NORME INTERNATIONALE

ISO/CEI 10181-5

Première édition
1996-09-15

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts: Cadre de confidentialité

Information technology — Open Systems Interconnection — Security frameworks for open systems: Confidentiality framework

Numéro de référence
ISO/CEI 10181-5:1996(F)

Sommaire

Version française tirée en 1997

Imprimé en Suisse

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 ou 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 10181-5 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 21, *Interconnexion des systèmes ouverts, gestion des données et traitement distribué ouvert*, en collaboration avec l'UIT-T. Le texte identique est publié en tant que Recommandation UIT-T X.814.

L'ISO/CEI 10181 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts*:

— *Partie 1: Vue d'ensemble*

— *Partie 2: Cadre d'authentification*

— *Partie 3: Cadre de contrôle d'accès*

— *Partie 4: Cadre de non-répudiation*

— *Partie 5: Cadre de confidentialité*

— *Partie 6: Cadre d'intégrité*

— *Partie 7: Cadre d'audit de sécurité*

Les annexes A à E de la présente partie de l'ISO/CEI 10181 sont données uniquement à titre d'information.

Introduction

De nombreuses applications de systèmes ouverts ont des exigences en matière de sécurité qui dépendent des mesures prises pour empêcher la divulgation des informations. Ces exigences peuvent inclure la protection des informations utilisées pour assurer d'autres services de sécurité tels que l'authentification, le contrôle d'accès ou l'intégrité qui, si elles sont connues d'un «attaquant», risquent de réduire ou d'annihiler l'efficacité de ces services.

La confidentialité est une propriété selon laquelle aucune information n'est communiquée ou divulguée à des individus, entités ou processus non autorisés.

La présente Recommandation | Norme internationale définit un cadre général pour la fourniture de services de confidentialité.

Page blanche

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DE SYSTÈMES OUVERTS (OSI) – CADRES DE SÉCURITÉ POUR LES SYSTÈMES OUVERTS: CADRE DE CONFIDENTIALITÉ

1 Domaine d'application

La présente Recommandation | Norme internationale sur les cadres de sécurité pour les systèmes ouverts couvre l'application des services de sécurité dans un environnement de systèmes ouverts, où le terme «systèmes ouverts» s'applique notamment à des domaines tels que les bases de données, les applications distribuées, le traitement réparti ouvert (ODP) et l'interconnexion OSI. Les cadres de sécurité ont pour but de définir les moyens d'assurer la protection pour les systèmes et les objets à l'intérieur des systèmes, ainsi que les interactions entre les systèmes. Ils ne couvrent pas la méthodologie de construction des systèmes ou mécanismes.

Les cadres de sécurité couvrent à la fois les éléments de données et les séquences d'opérations (mais non les éléments de protocole) qui peuvent servir à obtenir des services de sécurité spécifiques. Ces services de sécurité peuvent s'appliquer aux entités communicantes des systèmes ainsi qu'aux données échangées entre les systèmes et aux données gérées par les systèmes.

La présente Recommandation | Norme internationale qui traite de la confidentialité des informations lors de l'extraction, du transfert et de la gestion des données

1) définit les concepts élémentaires de confidentialité;
2) identifie les classes possibles de mécanismes de confidentialité;
3) classe et identifie les fonctionnalités pour chaque classe de mécanisme de confidentialité;
4) identifie les ressources de gestion requises pour prendre en charge les diverses classes de mécanisme de confidentialité;
5) examine l'interaction des mécanismes de confidentialité et des services supports avec d'autres services et mécanismes de sécurité.

Plusieurs types de normes peuvent utiliser ce cadre de sécurité, notamment

1) les normes qui incorporent le concept de confidentialité;
2) les normes qui spécifient des services abstraits incluant la confidentialité;
3) les normes qui spécifient les utilisations d'un service de confidentialité;
4) les normes qui spécifient les moyens d'assurer la confidentialité dans une architecture de système ouvert;
5) les normes qui spécifient les mécanismes de confidentialité.

De telles normes peuvent utiliser ce cadre de sécurité comme indiqué ci-dessous:

- les normes des types 1), 2), 3), 4) et 5) peuvent utiliser la terminologie de ce cadre de sécurité;
- les normes des types 2), 3), 4) et 5) peuvent utiliser les fonctionnalités définies à l'article 7 de ce cadre de sécurité;
- les normes du type 5) peuvent être fondées sur les classes de mécanisme définies à l'article 8 de ce cadre de sécurité.

