Union internationale des télécommunications

UIT-T M.3016.2

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(04/2005)

SÉRIE M: GESTION DES TÉLÉCOMMUNICATIONS Y COMPRIS LE RGT ET MAINTENANCE DES RÉSEAUX

Réseau de gestion des télécommunications

Sécurité pour le plan de gestion: services de sécurité

Recommandation UIT-T M.3016.2

RECOMMANDATIONS UIT-T DE LA SÉRIE M

GESTION DES TÉLÉCOMMUNICATIONS Y COMPRIS LE RGT ET MAINTENANCE DES RÉSEAUX

Introduction et principes généraux de maintenance et organisation de la maintenance	M.10–M.299
Systèmes de transmission internationaux	M.300–M.559
Circuits téléphoniques internationaux	M.560–M.759
Systèmes de signalisation à canal sémaphore	M.760–M.799
Systèmes internationaux de télégraphie et de phototélégraphie	M.800–M.899
Liaisons internationales louées par groupes primaires et secondaires	M.900–M.999
Circuits internationaux loués	M.1000–M.1099
Systèmes et services de télécommunication mobile	M.1100–M.1199
Réseau téléphonique public international	M.1200–M.1299
Systèmes internationaux de transmission de données	M.1300–M.1399
Appellations et échange d'informations	M.1400–M.1999
Réseau de transport international	M.2000–M.2999
Réseau de gestion des télécommunications	**M.3000–M.3599**
Réseaux numériques à intégration de services	M.3600–M.3999
Systèmes de signalisation par canal sémaphore	M.4000–M.4999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T M.3016.2

Sécurité pour le plan de gestion: services de sécurité

Résumé

La présente Recommandation détermine les services de sécurité pour le plan de gestion en matière de gestion des télécommunications. Elle porte plus précisément sur l'aspect sécurité du plan de gestion pour les éléments de réseau (NE, *network element*) et les systèmes de gestion (MS, *management systems*), qui font partie de l'infrastructure des télécommunications.

Source

La Recommandation UIT-T M.3016.2 a été approuvée le 13 avril 2005 par la Commission d'études 4 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Introduction

Les télécommunications constituent une infrastructure indispensable pour les communications et l'économie mondiales, de sorte qu'il est essentiel de protéger par une sécurité appropriée les fonctions de gestion qui permettent d'en commander l'infrastructure. S'il existe un grand nombre de normes en ce qui concerne la sécurité de la gestion des réseaux de télécommunication, leur application laisse beaucoup à désirer et il n'y a guère de cohérence entre les divers équipements de télécommunication et les diverses composantes logicielles. La présente Recommandation détermine les services de sécurité qui permettront aux fabricants, aux vendeurs et aux fournisseurs de services de mettre sur pied une infrastructure de gestion des télécommunications qui soit sûre. Bien que l'ensemble des services et des mécanismes de sécurité visés constitue le dernier cri technologique, le progrès va se poursuivre et les conditions changer, de sorte que pour être utile la présente Recommandation devra évoluer au gré des changements: c'est pourquoi la présente Recommandation se propose de jeter des fondations sur lesquelles les fournisseurs de services pourront construire et ajouter des services et des mécanismes de sécurité propres à satisfaire leurs besoins particuliers.

La présente Recommandation fait partie des Recommandations UIT-T de la série M.3016.x dont l'objet est d'établir des lignes directrices et des orientations destinées à rendre sûr le plan de gestion de réseaux qui sont appelés à évoluer:

Recommandation UIT-T M.3016.0 – *Sécurité pour le plan de gestion: aperçu général*.

Recommandation UIT-T M.3016.1 – *Sécurité pour le plan de gestion: prescriptions de sécurité*.

Recommandation UIT-T M.3016.2 – *Sécurité pour le plan de gestion: services de sécurité*.

Recommandation UIT-T M.3016.3 – *Sécurité pour le plan de gestion: mécanisme de sécurité*.

Recommandation UIT-T M.3016.4 – *Sécurité pour le plan de gestion: formulaire de sécurité*.

