UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T X.816

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(11/95)

RÉSEAUX DE COMMUNICATION DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

SÉCURITÉ

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS – CADRES DE SÉCURITÉ POUR LES SYSTÈMES OUVERTS: CADRE D'AUDIT ET D'ALARMES DE SÉCURITÉ

Recommandation UIT-T X.816

(Antérieurement «Recommandation du CCITT»)

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. Au sein de l'UIT-T, qui est l'entité qui établit les normes mondiales (Recommandations) sur les télécommunications, participent quelque 179 pays membres, 84 exploitations de télécommunications reconnues, 145 organisations scientifiques et industrielles et 38 organisations internationales.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution nº 1 de la Conférence mondiale de normalisation des télécommunications (CMNT), (Helsinki, 1993). De plus, la CMNT, qui se réunit tous les quatre ans, approuve les Recommandations qui lui sont soumises et établit le programme d'études pour la période suivante.

Dans certains secteurs de la technologie 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. Le texte de la Recommandation X.816 de l'UIT-T a été approuvé le 21 novembre 1995. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 10181-7.

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.

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE COMMUNICATION DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

(Février 1994)

ORGANISATION DES RECOMMANDATIONS DE LA SÉRIE X

Domaine	Recommandations
RÉSEAUX PUBLICS POUR DONNÉES	
Services et services complémentaires	X.1-X.19
Interfaces	X.20-X.49
Transmission, signalisation et commutation	X.50-X.89
Aspects réseau	X.90-X.149
Maintenance	X.150-X.179
Dispositions administratives	X.180-X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	
Modèle et notation	X.200-X.209
Définition des services	X.210-X.219
Spécifications des protocoles en mode connexion	X.220-X.229
Spécifications des protocoles en mode sans connexion	X.230-X.239
Formulaires PICS	X.240-X.259
Identification des protocoles	X.260-X.269
Protocoles de sécurité	X.270-X.279
Objets gérés de couche	X.280-X.289
Test de conformité	X.290-X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Considérations générales	X.300-X.349
Systèmes mobiles de transmission de données	X.350-X.369
Gestion	X.370-X.399
SYSTÈMES DE MESSAGERIE	X.400-X.499
ANNUAIRE	X.500-X.599
RÉSEAUTAGE OSI ET ASPECTS DES SYSTÈMES	
Réseautage	X.600-X.649
Dénomination, adressage et enregistrement	X.650-X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680-X.699
GESTION OSI	X.700-X.799
SÉCURITÉ	X.800-X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850-X.859
Traitement des transactions	X.860-X.879
Opérations distantes	X.880-X.899
TRAITEMENT OUVERT RÉPARTI	X.900-X.999

TABLE DES MATIÈRES

Résumé

La présente Recommandation | Norme internationale décrit un modèle de base permettant de manipuler les alarmes de sécurité et de conduire un audit de sécurité pour les systèmes ouverts. Un audit de sécurité est une analyse et un examen – effectués de façon indépendante – des enregistrements et activités du système. Le service d'audit de sécurité fournit à une autorité d'audit la capacité de spécifier, sélectionner et gérer les événements qui doivent être enregistrés dans un journal d'audit de sécurité.

Introduction

La présente Recommandation | Norme internationale précise le concept d'audit de sécurité défini dans la Rec. UIT-T X.810 | ISO/CEI 10181-1. Cela comprend la détection d'événements ainsi que les actions résultantes de ces événements. Le cadre couvre donc à la fois l'audit de sécurité et les alarmes de sécurité.

Un audit de sécurité est une analyse et un examen – effectués de façon indépendante – des enregistrements et activités du système. Les objectifs d'un audit de sécurité sont les suivants:

- aider à l'identification et l'analyse d'actions non autorisées ou d'attaques;
- aider à garantir que les actions peuvent être attribuées aux entités responsables de ces actions;
- contribuer au développement de procédures améliorées de contrôle des dommages;
- confirmer la conformité avec la politique de sécurité établie;
- signaler l'information qui peut indiquer des inadéquations dans le contrôle du système;
- identifier les changements possibles requis dans les contrôles, la politique et les procédures.

Dans ce cadre, un audit de sécurité consiste en la détection, la collecte et l'enregistrement des événements liés à la sécurité des systèmes ouverts dans un journal d'audit de sécurité et en l'analyse de ces événements.

L'audit mais aussi l'imputabilité nécessitent le stockage de l'information. Un audit de sécurité garantit que l'information enregistrée concerne à la fois les événements routiniers et les événements exceptionnels, de sorte que des investigations ultérieures puissent déterminer si des violations de sécurité sont survenues et, si tel est le cas, quelles sont les informations ou les autres ressources qui ont été compromises. L'imputabilité garantit que l'information relative aux actions réalisées par les utilisateurs, ou par des processus agissant pour leur compte, est enregistrée, de telle sorte que les conséquences de ces actions puissent être ultérieurement liées aux utilisateurs en question et que les utilisateurs puissent être tenus responsables de ces actions. La fourniture d'un service d'audit de sécurité peut contribuer à assurer l'imputabilité.