Comme avec d'autres services de sécurité, la confidentialité ne peut être assurée que dans le contexte d'une politique de sécurité déterminée pour une application particulière. Les définitions de politiques de sécurité spécifiques sortent du cadre de la présente Recommandation | Norme internationale.

La présente Recommandation | Norme internationale n'a pas pour but de spécifier les détails des échanges de protocole qu'il convient d'effectuer pour assurer la confidentialité.

La présente Recommandation | Norme internationale ne spécifie pas les mécanismes particuliers nécessaires pour assurer ces services de confidentialité ni les détails complets des services et protocoles de gestion de sécurité. Les mécanismes génériques nécessaires pour assurer la confidentialité sont décrits à l'article 8.

Certaines des procédures décrites dans ce cadre de sécurité assurent la confidentialité par l'application de techniques cryptographiques. Ce cadre de sécurité ne dépend pas de l'utilisation d'algorithmes cryptographiques ou autres particuliers mais certaines classes de mécanisme de confidentialité peuvent dépendre de propriétés d'algorithme particulières.

NOTE – Bien que l'ISO ne normalise pas les algorithmes cryptographiques, elle normalise néanmoins les procédures utilisées pour les enregistrer dans l'ISO/CEI 9979:1991 – Procédures pour l'enregistrement des algorithmes cryptographiques.

Ce cadre de sécurité s'applique à la mise en œuvre de la confidentialité lorsque les informations sont représentées par des données dont la lecture est accessible à d'éventuels «attaquants». Son domaine d'application englobe la confidentialité du flux de trafic.

2 Références normatives

Les Recommandations et les Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes Recommandations et Normes sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation | Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations de l'UIT-T en vigueur.

2.1 Recommandations | Normes internationales identiques

- Recommandation UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: le modèle de référence de base.*
- Recommandation UIT-T X.233 (1993) | ISO/CEI 8473-1:1994, *Technologies de l'information – Protocole assurant le service réseau en mode sans connexion de l'interconnexion de systèmes ouverts: spécification du protocole.*
- Recommandation UIT-T X.273 (1994) | ISO/CEI 11577:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole de sécurité de la couche réseau.*
- Recommandation UIT-T X.274 (1994) | ISO/CEI 10736:1995, *Technologies de l'information – Télécommunications et échange d'informations entre systèmes – Protocole de sécurité de la couche transport.*
- Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général.*
- Recommandation UIT-T X.812 (1995) | ISO/CEI 10181-3:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: contrôle d'accès.*

2.2 Paires de Recommandations | Normes internationales équivalentes par leur contenu technique

- Recommandation X.800 du CCITT (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*

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

3 Définitions

Pour les besoins de la présente Recommandation | Norme internationale, les définitions suivantes s'appliquent.

3.1 Définitions du modèle de référence de base

La présente Recommandation | Norme internationale utilise les termes généraux relatifs à la sécurité définis dans la Rec. UIT-T X.200 | ISO/CEI 7498-1 et énumérés ci-dessous:

a) connexion (N);

b) entité (N);

c) fonctionnalité (N);

d) couche (N);

e) PDU (N);

f) SDU (N);

g) service (N);

h) données sans connexion (N);

i) données d'utilisateur (N);

j) segmentation.

3.2 Définitions de l'architecture de sécurité

La présente Recommandation I Norme internationale utilise les termes suivants définis dans la Rec. X.800 du CCITT I ISO 7498-2:

a) menace active;

b) confidentialité;

c) déchiffrement (decipherment);

d) déchiffrement (decryption);

e) chiffrement (encipherment);

f) chiffrement (encryption);

g) politique de sécurité fondée sur l'identité;

h) clé;

i) menace passive;

j) contrôle de routage;

k) politique de sécurité fondée sur des règles;

l) sensibilité;

m) analyse du trafic;

n) bourrage.

3.3 Définitions de l'aperçu général des cadres de sécurité

La présente Recommandation I Norme internationale utilise les termes généraux relatifs à la sécurité définis dans la Rec. UIT-T X.810 I ISO/CEI 10181-1 et énumérés ci-dessous:

a) clé secrète;

b) clé privée;

c) clé publique.