Recommandation UIT-T M.3016.2

Sécurité pour le plan de gestion: services de sécurité

1 Domaine d'application

Les Recommandations UIT-T M.3016.1, M.3016.2 et M.3016.3 spécifient un ensemble de prescriptions, de services et de mécanismes pour assurer la sécurité des fonctions de gestion qui doivent être réalisées au profit d'une infrastructure de télécommunications. Etant donné que différentes administrations et organisations exigent des niveaux de sécurité différents, les Recommandations UIT-T M.3016.1-M.3016.3 n'indiquent pas si telle prescription, tel service ou tel mécanisme est obligatoire ou optionnel.

La présente Recommandation détermine les prescriptions des services de sécurité pour le plan de gestion en matière de gestion des télécommunications. Elle porte plus précisément sur l'aspect sécurité du plan de gestion pour les éléments de réseau (NE) et les systèmes de gestion (MS), qui font partie de l'infrastructure des télécommunications.

Générique par nature, la présente Recommandation ne spécifie pas, ni ne concerne les prescriptions d'une interface spécifique au réseau de gestion des télécommunications (RGT).

La présente Recommandation ne définit pas les prescriptions de sécurité ni les mécanismes de sécurité nécessaires à la mise en œuvre des prescriptions relatives aux services de sécurité.

La présente Recommandation fait partie des Recommandations UIT-T de la série M.3016.x. Les prescriptions, mécanisme et formulaire de sécurité sont spécifiés dans d'autres parties des Recommandations UIT-T de la série M.3016.x.

Le formulaire de sécurité présenté dans la Rec. UIT-T M.3016.4 est destiné à aider les organismes, administrations et autres organisations nationales/internationales à déterminer le caractère obligatoire ou optionnel des prescriptions ainsi que les valeurs et gammes de valeurs, etc., pour leur permettre d'implémenter leurs propres politiques de sécurité.

2 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

– Recommandation UIT-T E.408 (2004), *Prescriptions de sécurité des réseaux de télécommunication*.

– Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

– Recommandation UIT-T X.805 (2003), *Architecture de sécurité pour les systèmes assurant des communications de bout en bout*.

3 Définitions

La présente Recommandation utilise les termes ci-dessous empruntés à la Rec. UIT-T X.800:

– contrôle d'accès;

– authentification;
– confidentialité;
– intégrité des données;
– non-répudiation.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

NE élément de réseau (*network element*)

MS système de gestion (*management system*)

OAM&P exploitation, administration, maintenance et fourniture (*operations, administration, maintenance and provisioning*)

OSI interconnexion des systèmes ouverts (*open system interconnection*)

RGT réseau de gestion des télécommunications

5 Conventions

Dans les Recommandations UIT-T M.3016.1, M.3016.2 et M.3016.3, un descripteur, composé de trois lettres et d'un chiffre, est utilisé pour identifier les différentes prescriptions ainsi que les différents services ou mécanismes:

– REQ pour prescription (requirement);
– SER pour service;
– MEC pour mécanisme.

6 Services de sécurité

La Figure 1 décrit les relations existant entre les objectifs de sécurité, les menaces, les risques, les prescriptions de sécurité et les services. Elle décrit la procédure à utiliser pour déduire, à partir des "menaces" et des "objectifs de sécurité", des "prescriptions de sécurité" qui à leur tour seront appliquées moyennant un ensemble de services de sécurité. Ces "services" s'opposeront aux menaces et utiliseront des "mécanismes" qui emploieront à leur tour des "algorithmes de sécurité".

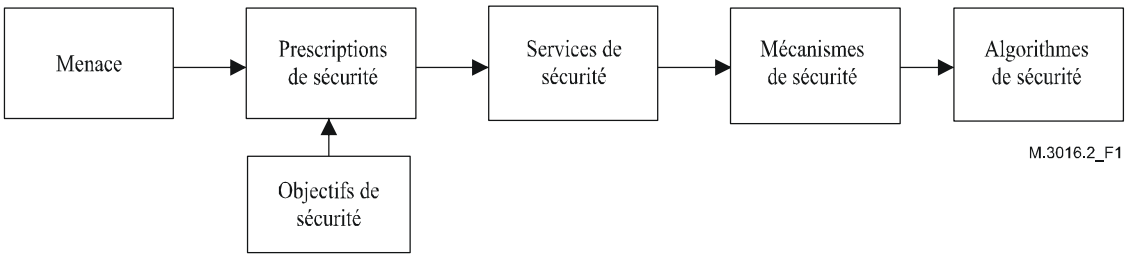

Figure 1/M.3016.2 – Cadre de sécurité

Emprunté à la Rec. UIT-T M.3016.0 (Tableau 4), le Tableau 1 ci-dessous donne un aperçu général des relations existant entre prescriptions et services de sécurité; il sert de base à l'organisation des autres documents de la série: par exemple, la Rec. UIT-T M.3016.1 est consacrée aux prescriptions fonctionnelles de sécurité, la Rec. UIT-T M.3016.2 traite des services de sécurité et la Rec. UIT-T M.3016.3 décrit les différents mécanismes correspondant à ces services.