Une alarme de sécurité est une indication émise vers un individu ou un processus pour indiquer qu'une situation pouvant nécessiter une action à temps est apparue. Les objectifs d'un service d'alarme de sécurité sont les suivants:

- signaler des tentatives réelles ou apparentes de violer la sécurité;
- signaler divers événements liés à la sécurité, y compris les événements «normaux»;
- signaler les événements déclenchés par l'atteinte des limites de seuil.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS – CADRES DE SÉCURITÉ POUR LES SYSTÈMES OUVERTS: CADRE D'AUDIT ET D'ALARMES DE SÉCURITÉ

1 Domaine d'application

La présente Recommandation | Norme internationale couvre l'application des services de sécurité dans un environnement de systèmes ouverts, où le terme «systèmes ouverts» est utilisé pour des domaines tels que les bases de données, les applications distribuées, le traitement ODP et l'interconnexion OSI. Les cadres de sécurité sont destinés à définir les moyens d'offrir la protection pour les systèmes et les objets au sein des systèmes, ainsi que les interactions entre systèmes. Les cadres ne couvrent pas la méthodologie de construction des systèmes ou mécanismes.

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

Le but de l'audit et des alarmes de sécurité décrits dans la présente Recommandation | Norme internationale est d'assurer que les événements liés à la sécurité des systèmes ouverts sont manipulés en accord avec la politique de sécurité de l'autorité de sécurité en vigueur.

En particulier, ce cadre de sécurité:

a) définit les concepts élémentaires d'audit et d'alarmes de sécurité;

b) fournit un modèle général pour l'audit et les alarmes de sécurité;

c) identifie les relations du service d'audit et d'alarmes de sécurité avec d'autres services de sécurité.

Comme les autre services de sécurité, un audit de sécurité ne peut être fourni que dans le contexte d'une politique de sécurité définie.

Le modèle d'audit et d'alarmes de sécurité indiqué dans l'article 6 de ce cadre répond à une variété d'objectifs qui peuvent ne pas être tous nécessaires ou souhaités dans un environnement particulier. Le service d'audit de sécurité offre à une autorité d'audit la possibilité de spécifier les événements qui doivent être enregistrés dans un journal d'audit de sécurité.

Plusieurs types de normes différents peuvent utiliser ce cadre, y compris:

1) les normes qui incorporent le concept d'audit et d'alarmes;

2) les normes qui spécifient des services abstraits comprenant l'audit et les alarmes;

3) les normes qui spécifient les utilisations d'audit et d'alarmes;

4) les normes qui spécifient les moyens de fournir l'audit et les alarmes au sein d'une architecture de système ouvert;

5) les normes qui spécifient les mécanismes d'audit et d'alarmes.

De telles normes peuvent utiliser ce cadre de la façon suivante:

– les normes de types 1), 2), 3), 4) et 5) peuvent utiliser la terminologie de ce cadre;

– les normes de types 2), 3), 4) et 5) peuvent utiliser les fonctionnalités définies dans l'article 8 de ce cadre;

– les normes de type 5) peuvent être basées sur les caractéristiques des mécanismes définis dans l'article 9 de ce cadre.

2 Références normatives

Les Recommandations et 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. Toute Recommandation et Norme 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) | Norme 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 X.734 du CCITT (1992) | ISO/CEI 10164-5:1993, *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: fonction de gestion des rapports d'événement.*
- Recommandation X.735 du CCITT (1992) | ISO/CEI 10164-6:1993, *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: fonction de commande des registres de consignation.*
- Recommandation X.736 du CCITT (1992) | ISO/CEI 10164-7:1992, *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: fonction de signalisation des alarmes de sécurité.*
- Recommandation X.740 du CCITT (1992) | ISO/CEI 10164-8:1993, *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: fonction de piste de vérification de sécurité.*
- 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.*

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

- Recommandation X.700 du CCITT (1992), *Cadre de gestion pour l'interconnexion de systèmes ouverts pour les applications du CCITT.*

  ISO/CEI 7498-4:1989, *Systèmes de traitement de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base – Partie 4: Cadre général de gestion.*
- 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 des 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 suivants définis dans la Rec. UIT-T X.200 | ISO/CEI 7498-1:

a) entité;

b) fonctionnalité;

c) fonction;

d) service.

3.2 Définitions de l'architecture de sécurité

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

a) imputabilité;

b) disponibilité;

c) audit de sécurité;

d) journal d'audit de sécurité;

e) politique de sécurité.

3.3 Définitions du cadre de gestion

La présente Recommandation | Norme internationale utilise le terme suivant défini dans la Rec. X.700 du CCITT | ISO/CEI 7498-4:

– objet géré.

3.4 Définitions de l'aperçu général du cadre de sécurité

La présente Recommandation | Norme internationale utilise le terme suivant défini dans la Rec. UIT-T X.810 | ISO/CEI 10181-1:

– domaine de sécurité.

3.5 Définitions additionnelles

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

3.5.1 processeur d'alarme: fonction qui, en réponse à une alarme de sécurité, génère une action appropriée et génère un message d'audit de sécurité.

3.5.2 autorité d'audit: gestionnaire responsable de la définition des aspects d'une politique de sécurité applicables à la conduite d'un audit de sécurité.

3.5.3 analyseur d'audit: fonction qui vérifie un journal d'audit de sécurité afin de produire, si cela est approprié, des messages d'alarme de sécurité et des messages d'audit de sécurité.

3.5.4 archiviste d'audit: fonction qui archive une partie du journal d'audit de sécurité.

3.5.5 expéditeur d'audit: fonction qui transfère, à la fonction de collecte de journal de sécurité, des parties ou la totalité d'un journal distribué d'audit de sécurité.

3.5.6 examinateur de journal d'audit: fonction qui, à partir d'un ou plusieurs journaux d'audit de sécurité, construit des rapports.

