RAPPORT TECHNIQUE

ISO/CEI TR 13594

Première édition
1995-12-15

Technologies de l'information — Modèle de sécurité des couches inférieures

Information technology — Lower layers security

Numéro de référence
ISO/CEI TR 13594:1995(F)

Sommaire

Version française tirée en 1996

Imprimé en Suisse

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment le système spécialisé de normalisation mondiale. 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.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Exceptionnellement, un comité technique peut proposer la publication d'un rapport technique de l'un des types suivants:

— type 1, lorsque, en dépit de maints efforts, l'accord requis ne peut être réalisé en faveur de la publication d'une Norme internationale;

— type 2, lorsque le sujet en question est encore en cours de développement technique ou lorsque, pour toute autre raison, la possibilité d'un accord pour la publication d'une Norme internationale peut être envisagée pour l'avenir mais pas dans l'immédiat;

— type 3, lorsqu'un comité technique a réuni des données de nature différente de celles qui sont normalement publiées comme Normes internationales (ceci pouvant comprendre des informations sur l'état de la technique, par exemple).

Les rapports techniques des types 1 et 2 font l'objet d'un nouvel examen trois ans au plus tard après leur publication afin de décider éventuellement de leur transformation en Normes internationales. Les rapports techniques du type 3 ne doivent pas nécessairement être révisés avant que les données fournies ne soient plus jugées valables ou utiles.

L'ISO/CEI TR 13594, rapport technique du type 3, a été élaboré par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, en collaboration avec l'UIT-T. Le texte identique est publié en tant que Recommandation UIT-T X.802.

Introduction

La présente Recommandation I Rapport technique décrit les aspects inter-couches de la fourniture des services de sécurité dans les couches inférieures du Modèle de référence OSI (couches transport, réseau, liaison de données et physique). Elle décrit les concepts architecturaux communs à ces couches, la base des interactions entre couches relatives à la sécurité, et le positionnement des protocoles de sécurité dans les couches inférieures.

Page blanche

RAPPORT TECHNIQUE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – MODÈLE DE SÉCURITÉ DES COUCHES INFÉRIEURES

1 Domaine d'application

La présente Recommandation | Rapport technique décrit les aspects inter-couches de la fourniture de services de sécurité dans les couches inférieures du Modèle de référence OSI (couches transport, réseau, liaison de données et physique).

La présente Recommandation | Rapport technique décrit:

a) les concepts architecturaux communs aux couches inférieures sur la base des éléments définis dans la Rec. X.800 du CCITT | ISO 7498-2;

b) les bases des interactions relatives à la sécurité entre les protocoles des couches inférieures;

c) les bases de toute interaction relative à la sécurité entre couches inférieures et couches supérieures de l'OSI;

d) le positionnement des protocoles de sécurité par rapport aux autres protocoles des couches inférieures, et le rôle relatif de tels positionnements.

Il ne doit pas y avoir de conflit entre les protocoles de sécurité des couches inférieures et le modèle décrit dans la présente Recommandation | Rapport technique.

La Rec. X.500 du CCITT | ISO/CEI 9594-1 identifie les services de sécurité qui relèvent de chacune des couches inférieures du Modèle de référence OSI.

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 | Rapport technique. 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 | Rapport technique 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 de systèmes ouverts – Modèle de référence: 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.234 (1994) | ISO/CEI 8602:1995, *Technologies de l'information – Protocole assurant le service de transport en mode sans connexion de l'interconnexion des systèmes ouverts (OSI).*
- Recommandation UIT-T X.273 (1994) | ISO/CEI 11577:1995, *Technologies de l'information – Interconnexion de 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.803 (1994) | ISO/CEI 10745:1994, *Technologies de l'information – Interconnexion de systèmes ouverts – Modèle de sécurité pour les couches supérieures.*
- Recommandation UIT-T X.810[1] | ISO/CEI 10181-1...[1], *Technologies de l'information – Interconnexion de systèmes ouverts – Cadre général de la sécurité dans les systèmes ouverts: Aperçu général.*
- Recommandation UIT-T X.812[1] | ISO/CEI 10181-3...[1], *Technologies de l'information – Interconnexion de systèmes ouverts – Cadre général de la sécurité dans 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.*
- Recommandation UIT-T X.224 (1993), *Protocole pour assurer le service de couche transport en mode connexion pour l'interconnexion de systèmes ouverts.*

  ISO/CEI 8073:1992, *Technologies de l'information – Télécommunications et échanges d'informations entre systèmes – Interconnexion de systèmes ouverts (OSI) – Protocole pour fourniture du service de transport en mode connexion.*
- Recommandation X.208 du CCITT (1988), *Spécification de la syntaxe abstraite numéro un (ASN.1).*