Le présent paragraphe définit uniquement les services de sécurité, qui font l'objet de solutions normalisées, d'autres services possibles (par exemple, détection du déni de service) n'étant pas pris en considération.

Tableau 1/M.3016.2 – Mappage entre prescriptions et services de sécurité

Prescription fonctionnelle	Service de sécurité
Vérification d'identité	Authentification de l'utilisateur Authentification d'entité homologue Authentification de l'origine des données
Contrôle d'accès et d'autorisation	Contrôle d'accès
Protection de la confidentialité – données stockées	Contrôle d'accès
Protection de la confidentialité – données transférées	Confidentialité
Protection de l'intégrité des données – données stockées	Contrôle d'accès
Protection de l'intégrité des données – données transférées	Intégrité
Responsabilité	Non-répudiation
Journal d'activités	Trace d'audit
Compte rendu d'alarme de sécurité	Alarme de sécurité
Audit de sécurité	Trace d'audit
Protection du DCN	Inspection des paquets

La Tableau 2 ci-dessous présente l'organisation du présent paragraphe:

Tableau 2/M.3016.2 – Organisation du paragraphe 6

Paragraphe	Contenu
6.1	Services d'authentification, en particulier l'authentification de l'utilisateur, l'authentification d'entité homologue et l'authentification de l'origine des données
6.2	Service de contrôle d'accès
6.3	Service de confidentialité des données
6.4	Service d'intégrité des données
6.5	Service de non-répudiation
6.6	Service de trace d'audit
6.7	Service d'alarme de sécurité

6.1 Authentification

Un RGT doit fournir des capacités permettant d'établir et de vérifier l'identité déclarée par tout acteur du RGT.

Les acteurs sont des utilisateurs humains ou des entités au sein du RGT. Les identités vérifiées fournissent la base de la responsabilité et jouent un rôle essentiel dans la prise en charge de la plupart des prescriptions de sécurité analysées dans le présent paragraphe.

Le service de sécurité qui prend en charge la vérification des identités est l'**authentification**. Ce service fournit la preuve qu'un objet ou un sujet possède effectivement l'identité qu'il déclare. Les

types d'authentification suivants peuvent être nécessaires en fonction du type d'acteur et du but de l'identification:

– authentification de l'utilisateur, fournissant la preuve de l'identité d'un utilisateur humain ou d'un processus d'application;
– authentification de l'entité homologue, fournissant la preuve de l'identité d'une entité homologue durant une relation de communication;
– authentification de l'origine des données, fournissant la preuve de l'identité du responsable d'une unité de données spécifique.

L'utilisation d'un service d'authentification fournit une preuve à un instant donné. La garantie de la continuité de la preuve nécessite la répétition de l'authentification dans le temps ou la constitution d'un lien avec un service d'intégrité.

Des exemples de mécanismes utilisés pour implémenter le service d'authentification sont l'authentification simple par mot de passe et numéro d'identification personnel (PIN, *personal identification number*) et l'authentification forte basée sur des méthodes de chiffrement.

Dans la sécurisation du **plan de gestion** l'**authentification** sert deux objectifs:

1) elle garantit l'identité des parties qui communiquent, fournissant une base pour établir des communications privées avec intégrité et confidentialité pleines des données entre deux systèmes;
2) elle constitue un mécanisme de base pour enregistrer des événements dans un système de gestion et/ou vérifier les activités de gestion sur n'importe quel système.

Les couches ci-dessous peuvent assurer ce service (suivant les dispositions de la Rec. UIT-T X.800):

– couche Réseau (corroboration de l'identité des entités homologues de la couche Transport);
– couche Transport (corroboration de l'identité des entités homologues de la couche Session);
– couche Application (corroboration de l'identité des processus d'application);
– extérieur OSI: dans le processus d'application lui-même.