3.5.7 enregistreur d'audit: fonction qui génère des enregistrements d'audit de sécurité et les stocke dans un journal d'audit de sécurité.

3.5.8 fournisseur d'audit: fonction qui fournit des enregistrements de journal d'audit de sécurité en fonction de certains critères.

3.5.9 collecteur de journal d'audit: fonction qui rassemble les enregistrements d'un journal distribué d'audit dans un journal d'audit de sécurité.

3.5.10 filtre d'événement: fonction qui fournit une analyse initiale des événements liés à la sécurité et génère un message d'audit de sécurité et/ou un message d'alarme.

3.5.11 alarme de sécurité: message généré lorsqu'un événement lié à la sécurité, défini par la politique de sécurité comme étant une condition d'alarme, a été détecté. Une alarme de sécurité est destinée à être portée à temps à l'attention d'entités appropriées.

3.5.12 administrateur d'alarme de sécurité: individu ou processus qui détermine la nature des alarmes de sécurité.

3.5.13 événement lié à la sécurité: tout événement qui a été défini par la politique de sécurité comme une brèche potentielle dans la politique de sécurité, ou comme ayant un intérêt potentiel pour la sécurité. L'arrivée à une valeur prédéfinie de seuil est un exemple d'événement lié à la sécurité.

3.5.14 message d'audit de sécurité: message généré à la suite d'un événement vérifiable lié à la sécurité.

3.5.15 enregistrement d'audit de sécurité: enregistrement unique dans un journal d'audit de sécurité.

3.5.16 agent d'audit de sécurité: individu ou processus autorisé à avoir accès au journal de sécurité et à bâtir des rapports d'audit.

3.5.17 rapport de sécurité: rapport qui résulte d'une analyse du journal d'audit de sécurité et qui peut être utilisé pour déterminer si une brèche est apparue dans la sécurité.

4 Abréviations

OSI Interconnexion des systèmes ouverts (*open systems interconnection*).

5 Notation

Sauf indication contraire, les termes «service» et «mécanisme» sont utilisés pour désigner, respectivement, le «service d'audit de sécurité» et le «mécanisme d'audit de sécurité»; celui d'«audit» désigne un «audit de sécurité» et enfin, celui d'«alarme» désigne une «alarme de sécurité».

6 Présentation générale de l'audit et des alarmes de sécurité

Cet article décrit un modèle permettant de manipuler les alarmes de sécurité et de conduire un audit de sécurité pour les systèmes ouverts.

Un audit de sécurité permet d'évaluer l'adéquation de la politique de sécurité, d'aider à la détection des violations de sécurité, de faciliter l'imputation de leurs actions aux individus (ou des actions des entités agissant pour leur compte), d'aider à la détection de mauvaise utilisation des ressources, et agit comme élément préventif pour les individus qui pourraient tenter d'endommager le système. Les mécanismes d'audit de sécurité ne sont pas directement mis en jeu dans la prévention des violations de sécurité: ils sont impliqués pour la détection, l'enregistrement et l'analyse des événements. Cela permet de mettre en œuvre des changements dans les procédures opérationnelles en réponse à des événements anormaux comme des violations de sécurité.

Une alarme de sécurité est générée suite à la détection de tout événement lié à la sécurité qui a été défini par la politique de sécurité comme étant une condition d'alarme. Cela pourrait inclure le cas de l'obtention d'un seuil prédéfini. Certains de ces événements peuvent nécessiter une action immédiate alors que d'autres peuvent nécessiter une investigation plus poussée pour déterminer si une action est requise.

Une mise en œuvre du modèle d'audit et d'alarmes de sécurité peut nécessiter l'utilisation d'autres services de sécurité pour réaliser le service d'audit et d'alarmes de sécurité et pour assurer son fonctionnement correct et sûr. Ce sujet est abordé plus loin dans l'article 10.

Bien que l'utilisation des journaux d'audit de sécurité et d'audits de sécurité ait des caractéristiques spéciales, d'autres journaux d'audit et d'autres audits (autres que de sécurité) peuvent recourir aux fonctions et mécanismes décrits dans le présent cadre.

Comme avec les autres aspects de la sécurité, on obtient une efficacité maximale en s'assurant que les besoins spécifiques d'audit de sécurité sont conçus dans le système. Les concepteurs de système devraient donc tenir compte du besoin de vérifier (par exemple, examen et analyse tout prêts) à la fois le processus de conception et le système en cours de développement.

NOTE – Le modèle d'audit et d'alarmes de sécurité n'indique pas comment les autres systèmes de gestion et les caractéristiques opérationnelles sont liés à ce modèle.

6.1 Modèle et fonctions

Le modèle présenté ci-dessous illustre les fonctions utilisées dans la fourniture du service d'audit et d'alarmes de sécurité.

6.1.1 Fonctions du service d'audit et d'alarmes de sécurité

Diverses fonctions sont nécessaires pour mettre en œuvre un service complet d'audit et d'alarmes de sécurité, à savoir:

- le **filtre d'événement** qui fournit une analyse initiale de l'événement et détermine s'il envoie l'événement à l'enregistreur d'audit ou au processeur d'alarme;
- l'**enregistreur d'audit** qui génère les enregistrements d'audit à partir des messages reçus et stocke les enregistrements dans un journal d'audit de sécurité;
- le **processeur d'alarme** qui génère à la fois un message d'audit et une action appropriée en réponse à une alarme de sécurité;
- l'**analyseur d'audit** qui vérifie un journal d'audit de sécurité et, si cela est approprié, produit des messages d'alarme et des messages d'audit de sécurité;
- l'**examinateur de journal d'audit** qui bâtit des rapports de sécurité à partir d'un ou de plusieurs journaux d'audit de sécurité;
- le **fournisseur d'audit** qui fournit des enregistrements d'audit de sécurité en fonction de certains critères;
- l'**archiviste d'audit** qui archive une partie du journal d'audit de sécurité.