3.4 Définitions additionnelles

Pour les besoins de la présente Recommandation I Norme internationale, les définitions suivantes s'appliquent:

3.4.1 environnement protégé par la confidentialité: Environnement qui empêche la divulgation non autorisée d'informations en prévenant toute inspection non autorisée des données ou toute obtention non autorisée d'informations sensibles par l'inspection des données. Les informations sensibles peuvent inclure une partie ou la totalité des attributs de données (valeur, taille, existence, etc.).

3.4.2 données protégées par la confidentialité: Données et tous attributs associés contenus dans un environnement protégé par la confidentialité.

NOTE – Un environnement protégé par la confidentialité peut également protéger une partie (ou la totalité) des attributs des données protégées par la confidentialité.

3.4.3 informations protégées par la confidentialité: Informations dont tous les codages concrets (c'est-à-dire les données) sont protégés par la confidentialité.

3.4.4 dissimulation: Opération qui applique une protection par confidentialité à des données non protégées ou une protection par confidentialité supplémentaire à des données déjà protégées.

3.4.5 révélation: Opération qui supprime une partie ou la totalité de la protection par confidentialité appliquée précédemment.

3.4.6 informations de confidentialité «dissimulation»: Informations utilisées pour exécuter l'opération de **dissimulation**.

3.4.7 informations de confidentialité «révélation»: Informations utilisées pour exécuter l'opération de révélation.

3.4.8 attaque directe: Attaque d'un système fondé sur les déficiences des algorithmes, des principes ou des propriétés sur lesquels s'appuie un mécanisme de sécurité.

3.4.9 attaque indirecte: Attaque d'un système qui n'est pas fondé sur les déficiences d'un mécanisme de sécurité particulier (par exemple, attaques qui contournent le mécanisme ou qui dépendent de l'utilisation incorrecte du mécanisme par le système).

4 Abréviations

Pour les besoins de la présente Recommandation | Norme internationale, les abréviations suivantes sont utilisées:

HCI Informations de confidentialité dissimulation (*hiding confidentiality information*)

PDU Unité de données de protocole (*protocol data unit*)

RCI Informations de confidentialité révélation (*revealing confidentiality information*)

SDU Unité de données de service (*service data unit*)

5 Présentation générale de la confidentialité

5.1 Principes de base

Le but du service de confidentialité est de faire en sorte que les informations ne soient communiquées qu'à des parties autorisées. Dans la mesure où les informations sont représentées par des données et où ces données peuvent entraîner des modifications contextuelles (par exemple, des manipulations de fichiers peuvent entraîner des modifications de répertoire ou des modifications du nombre d'emplacements de mise en mémoire disponibles), les informations peuvent être obtenues de diverses manières à partir d'une donnée, comme indiqué ci-après:

1) par la compréhension de la sémantique des données (par exemple, la valeur des données);
2) par l'utilisation des attributs associés des données (par exemple, existence, date de création, taille, date de la dernière mise à jour, etc.) pour en tirer des déductions;
3) par l'examen du contexte des données, c'est-à-dire des autres objets de données qui lui sont associés;
4) par l'observation des variations dynamiques de la représentation.

On peut protéger les informations en veillant à ce que la communication des données soit limitée aux parties autorisées ou en représentant les données de telle sorte que leur sémantique ne reste accessible qu'à ceux qui possèdent certaines informations critiques. Pour qu'une protection par la confidentialité soit efficace, il faut que les informations de contrôle nécessaires (telles que les clés et autres informations RCI) soient protégées. Cette protection peut être assurée par des mécanismes qui sont différents de ceux que l'on utilise pour protéger les données (par exemple, les clés cryptographiques peuvent être protégées par des moyens physiques).

Les notions d'environnements protégés et d'environnements de chevauchement protégés sont utilisées dans ce cadre de sécurité. Les données contenues dans les environnements protégés sont protégées par l'application d'un mécanisme (ou de mécanismes) de sécurité particulier(s). Toutes les données contenues dans un environnement protégé sont donc protégées de la même façon. Lorsque deux environnements ou plus se chevauchent, les données contenues dans la zone de chevauchement bénéficient d'une protection multiple. On peut en déduire que la protection continue de données transférées d'un environnement à l'autre implique nécessairement l'existence d'environnements de chevauchement protégés.