Compte tenu du fait que le RGT sera dans l'obligation d'identifier et d'authentifier les gestionnaires et les agents ainsi que la liaison d'authentification avec contrôle d'accès, les positions recommandées par rapport à la pile OSI sont la couche Application et le processus d'application.

6.1.1 Authentification de l'utilisateur

Par **authentification de l'utilisateur** on entend l'**authentification** des clients intervenant dans la gestion du réseau. Plus précisément, l'**authentification** prouve l'identité de l'utilisateur légitime et permet de déjouer les attaques d'usurpateurs d'identité, utilisateurs illégitimes. Grâce à une **authentification** dans les règles il est possible de suivre les activités et de limiter les utilisateurs à des activités ou rôles ayant fait l'objet d'une autorisation préalable.

SER 1: chaque NE/MS fournissant un accès aux utilisateurs doit prendre en charge un service d'authentification forte pour prouver les identités.

Il convient d'observer que la présente Recommandation ne prescrit pas l'utilisation d'un seul et unique service par signature, ce qui pourrait être le cas dans une Recommandation future. Toutefois, dans le cas d'établissement d'un service de ce type, le protocole n'en doit pas moins demander l'identité de l'entité ou des entités. Un utilisateur peut ne pas avoir à indiquer ses coordonnées si celles-ci sont conservées en sécurité dans un système (par exemple, mécanisme Kerberos).

6.1.2 Authentification d'entité homologue

Par **authentification** d'entité homologue on entend l'authentification de l'entité homologue pendant une communication entre des entités, telles qu'applications, systèmes ou dispositifs.

L'**authentification** fournit l'identité de l'entité homologue et permet de déjouer des attaques par des usurpateurs d'identité, dispositifs illégitimes.

L'**authentification** d'identité homologue fournit l'**authentification** pendant la transmission de données entre systèmes (par exemple, de système à système, d'application à application) et constitue la base pour établir des communications privées avec pleine intégrité des données. Pendant la transmission des données, l'**authentification** de l'entité expéditrice permet au destinataire de vérifier l'origine du message qu'il reçoit. A l'intérieur d'une voie de transmission sécurisée, l'**authentification** cryptographique doit être associée à chaque message pour qu'à ce dernier soit attachée l'identité de l'entité expéditrice. Le destinataire vérifiera l'information cryptographique fournie avec le message pour vérifier la véritable identité de l'entité expéditrice.

SER 2: chaque NE/MS assurant une transmission de données entre des systèmes doit permettre l'**authentification** d'entité homologue pour les transmissions, et doit utiliser pour l'**authentification** ou pour l'**authentification protégée** des systèmes sur base de certificat X.509.

6.1.3 Authentification de l'origine des données

Par **authentification** de l'origine des données on entend l'établissement de la preuve de l'identité d'une entité système qui prétend être la source originelle des données reçues. L'**authentification** permet de prouver que la source de données déclarée est bien la source originelle. Ce service est normalement groupé avec un service d'intégrité des données, et est indépendant de toute association entre l'expéditeur et le destinataire; de plus, les données en question peuvent avoir été transmises à n'importe quel moment dans le passé.

SER 3: chaque NE/MS fournissant l'identité d'une entité système avec la vérification de la source des données doit prendre en charge le service d'**authentification** de l'origine des données.

6.2 Contrôle de l'accès

Un RGT doit fournir des capacités garantissant que les acteurs ne peuvent pas obtenir un accès à des informations ou des ressources pour lesquelles ils ne possèdent pas d'autorisation d'accès.

Le service de sécurité qui prend en charge cette prescription est le **contrôle d'accès**. Ce service fournit le moyen de garantir que l'accès à des ressources par les acteurs se fait uniquement de manière autorisée. Il est possible qu'une nouvelle authentification soit nécessaire après un laps de temps trop long, ou un changement de mot de passe. Les ressources en question peuvent être le système physique, le logiciel système, les applications et les données. Le service de contrôle d'accès peut être défini et implémenté dans le RGT au niveau agent, au niveau objet ou au niveau attribut.

Les limitations d'accès sont indiquées dans les informations de contrôle d'accès qui spécifient:

– les moyens permettant de déterminer quelles sont les entités qui disposent d'une autorisation d'accès;
– le type d'accès autorisé (lecture, écriture, modification, création, suppression);
– les moyens à utiliser pour associer la dimension temporelle avec les entités authentifiées et les éléments qu'elles utilisent pour leur authentification.