Des fonctions supplémentaires peuvent s'avérer nécessaires pour mettre en œuvre des journaux d'audit de sécurité distribués et des alarmes. Parmi celles-ci:

- la fonction de **collecteur de journal d'audit** qui rassemble les enregistrements d'un journal distribué d'audit dans un journal d'audit de sécurité;
- la fonction d'**expéditeur d'audit** qui transfère, à la fonction de collecte de journal de sécurité, des parties ou la totalité d'un journal distribué d'audit de sécurité.

6.1.2 Modèle d'audit et d'alarmes de sécurité

Le modèle d'audit et d'alarmes de sécurité décrit ci-dessous fait intervenir plusieurs phases. Suite à la détection d'un événement, la détermination de son intérêt ou non pour la sécurité doit être effectuée. Le *filtre d'événement* évalue l'événement pour déterminer si un message d'audit de sécurité et/ou un message d'alarme de sécurité devrait être généré. Les messages d'audit de sécurité sont envoyés à l'*enregistreur d'audit*: les alarmes de sécurité sont envoyées au *processeur d'alarme* pour évaluation et action ultérieure. Les messages d'audit de sécurité sont alors formatés puis transformés en enregistrements d'audit de sécurité pour être consignés dans le journal d'audit de sécurité. Les anciennes parties du journal d'audit de sécurité peuvent être archivées et le journal d'audit de sécurité ainsi que les archives de journal d'audit de sécurité peuvent être utilisés pour bâtir des rapports d'audit en sélectionnant, en fonction de critères spécifiés, des enregistrements particuliers d'audit de sécurité. C'est ainsi que le journal d'audit de sécurité peut être analysé et que des rapports et/ou des alarmes de sécurité peuvent être générés. Le modèle d'audit et d'alarmes de sécurité est indiqué sur la Figure 1.

6.1.3 Groupement des fonctions d'audit et d'alarmes de sécurité

Les fonctions décrites dans le modèle peuvent être colocalisées dans un composant d'un système ou distribuées sur plusieurs composants du système. Ces fonctions peuvent également être localisées dans des systèmes d'extrémité différents et peuvent être dupliquées. Dans certains cas, comme pour des raisons de performances, il sera avantageux de grouper ces fonctions. En particulier, un *enregistreur d'audit*, un *expéditeur d'audit*, un *fournisseur d'audit* et un *analyseur d'audit* travaillant ensemble sur le même journal d'audit de sécurité peuvent constituer une partie d'un seul système d'extrémité.

Un autre groupement pourrait être constitué d'un *examinateur de journal d'audit* et d'un *analyseur d'audit* qui peuvent être utiles à un auditeur de sécurité.

Il peut y avoir une chaîne de fonctions arrangées de façon hiérarchique, en particulier dans un journal d'audit de sécurité distribué (voir la Figure 2). Ici un *collecteur de journal d'audit* d'un composant collecte les messages d'audit de l'*expéditeur d'audit* d'un autre composant. La chaîne se termine lorsqu'un composant ne met pas en œuvre un *expéditeur d'audit*: dans ce cas, le composant doit mettre en œuvre un *archiviste d'audit* pour être en mesure d'archiver son journal d'audit de sécurité.

La décision des fonctions, s'il y en a, devant être groupées, est un problème de mise en œuvre. Les exemples ci-dessus ne sont donnés qu'à titre d'exemple.