  ISO/CEI 8824:1990, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Spécification de la notation de syntaxe abstraite numéro 1 (ASN.1).*
- Recommandation X.209 du CCITT (1988), *Spécification des règles de codage de base pour la notation de syntaxe abstraite numéro un (ASN.1).*

  ISO/CEI 8825:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – Spécification de règles de base pour coder la notation de syntaxe abstraite numéro 1 (ASN.1).*

2.3 Autres références

- ISO/CEI 8208:1995, *Technologies de l'information – Communications de données – Protocole X.25 de couche paquet pour terminal de données.*
- Recommandation UIT-T X.25 (1993), *Interface entre équipement terminal de traitement de données et équipement de terminaison du circuit de données pour terminaux fonctionnant en mode paquet et raccordés par circuit spécialisé à des réseaux publics pour données.*
- ISO 8648:1988, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Organisation interne de la couche Réseau.*
- ISO 9542:1988[2], *Systèmes de traitement de l'information – Téléinformatique – Protocole de routage d'un système d'extrémité à un système intermédiaire à utiliser conjointement avec le protocole fournissant le service de réseau en mode sans connexion (ISO 8473).*
- ISO/CEI 10589:1992, *Technologies de l'information – Communication de données et échange d'informations entre systèmes – Protocole intra-domaine de routage d'un système intermédiaire à un système intermédiaire à utiliser conjointement avec le protocole fournissant le service de réseau en mode sans connexion (ISO 8473).*
- ISO/CEI 10747:1994, *Technologies de l'information – Télécommunications et échange d'informations entre systèmes – Protocole pour échange d'informations inter-domaine de routage parmi les systèmes intermédiaires supportant la transmission de PDU de l'ISO 8473.*

---

[1] Actuellement à l'état de projet.

[2] Actuellement en révision.

3 Définitions

3.1 Définitions du modèle de référence OSI

La présente Recommandation | Rapport technique utilise les termes suivants définis dans la Rec. UIT-T X.200 | ISO/CEI 7498-1:

– qualité de service

3.2 Définitions du cadre général de la sécurité dans les systèmes ouverts

La présente Recommandation | Rapport technique utilise les termes suivants définis dans la Rec. UIT-T X.810 | ISO/CEI 10181-1:

– domaine de sécurité

3.3 Définitions de l'organisation interne de la couche réseau

La présente Recommandation | Rapport technique utilise les termes suivants définis dans ISO 8648:

a) protocole d'accès de sous-réseau;

b) système d'extrémité;

c) système intermédiaire.

3.4 Définitions supplémentaires

Pour les besoins de la présente Recommandation | Rapport technique les définitions suivantes s'appliquent:

3.4.1 protection de réflexion: Mécanisme de protection qui détecte le renvoi d'une unité de donnée protocolaire vers son expéditeur.

3.4.2 attributs d'association de sécurité: Collection des informations requises pour régir la sécurité des communications entre une entité et son entité homologue.

3.4.3 association de sécurité: Relation établie entre des entités communicantes de couches inférieures pour laquelle sont définis les attributs d'association de sécurité correspondants.

3.4.4 règles de sécurité: Information locale qui, pour les services de sécurité choisis, spécifie les mécanismes de sécurité sous-jacents à utiliser, y compris l'ensemble des paramètres nécessaires au fonctionnement de ces mécanismes.

NOTE – Les règles de sécurité sont une forme de règles d'interaction sûres telles que celles-ci sont définies dans le Modèle de sécurité pour les couches supérieures (Rec. UIT-T X.803 | ISO/CEI 10745).

4 Abréviations

ISN	Numéro de séquence d'intégrité (*integrity sequence number*)
SSAA	Ensemble d'attributs d'association de sécurité (*set of SA-attributes*)
NLSP	Protocole de sécurité de couche réseau (*network layer security protocol*)
NLSP-CO	Protocole NLSP en mode connexion (*NLSP connection mode*)
NLSP-CL	Protocole NLSP en mode sans connexion (*NLSP connectionless mode*)
QOS	Qualité de service (quality of service) (conformément à la définition de la Rec. X.200 du CCITT | ISO/CEI 7498-1)
SA	Association de sécurité (*security association*)
SA-ID	Identificateur d'association de sécurité (*security association identifier*)
SNAcP	Protocole d'accès de sous-réseau (*subnetwork access protocol*) (conformément à la définition de ISO 8648)
SNISP	Protocole indépendant de sécurité de sous-réseau (*subnetwork independent security protocol*)
TLSP	Protocole de sécurité de couche transport (*transport layer security protocol*)