Des contrôles d'accès plus spécifiques du RGT peuvent être subdivisés en trois types:

– *contrôle d'accès à une association de gestion*

  Ce service permet le contrôle d'accès au niveau d'une association de gestion, ce qui signifie que les droits d'accès sont relatifs à l'association en elle-même, c'est-à-dire à l'autorisation d'établissement de l'association;

– *contrôle d'accès à une notification de gestion*

Ce service permet un contrôle d'accès portant sur les notifications, en assurant que les notifications ne sont visibles que pour des entités autorisées à les recevoir;

– *contrôle d'accès à une ressource gérée*

Ce service permet un contrôle d'accès concernant les ressources proprement dites.

L'identité de l'entité qui tente d'obtenir l'accès doit être vérifiée avant que l'accès à la ressource soit accordé. Ceci signifie que le contrôle d'accès est toujours lié à l'utilisation d'un service d'authentification.

SER 4: chaque NE/MS doit prendre en charge des services de contrôle d'accès en ce qui concerne les associations, les notifications et les ressources de gestion.

6.3 Confidentialité des données

Un RGT doit fournir des capacités permettant d'assurer la confidentialité des données stockées et transmises.

Les services de sécurité prenant en charge cette prescription sont le **contrôle d'accès** aux données stockées et la **confidentialité des données** transmises.

Le service de confidentialité fournit une protection contre la divulgation non autorisée de données échangées. On peut distinguer les types de service de confidentialité suivants:

– *confidentialité sélective de champ*

Ce service peut être utilisé dans la couche Application ou dans le processus d'application lui-même, étant donné que c'est ce dernier qui peut distinguer les champs;

– *confidentialité avec ou sans connexion*

Etant donné qu'une confidentialité de bout en bout doit être assurée, ce qui exclut la couche Physique et la couche Liaison de données, il est possible de l'assurer au niveau de la couche Réseau, de la couche Transport, de la couche Présentation, de la couche Application ou dans le processus d'application.

SER 5: chaque NE/MS doit prendre en charge un service de confidentialité des données pour assurer une protection contre la divulgation non autorisée d'échanges de données avec ou sans connexion, et pour assurer la confidentialité dans des champs choisis.

6.4 Intégrité des données

Un RGT doit être en mesure de garantir l'intégrité des données stockées et des données transmises.

Les services de sécurité à utiliser pour satisfaire à cette prescription sont le **contrôle d'accès** aux données stockées et l'**intégrité des données** transmises.

Le service d'intégrité fournit des moyens permettant d'assurer que les données échangées sont correctes en fournissant une protection contre la modification, la suppression, la création (insertion) et la répétition des données échangées. On peut distinguer les types de service d'intégrité suivants:

– intégrité sélective de champ;

– intégrité de connexion sans reprise;

– intégrité de connexion avec reprise.

Le service d'intégrité des données exige l'utilisation d'une valeur secrète connue uniquement des parties qui communiquent. Plusieurs protocoles utilisent la valeur secrète pour créer un recueil HMAC-MD5, lequel est ajouté à chaque message.

SER 6: chaque NE/MS doit prendre en charge un service d'intégrité des données pour assurer une protection contre toute modification, suppression, insertion ou retransmission de données échangées.

6.5 Non-répudiation

Un RGT doit fournir la capacité d'éviter qu'une entité puisse nier la responsabilité de toute action qu'elle a effectuée ainsi que de toute conséquence de cette action.

Cette prescription est prise en charge par le service de **non-répudiation** qui établit un lien entre l'individu (ou l'entité) et l'opération effectuée. Les services de non-répudiation fournissent un moyen permettant d'établir la preuve qu'un échange de données a effectivement eu lieu. Ils peuvent se présenter sous l'une des formes suivantes:

– non-répudiation: preuve de l'origine;

– non-répudiation: preuve de la livraison.

Pour obtenir un autre type plus général de non-répudiation il est possible de combiner de manière appropriée les services d'authentification, de contrôle d'accès et de trace d'audit.

SER 7: chaque NE/MS doit prendre en charge un service de non-répudiation pour qu'aucune entité ne puisse rejeter la responsabilité de ses actions et de leurs conséquences.