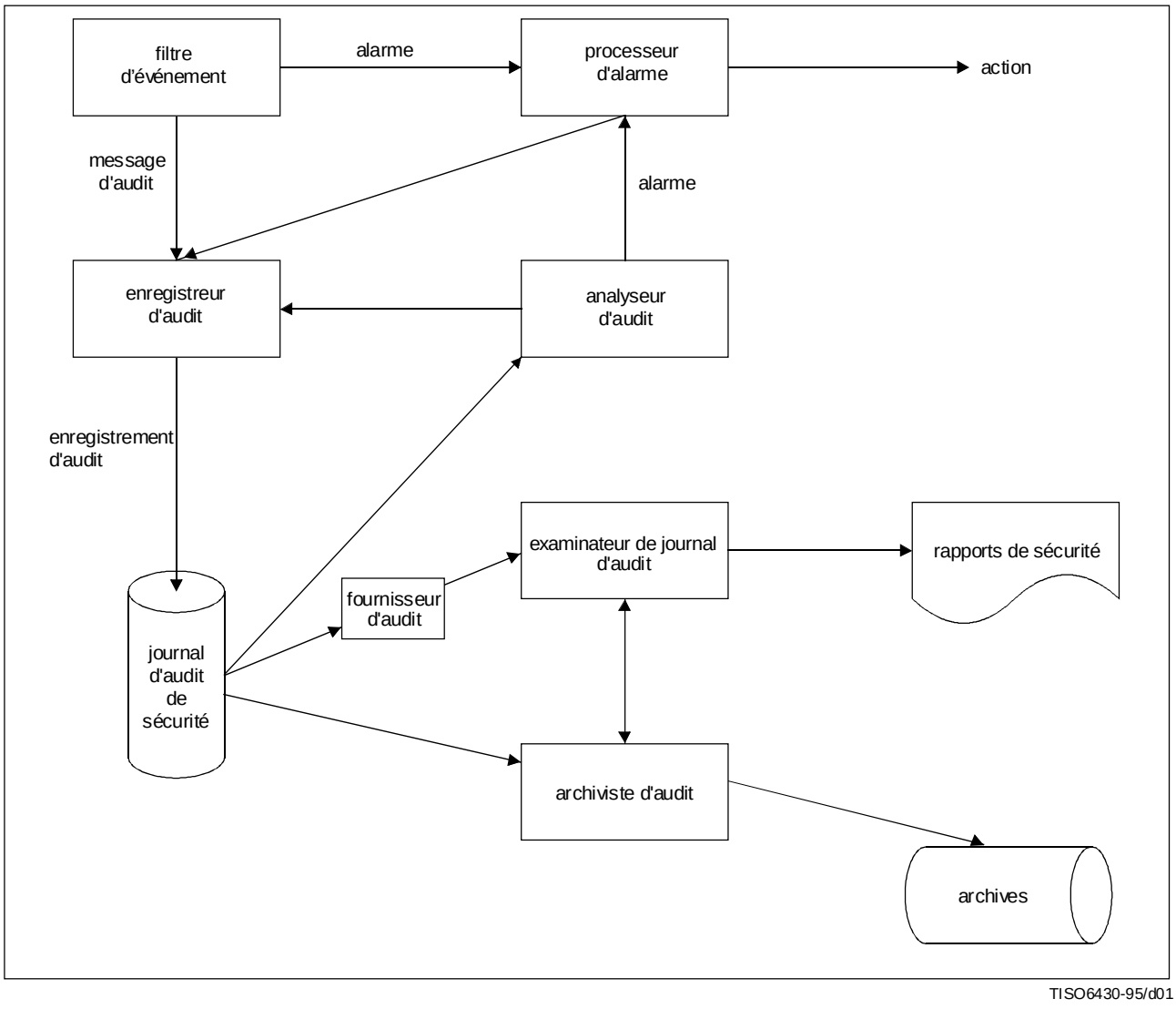

Figure 1 – Modèle d'audit et d'alarmes de sécurité

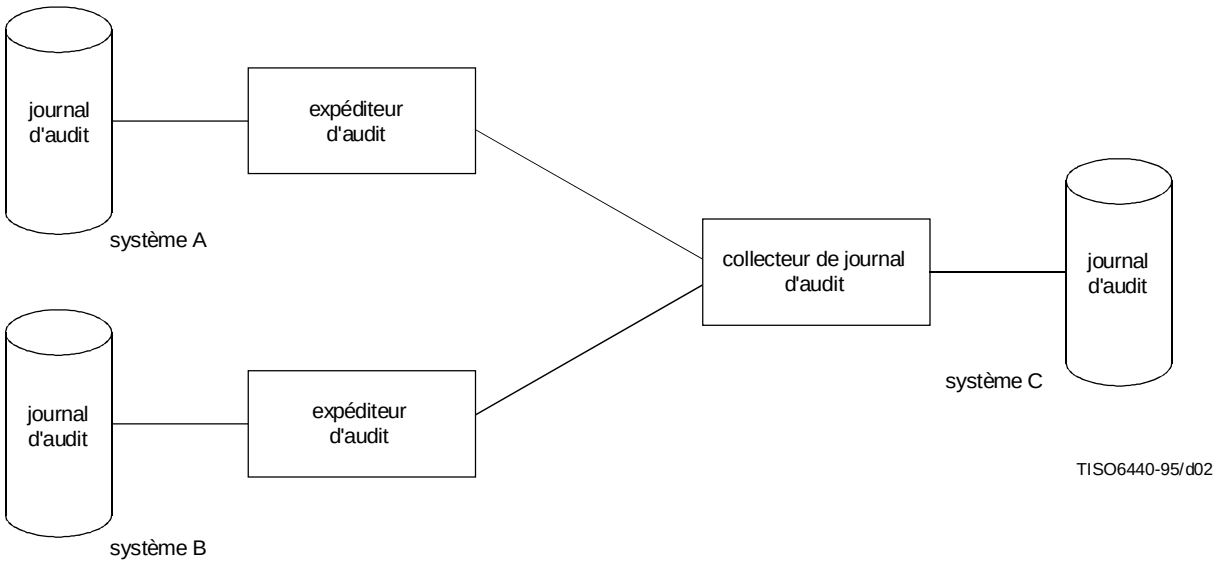

Figure 2 – Modèle de journal d'audit distribué

6.2 Phases des procédures d'audit et d'alarmes de sécurité

Le service d'audit de sécurité fournit à une autorité d'audit la possibilité de spécifier et de sélectionner les événements qui doivent être détectés et enregistrés dans un journal d'audit de sécurité, et les événements qui nécessitent le déclenchement d'une alarme de sécurité et d'un message d'audit de sécurité.