5 Associations de sécurité

5.1 Vue d'ensemble

5.1.1 Chaque protocole de sécurité utilise un certain nombre de mécanismes de sécurité pour fournir des services de sécurité à la couche immédiatement supérieure. Les services de sécurité nécessaires aux couches supérieures peuvent être indiqués aux couches inférieures au moyen de fonctions locales de supervision de la sécurité. Pour établir des communications sécurisées, le protocole de sécurité et tous les mécanismes de sécurité nécessitent un supplément d'information par rapport à ce qui est codé dans les PDU. Il s'agira par exemple de la spécification des mécanismes à utiliser par le protocole et, pour chaque mécanisme, d'informations spécifiques comme les clés nécessaires au mécanisme de chiffrement. Chaque élément d'information additionnelle est connu sous le nom d'attribut d'association de sécurité.

5.1.2 Les attributs d'association de sécurité peuvent être placés dans une entité de protocole au moyen d'un certain nombre de mécanismes de positionnement. Il s'agira par exemple des mécanismes suivants:

a) positionnement pendant la fabrication d'un dispositif;

b) positionnement pendant l'initialisation d'un dispositif;

c) positionnement via une interface manuelle, par exemple par les commandes des panneaux de face avant;

d) positionnement par la gestion de sécurité des systèmes OSI;

e) positionnement par la gestion de sécurité de couche OSI;

f) positionnement par la gestion de sécurité des opérations OSI.

5.1.3 Les attributs d'association de sécurité (SA) peuvent être positionnés à n'importe quel moment avant la communication à laquelle ils se rapportent. Quand des ensembles compatibles d'attributs d'associations de sécurité (SSAA) sont positionnés dans chaque entité de protocole, on dit qu'une association de sécurité existe entre ces entités.

5.1.4 Des ensembles SSAA (et des associations de sécurité) peuvent exister avec différents niveaux de granularité. Parfois il est utile de pouvoir se référer à des ensembles SSAA de granularité différente. Par exemple, l'ensemble SSAA défini par un ensemble convenu de règles de sécurité (ASSR) pourrait être appelé SSAA ASSR. Ou une clef appariée pourrait être établie entre deux entités de protocole pour être employée sur un certain nombre d'instances de couples d'adresses ayant des sources et destinations communes. De façon similaire le SSAA pour une instance de communication pourrait être dénommé instance de communication SSAA. De même l'ensemble SSAA pour une PDU orientée connexion pourrait être appelée SSAA CO PDU.

5.1.5 En règle générale, les attributs d'associations SA doivent être placés dans l'entité de protocole par un moyen sécurisé afin d'en préserver la sécurité. Ceci implique que les attributs d'associations de sécurité soient positionnés par un moyen physique sécurisé ou à l'aide d'une association de sécurité existante qui aura préalablement été positionnée à cette fin.

5.1.6 Les ensembles d'attributs SSAA qui font partie d'une association de sécurité sont souvent désignés par un identificateur dénommé SA-ID ayant une signification locale. A un instant donné, certains éléments de l'ensemble d'attributs d'association de sécurité peuvent être indéfinis. Au moment de l'initialisation d'une communication sécurisée, l'ensemble des attributs SSAA ne sera généralement pas complètement valué, et les échanges initiaux seront utilisés pour compléter la valuation des attributs SSAA avant l'échange des données utilisateur.

5.1.7 Afin de fournir une protection de répétition, il faut appliquer des contraintes à l'usage d'identificateurs SA-ID, leurs ensembles SSAA de référence et les attributs d'association SA.

a) Les identificateurs SA-ID ne peuvent pas être réutilisés avec la même clé de chiffrement.

b) Après qu'un quelconque attribut SA a été valué dans un ensemble SSAA identifié par un identificateur SA-ID, cet attribut ne pourra jamais être changé, à moins que le protocole de sécurité ne possède un moyen de signaler le changement aux entités en communication. Ceci implique que, pour autoriser un basculement de clé, un nouvel identificateur de SA-ID doit être utilisé avec des copies des anciens attributs SA et une nouvelle clé, à moins que le protocole de sécurité ne dispose d'un autre moyen de signaler le changement de clé (fonction assurée par exemple par l'unité de données protocolaires NLSP-CO CSC).