6.6 Trace d'audit

Un RGT doit fournir la capacité de stockage d'informations concernant des activités au sein du système, avec la possibilité de retrouver la trace entre ces informations et les entités ou individus impliqués. Un RGT doit également fournir la capacité d'analyser des données du journal de sécurité à des fins de contrôle portant sur les violations de la politique de sécurité.

Un journal constitue un recueil pour des enregistrements: il s'agit de l'abstraction OSI qui représente le journal d'utilisation des ressources pour des systèmes ouverts réels. Les enregistrements contiennent les informations journalisées.

Beaucoup de fonctions de gestion doivent être en mesure de conserver des informations au sujet d'événements qui se sont manifestés ou d'opérations qui ont été exécutées ou qui ont fait l'objet d'une tentative d'exécution pour des ressources diverses.

Il doit en outre être possible d'extraire ces informations du journal. Un gestionnaire doit pouvoir être en mesure de déterminer si un enregistrement quelconque a été perdu ou si les caractéristiques des enregistrements stockés ont été modifiées à un moment quelconque.

Un audit doit être considéré comme une action indépendante de révision et d'examen d'enregistrements et d'activités du système qui a pour but de vérifier si les contrôles du système sont adéquats, d'assurer la conformité avec la politique de sécurité et les procédures de fonctionnement en vigueur et de détecter les infractions à la sécurité. Le résultat de l'audit peut identifier des modifications à apporter aux contrôles, aux politiques et aux procédures.

Il est important que chaque NE/MS soit pourvu de fonctions suffisantes pour permettre des opérations d'investigation, d'audit, de détection en temps réel et d'analyse, pour que des mesures correctives adaptées puissent être apportées. Le présent paragraphe concerne la journalisation des audits de sécurité, mais le détail de leur contenu et de leur format ne relève pas de la présente Recommandation.

On notera que les opérations d'investigation et d'analyse détaillée peuvent inclure l'investigation de messages OAM&P n'ayant pas trait à la sécurité ainsi que des informations stockées dans les journaux d'audit de sécurité visés dans le présent paragraphe. L'enregistrement de messages

OAM&P n'ayant pas trait à la sécurité, parfois désignés comme messages de "modification récente", est une obligation pour toutes les actions qui peuvent faire l'objet d'un audit.

SER 8: chaque NE/MS doit pouvoir enregistrer toute action modifiant les attributs et services de sécurité, les contrôles d'accès, les paramètres de configuration des dispositifs, ainsi que chaque tentative d'enregistrement et son résultat ayant entraîné le lancement de l'horloge d'inactivité du système, et de toute action qui exige un audit. Chaque NE/MS doit permettre de procéder à l'audit des journaux en question.

Il est recommandé d'envoyer les entrées d'enregistrement d'audit à un serveur d'audit inaltérable après que le NE/MS en aura étiqueté la séquence et les aura authentifiées (signées) cryptographiquement.

6.7 Signalisation d'alarme

Un RGT doit fournir la capacité de générer des notifications d'alarme concernant des événements sélectionnés. L'utilisateur doit pouvoir définir les critères de sélection.

La fonction d'audit de sécurité est une fonction de gestion-systèmes qui décrit les notifications concernant un ensemble d'événements de sécurité. La notification d'alarme de sécurité définie par cette fonction de gestion-systèmes fournit des informations concernant l'état de fonctionnement du point de vue de la sécurité.

SER 9: chaque NE/MS doit prendre en charge un service de notification d'alarme pour alerter les administrateurs de sécurité à propos de situations opérationnelles posant un problème de sécurité.

6.8 Inspection des paquets

Un RGT doit permettre d'inspecter les paquets de tout trafic par paquets destiné au plan de gestion de n'importe lequel de ses dispositifs. L'utilisateur doit être en mesure de déterminer le filtrage en fonction des adresses des réseaux d'origine et de destination, du protocole ainsi que des ports d'origine et de destination d'un paquet.

L'inspection des paquets est le processus par lequel sont examinées les valeurs d'en-tête de chaque paquet passant au travers d'un élément de réseau en fonction de critères de correspondance spécifiés. Une action peut être entreprise au vu des résultats de l'inspection des paquets.

SER 10: chaque NE/MS doit prendre en charge un service d'inspection des paquets pour protéger le plan de gestion du RGT de tout trafic ne satisfaisant pas aux prescriptions de sécurité.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	**Gestion des télécommunications y compris le RGT et maintenance des réseaux**
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2005