Les phases suivantes peuvent intervenir dans les procédures d'audit:

- phase de détection, dans laquelle un événement lié à la sécurité est détecté;
- phase de filtrage, dans laquelle une détermination initiale est effectuée sur la nécessité d'enregistrer l'événement dans un journal d'audit de sécurité ou d'envoyer une alarme;
- phase de traitement d'alarme, dans laquelle une alarme de sécurité ou un message d'audit de sécurité peut être émis;
- phase d'analyse, dans laquelle un événement lié à la sécurité est évalué avec l'ensemble, et dans le contexte, des éléments précédemment détectés et enregistrés dans le journal d'audit, et une ligne de conduite déterminée;
- phase d'agrégation, dans laquelle des enregistrements de journal d'audit de sécurité distribué sont collectés dans un seul système de journal d'audit de sécurité;
- phase de génération de rapport d'événement, dans laquelle des rapports d'audit de sécurité sont bâtis à partir des enregistrements de journal d'audit de sécurité;
- phase d'archivage, dans laquelle des enregistrements du journal d'audit de sécurité sont transférés dans l'archive de journal d'audit de sécurité.

Les phases décrites ici ne sont pas nécessairement concomitantes dans le temps; elles peuvent, par exemple, se recouvrir.

6.2.1 Phase de détection

La phase de détection met en jeu la détermination de l'apparition d'un événement pouvant être lié à la sécurité. La détermination concrète de l'action, s'il y en a une, devant être prise en réponse à cet événement est la tâche du *filtre d'événement* (voir 6.2.2) mais, dans certains cas, déterminée par la politique de sécurité, une action immédiate peut être initiée.

6.2.2 Phase de filtrage

Lorsqu'un événement lié à la sécurité a été détecté, le filtre d'événement déterminera la ligne de conduite initiale appropriée. L'action sera l'une des suivantes:

a) ne pas prendre d'action;

b) générer un message d'audit de sécurité;

c) générer à la fois une alarme de sécurité et un message d'audit de sécurité.

La décision relative à la ligne de conduite qui devrait être suivie pour chaque événement dépend de la politique de sécurité en vigueur.

6.2.3 Phase de traitement d’alarme

Le processeur de sécurité analyse l'alarme pour déterminer la ligne de conduite adéquate. L'action sera l'une des suivantes:

a) ne pas prendre d'action;

b) initier une action de récupération;

c) initier une action de récupération et générer un message d'audit de sécurité.

La décision de la ligne de conduite qui devrait être suivie pour chaque événement dépend de la politique de sécurité en vigueur.

NOTE – b) et c) pourraient impliquer que l'événement soit porté à l'attention d'une personne comme un responsable de sécurité ou un administrateur d'audit.

6.2.4 Phase d'analyse

Dans la phase d'analyse, un événement lié à la sécurité est traité pour déterminer la ligne de conduite appropriée. Le traitement peut également utiliser de l'information sur des événements précédents liés à la sécurité, enregistrés dans le journal d'audit de sécurité. L'action sera l'une des suivantes:

a) ne pas prendre d'action;

b) générer une alarme de sécurité;

c) générer un enregistrement d'audit de sécurité;

d) générer à la fois une alarme de sécurité et un enregistrement d'audit de sécurité.

La décision relative à la ligne de conduite qui devrait être suivie pour chaque événement dépend de la politique de sécurité en vigueur.

En tant qu'élément du processus d'analyse, une référence aux précédents événements peut être faite par l'examen des enregistrements dans le journal d'audit de sécurité et l'archive du journal d'audit de sécurité.

6.2.5 Phase d'agrégation

Les enregistrements individuels d'audit de sécurité d'un journal d'audit de sécurité distribué doivent être périodiquement collectés dans un journal d'audit de sécurité. Ce processus, qui comprend l'utilisation d'un *collecteur de journal d'audit* (au point de collecte) et l'utilisation d'un *expéditeur d'audit* (au niveau des systèmes distants), est appelé agrégation. (Comme cela est indiqué au 6.1.3, ce processus pourrait être hiérarchique.)

6.2.6 Phase de génération de rapport

Lorsque cela est requis ou mandaté en accord avec la politique de sécurité, le journal d'audit de sécurité peut être traité. Ce traitement mettra en jeu un élément d'analyse et peut également impliquer la manipulation des enregistrements de sécurité dans un format approprié. La sortie de l'analyse d'un journal d'audit de sécurité est un rapport de sécurité qui peut indiquer qu'un essai d'ouverture de brèche dans le système de sécurité a été tenté; dans ce cas, des actions de récupération peuvent être nécessaires. On peut recourir à l'analyse du journal d'audit de sécurité pour évaluer l'étendue d'une attaque et déterminer les procédures de contrôle des dommages.

Un rapport de sécurité peut être utilisé par la récupération de sécurité afin d'identifier l'étendue du dommage résultant d'un problème de sécurité. En particulier, il peut servir à identifier les ressources qui ont été employées par un utilisateur autorisé ayant utilisé ses droits de manière anormale. Il peut aussi servir à identifier tout fichier endommagé afin qu'un rétablissement de ces fichiers puisse être tenté.

6.2.7 Phase d'archivage

Les journaux d'audit de sécurité peuvent devoir être conservés pendant de longues périodes. Dans la phase d'archivage, une partie d'un journal d'audit de sécurité est transférée sur un support de conservation à long terme. Ce support d'archivage doit assurer la conservation intégrale des enregistrements originaux. L'archivage des journaux d'audit de sécurité peut être situé à proximité ou à distance de la source originale du journal d'audit. Des mécanismes peuvent être fournis pour l'archivage à distance.