5.1.8 Le retrait de l'un quelconque des attributs de sécurité SSAA a pour effet de clôturer l'association de sécurité.

5.1.9 Certains attributs d'association de sécurité ont une signification pour une instance de communication (une PDU sans connexion ou une connexion). D'autres attributs d'association de sécurité ont une signification pour une seule PDU sur une connexion. Comme exemple de tels attributs, on citera les numéros de séquence d'intégrité (ISN) et les étiquettes de sécurité. Il peut sembler que la modification de ces attributs viole les contraintes citées au point b) du 5.1.7. Cependant, l'association de sécurité comprenant ces attributs SA n'est logiquement valide que pour la durée de vie d'une

seule PDU. Le numéro ISN joue le rôle d'une extension logique de l'identificateur SA-ID, et modifie par conséquent l'identificateur SA-ID en vigueur. L'étiquette de sécurité n'est alors valide que pour cette instance d'identificateur SA-ID étendu. Ainsi les contraintes sont-elles respectées. De tels attributs sont parfois qualifiés de «dynamiques».

5.1.10 Une part de la politique de sécurité va imposer des contraintes aux opérations de l'entité protocolaire. Cette partie de la politique de sécurité est appelée «ensemble de règles de sécurité pour l'entité protocolaire». Cet ensemble de règles peut imposer des contraintes à des composants tels que le mécanisme de sécurité à utiliser ainsi que les valeurs et le mécanisme de positionnement des attributs d'association de sécurité. L'ensemble des règles de sécurité définira aussi le mappage des services de sécurité sélectionnés sur les mécanisme utilisés par le protocole de sécurité. L'ensemble de règles de sécurité est une forme de règles d'interaction sécurisée.

5.1.11 Lorsqu'un tel ensemble est utilisé en exploitation intra ou inter domaines, il recevra un identificateur unique, et cet ensemble est alors appelé «ensemble mutuellement convenu de règles de sécurité (ASSR) (*agreed set of security rules*)». L'identificateur de l'ensemble ASSR peut être modifié lors de l'établissement de l'association de sécurité pour déterminer ou contraindre l'ensemble des règles de sécurité s'appliquant à l'ensemble des attributs et qui est défini pour l'association de sécurité. Les attributs d'association de sécurité, s'il y en a, doivent être établis en utilisant d'autres moyens, par exemple ceux qui sont énumérés au 5.1.2.

5.2 Etablissement d'associations de sécurité pour les couches inférieures

5.2.1 Afin de protéger une instance de communication (une SDU sans connexion ou une connexion) une association de sécurité doit être établie entre les entités en communication.

5.2.2 L'information constitutive d'une association de sécurité est soit une information statique qui peut être «négociée» lorsque l'association est établie et qui demeure ensuite fixe pour toute la durée de l'association, soit une information dynamique qui peut être mise à jour au cours d'une instance de communication.

5.2.3 Une association SA peut être établie par un protocole des couches OSI 1 à 4 par l'échange d'unités de données protocolaires (PDU) d'association de sécurité, ou par des mécanismes ne relevant pas des couches inférieures de l'OSI.

5.2.4 Avant d'établir une association de sécurité, chaque entité aura préétabli un ensemble de règles de sécurité commun, mutuellement accepté et uniquement défini, ainsi que les services de sécurité qui peuvent être sélectionnés.

5.2.5 Si l'association de sécurité doit être établie par l'échange de PDU d'association de sécurité, alors les éléments suivants doivent aussi être préétablis:

a) une sélection initiale des services de sécurité et, par conséquent, les mécanismes de sécurité à appliquer pendant l'établissement de l'association de sécurité;

b) les informations élémentaires d'encodage nécessaires pour établir l'association de sécurité.

5.2.6 A l'établissement d'une association SA, une entité détermine avec son homologue distant les informations partagées suivantes qui doivent rester inchangées (c'est-à-dire statiques) pour la durée de l'association:

a) les identificateurs SA-ID local et distant;

b) les services de sécurité sélectionnés pour être utilisés par les entités associées pour les instances de communication qu'elles établissent entre elles.

NOTE – Les services de sécurité à utiliser peuvent être sélectionnés parmi les services de sécurité préétablis.

c) les mécanismes et leurs propriétés à utiliser en conséquence des services de sécurité sélectionnés;

d) les clés partagées initialement pour l'intégrité, les mécanismes de chiffrement et l'authentification d'une instance de communication;

e) l'ensemble des étiquettes de sécurité et des adresses qui peuvent être utilisées dans cette association pour le contrôle d'accès.

5.2.7 Les identificateurs SA-ID et les clés partagées [points a) et b) ci-dessus] doivent être établis sur la base de chaque association. Les autres informations peuvent être préétablies. En plus, dans l'établissement d'une association de sécurité, l'identité du correspondant distant doit être validée pour assurer la fonction d'authentification de l'entité homologue.