disque.

08.08.09
piste décalée
*Piste * écrite* à une position anormale sur une *disque*, en tant que technique de *protection contre la copie*.

08.08.10
alignement de secteur
Technique de *protection contre la copie* qui détermine si une *disque* est une copie non autorisée en vérifiant si les *secteurs* sont correctement positionnés de *piste* en piste.

08.08.11
piste en spirale
piste spiralée
Piste en spirale sur une *disque,* en tant que technique de *protection contre la copie.*

08.08.12
supersecteur
Secteur surdimensionné *écrit* sur une *disque*, en tant que technique de *protection contre la copie.*

08.08.13
bit faible
Bit écrit sur une *disque* avec un champ magnétique volontairement faible qui peut être interprété comme zéro ou un et qui est *écrit* en tant que technique de *protection contre la copie.*

08.08.14
piste large
Ensemble d'au moins deux *pistes* adjacentes d'un *disque* sur lesquelles les mêmes *données* sont *écrites*, participant à une technique de *protection contre la copie.*

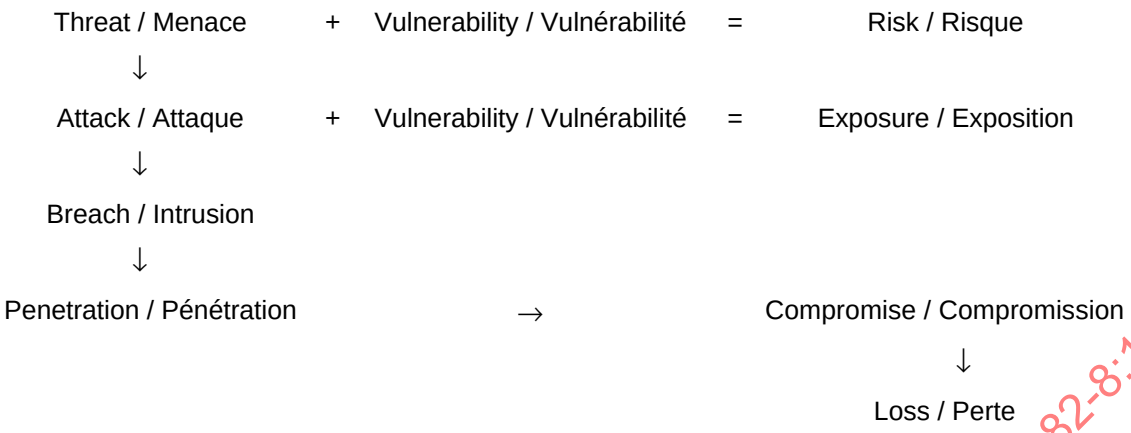

Figure 1 — Levels of security violations
Figure 1 — Niveaux d'atteintes à la sécurité

English alphabetical index