6.3 Corrélation des informations d'audit

Les enregistrements d'audit peuvent être associés les uns aux autres à l'intérieur d'un ou de plusieurs journaux d'audit de sécurité. Par exemple, une demande de connexion peut être transmise par le biais de plusieurs systèmes intermédiaires et peut, par conséquent, produire plusieurs enregistrements d'audit de sécurité dans différents journaux d'audit de sécurité. Il peut être important de correctement dater ou identifier comme étant corrélés ces enregistrements d'audit de sécurité. Un autre exemple concerne le cas de l'enregistrement de deux événements différents dans deux journaux différents d'audit de sécurité lorsqu'il est important de déterminer quel événement est survenu en premier. Une présentation des problèmes intervenant dans la corrélation des dates d'événements de différents générateurs d'événements se trouve dans l'Annexe D.

7 Politique et autres aspects de l'audit et des alarmes de sécurité

7.1 Politique

Une politique d'audit définit les événements liés à la sécurité et identifie les règles à appliquer pour la collecte, l'enregistrement (dans un journal d'audit de sécurité) et l'analyse des divers événements liés à la sécurité. Plusieurs points de vue peuvent être pris en compte dans les politiques d'audit de sécurité et dans leurs expressions en tant que règles. Un ou plusieurs de ces points de vue peuvent être applicables à une politique particulière de sécurité.

Une politique de sécurité devrait exprimer des besoins pour la réalisation de divers niveaux et types d'audit de sécurité et devrait également définir les critères pour la génération des alarmes de sécurité. Le test de l'adéquation des contrôles du système, confirmant la conformité avec la politique de sécurité et déterminant des changements indiqués dans la politique, ainsi que les contrôles et les procédures nécessiteront l'analyse d'enregistrements de journal d'audit de sécurité et plusieurs autres aspects de la conception, la configuration et l'exploitation des systèmes.

NOTE – La façon de définir les événements liés à la sécurité dans une politique de sécurité ne fait pas partie du champ d'application de la présente Recommandation | Norme internationale.

7.2 Aspects légaux

Dans plusieurs pays il y a des lois conçues pour protéger la vie privée des citoyens. Dans certains cas, cela signifie qu'un enregistrement de journal d'audit contenant de l'information de nature personnelle tombera sous le coup des lois nationales liées à la vie privée et à l'accès à l'information. De tels enregistrements devront être protégés contre une divulgation non autorisée.

Lorsque les enregistrements d'audit de sécurité sont utilisés comme une preuve légalement admissible, il peut exister des besoins spécifiques concernant l'utilisation, le stockage et la protection des enregistrements de sécurité.

7.3 Besoins de protection

Deux aspects de la protection doivent être pris en compte:

- protection du journal d'audit de sécurité et de l'information d'audit;
- protection du service d'audit de sécurité.

7.3.1 Protection de l'information d'audit de sécurité

L'information collectée dans un journal d'audit de sécurité peut provenir directement des messages d'audit ou d'autres journaux d'audit de sécurité. Un journal d'audit de sécurité peut ainsi être l'agrégat d'enregistrements de journaux d'audit de sécurité générés par une ou plusieurs sources. Dans le cas le plus simple, un journal d'audit de sécurité contient tous les enregistrements d'audit de sécurité générés par un seul système.

Le journal d'audit de sécurité doit être protégé contre une divulgation non autorisée et/ou une modification non autorisée. Les mécanismes de contrôle d'accès, de confidentialité, d'intégrité et d'authentification peuvent être utilisés pour sa protection. Une technique de protection spécifique est utilisée pour stocker les enregistrements d'audit sur un support qui ne peut être inscrit qu'une seule fois afin qu'une superposition ne puisse pas être utilisée pour effacer l'enregistrement d'un événement.

Les messages d'audit de sécurité, les alarmes de sécurité et les rapports de sécurité doivent également être protégés contre une divulgation non autorisée et/ou une modification non autorisée. En outre, il est important que l'émetteur et le récepteur de l'information aient confiance dans le fait que la source et la destination des données sont celles qui sont déclarées et que l'information n'a en aucune façon été corrompue.

La confidentialité d'au moins certaines informations doit également être requise. Cela est nécessaire pour plusieurs raisons:

- aspects légaux en rapport avec la vie personnelle et privée;
- dissimuler quels événements d'audit sont ou non enregistrés;
- dissimuler les identités des récepteurs (ou des non-récepteurs) des actions résultant des alarmes.

7.3.2 Protection du service d'audit et d'alarmes

Un service d'audit et d'alarmes de sécurité dépend de l'existence d'un haut niveau de disponibilité. Le déni de service est une menace au service d'audit et d'alarmes de sécurité. L'information destinée soit à l'administrateur d'alarme soit à l'auditeur de sécurité pourrait être retardée jusqu'au moment où cette information n'est plus valide. Il est de première importance que l'information parvienne dans les délais au correspondant auquel elle est destinée.

Une présentation plus détaillée de ces aspects de protection se trouve dans l'article 10.

8 Informations et fonctionnalités de l'audit et des alarmes de sécurité

Le traitement de l'information d'audit et d'alarmes de sécurité peut être considéré selon deux aspects:

- le traitement des messages générés en réponse à un événement non attendu (par exemple, information non sollicitée d'audit et d'alarmes de sécurité);
- le traitement des demandes pour des informations spécifiques d'audit et d'alarmes de sécurité (par exemple, information sollicitée).

Les services de gestion sont nécessaires pour contrôler plusieurs aspects du processus d'audit et d'alarmes de sécurité y compris les mécanismes de journal d'audit de sécurité, les critères définissant les actions spécifiques prises lors d'une détection d'événements liés à la sécurité et le processus mis en jeu dans la manipulation des informations d'audit et d'alarmes.