5.1.1 Protection des informations

On réalise la communication ou la mise en mémoire d'informations en représentant les informations sous la forme d'éléments de données. Les mécanismes de confidentialité assurent la protection contre la divulgation d'informations en protégeant les parties ou la totalité des éléments de données énumérées au 5.1 ci-dessus.

Pour assurer la confidentialité, on peut utiliser notamment les moyens suivants:

1) empêcher que l'on connaisse l'existence des données ou les caractéristiques des données (telles que la taille ou la date de création des données);
2) empêcher l'accès à la lecture des données;
3) empêcher que l'on connaisse la sémantique des données.

Les mécanismes de confidentialité assurent la protection contre la divulgation des informations

1) en empêchant la divulgation du mode de représentation des éléments d'information; ou
2) en empêchant la divulgation des règles de représentation.

Dans le second cas, on peut assurer la protection contre la divulgation de l'existence ou d'autres attributs d'un élément de données en combinant plusieurs éléments de données en un élément de données composite et en empêchant la divulgation des règles de représentation de l'objet composite.

5.1.2 Opérations de dissimulation et de révélation

L'opération de **dissimulation** peut être modélisée sous la forme d'un transfert d'informations d'un environnement A à (B), environnement de chevauchement de A avec un autre environnement C. L'opération de révélation peut être considérée comme étant l'opposé de l'opération de dissimulation. Ces opérations sont illustrées par un graphique dans l'Annexe B.

Lorsque des informations sont transférées d'un environnement protégé par un mécanisme de confidentialité à un environnement protégé par un autre mécanisme de confidentialité:

1) si l'opération de **dissimulation** du second mécanisme précède l'opération de **révélation** du premier mécanisme, les informations sont protégées d'une manière continue;
2) si l'opération de **révélation** du premier mécanisme précède l'opération de **dissimulation** du second mécanisme, les informations ne sont pas protégées d'une manière continue.

Pour que le point 1) ci-dessus soit possible, une certaine forme de commutativité doit exister entre l'opération de **révélation** de l'ancien mécanisme et l'opération de **dissimulation** du nouveau mécanisme. A titre d'exemple d'opérations de **dissimulation** et de **révélation** avec des propriétés commutatives, on peut citer le cas où un environnement est protégé par le contrôle d'accès ou par des moyens physiques et où l'autre environnement est protégé par des transformations cryptographiques.

La confidentialité a une incidence, comme indiqué ci-après, sur l'extraction, le transfert et la gestion des informations:

1) la confidentialité est assurée, dans le transfert d'informations utilisant l'interconnexion OSI, lorsque l'opération de **dissimulation**, l'opération de transfert utilisant une fonctionnalité (N-1), et l'opération de **révélation** sont combinées pour former la partie transmission d'un service (N);
2) la confidentialité est assurée, dans l'extraction et la mise en mémoire de données, lorsque l'opération de **dissimulation**, l'opération de mise en mémoire et d'extraction, et l'opération de **révélation** sont combinées pour former un service de mise en mémoire et d'extraction d'un niveau plus élevé;
3) d'autres formes de confidentialité peuvent être assurées par la combinaison des opérations de **dissimulation** et de **révélation** avec d'autres opérations (par exemple, celles qui sont utilisées pour les besoins de la gestion des données).

Avec certains mécanismes de confidentialité, la fonction de **dissimulation** divulgue une partie des données protégées par la confidentialité à l'utilisateur du service avant que la fonction ait achevé le traitement de toutes les données. De même, avec certains mécanismes, la fonction de **révélation** peut commencer à travailler sur la partie traitement d'un élément de données protégé par la confidentialité avant même qu'il soit totalement disponible. Ainsi, un élément de données peut comprendre simultanément des parties qui ne sont pas encore **dissimulées**, des parties qui sont **dissimulées** et des parties qui ont été **révélées**.

5.2 Types de services de confidentialité

Les services de confidentialité peuvent être classés selon le type de protection des informations qu'ils assurent.

Les types de protection des informations sont les suivants:

1) protection de la sémantique des données;
2) protection de la sémantique des données et des attributs associés;
3) protection de la sémantique des données, des attributs associés et de toute information susceptible d'être obtenue à partir des données en question.