8.1 Informations d'audit et d'alarmes

Les informations d'audit et d'alarmes comprennent les alarmes de sécurité, les messages d'audit de sécurité, les enregistrements d'audit de sécurité et les rapports de sécurité.

8.1.1 Messages d'audit de sécurité

Un *message d'audit de sécurité* est un message généré comme résultat d'un événement vérifiable lié à la sécurité.

Un message d'audit de sécurité peut, par exemple, être généré à partir d'une analyse initiale d'un événement lié à la sécurité effectuée par le *filtre d'événement* ou comme résultat d'une évaluation consécutive du *processeur d'alarme* ou de l'*analyseur d'audit*.

8.1.2 Enregistrements d'audit de sécurité

Le terme *enregistrement d'audit de sécurité* est utilisé pour décrire un enregistrement unique dans un journal d'audit de sécurité. Dans de nombreux cas cela correspondra à un événement unique lié à la sécurité mais il est également concevable que, dans certaines mises en œuvre, un enregistrement d'audit de sécurité puisse être généré comme le résultat de plusieurs événements liés à la sécurité.

Un enregistrement typique de journal d'audit de sécurité comprend l'information sur l'origine et la cause du message, et peut contenir des informations sur les entités mises en jeu dans la détection et le traitement du message.

8.1.3 Alarmes de sécurité

Une *alarme de sécurité* est un message généré suite à la détection d'un événement lié à la sécurité qui est défini comme étant une brèche potentielle dans la sécurité et comme constituant une condition d'alarme. Cela pourrait être un événement unique ou le résultat de l'arrivée à un seuil. Dans l'un ou l'autre cas, la définition de ce qui constitue la condition d'alarme est spécifiée dans la politique de sécurité.

Les alarmes de sécurité peuvent être initiées par le *filtre d'événement* (comme résultat d'une évaluation initiale d'un événement de sécurité) ou par l'*analyseur d'audit* si, à n'importe quel moment, il détermine l'existence d'une condition d'alarme.

8.1.4 Rapports de sécurité

Les *rapports de sécurité* sont des informations produites en tant que résultat d'analyses des journaux d'audit de sécurité. L'*examinateur du journal d'audit* est utilisé pour bâtir les rapports à partir d'un ou de plusieurs journaux d'audit de sécurité.

8.1.5 Exemple d'élaboration des informations d'audit et d'alarmes

Les informations d'audit et d'alarmes contiennent en général les éléments suivants:

- les informations/types de message (par exemple, alarme de sécurité, message d'audit de sécurité ou rapport de sécurité);
- l'identificateur caractéristique des éléments (par exemple, initiateur/cible pour l'événement lié à la sécurité; sujet/objet de l'action);
- la cause du message;
- l'identificateur caractéristique du *filtre d'événement*, du *fournisseur d'audit* et/ou de l'*enregistreur d'audit*.

8.2 Fonctionnalités d'audit et d'alarmes de sécurité

Afin d'appliquer un audit efficacement et permettre une analyse efficace d'événements, il est nécessaire de disposer d'une méthode pour déterminer les événements qui sont liés à la sécurité et la façon dont ils doivent être traités. L'analyse des messages est effectuée par un mécanisme de filtrage qui détermine l'action adéquate à prendre lors de la réception d'un message d'audit. Le filtre agit en fonction de critères (identifiés par l'autorité d'audit de sécurité) qui établissent l'action à prendre pour chaque type de message. Les critères à partir desquels une action peut être déclenchée comprennent:

- l'heure du jour;
- un compteur de seuil;
- le type d'événement;
- l'entité provoquant l'événement.

A des fins de gestion, le filtre peut être défini comme un objet géré avec un comportement et des paramètres spécifiés.

La fonctionnalité liée à la gestion offre un moyen d'établir les critères de sélection permettant à un utilisateur de traiter l'information nécessaire pour la fourniture du service d'audit et d'alarmes de sécurité. En termes généraux, ces fonctionnalités sont:

a) créer, modifier et détruire les critères pour traiter les événements concernant la sécurité;

b) permettre et interdire la génération de messages spécifiés d'audit de sécurité;

c) permettre et interdire la génération de journaux d'audit de sécurité;

d) permettre et interdire la génération et le traitement des alarmes.

Les fonctionnalités opérationnelles apparentées à l'audit sont:

a) générer les informations d'audit et d'alarmes (par exemple, générer des alarmes, des messages d'audit ou un rapport de sécurité);

b) enregistrer les informations d'audit et d'alarmes;

c) collecter/agréger les informations d'audit et d'alarmes;

d) analyser les informations d'audit et d'alarmes;

e) archiver les informations d'audit et d'alarmes.

8.2.1 Détermination et analyse des événements de sécurité – Critères pour les fonctions d'audit et d'alarmes de sécurité

Une alarme de sécurité et un message d'audit de sécurité identifient l'un et l'autre le type d'événement, la cause de l'événement, l'heure à laquelle l'événement a été détecté, l'identité du détecteur d'événement et les entités associées à cet événement (par exemple, le sujet et l'objet de l'action qui provoque l'événement).

Les critères sont établis pour préciser l'action à prendre lors du traitement des différents types d'information. Les critères définis sont:

Critères 1 – Filtrage d'événement

Ces critères détermineront les actions à prendre lors de la détection d'un événement lié à la sécurité.

Paramètres d'entrée possibles:

- type d'événement lié à la sécurité;
- heure du jour;
- entité provoquant l'événement.

Paramètres de sortie possibles:

- action à prendre;
- alarme de sécurité à générer;
- message d'audit de sécurité à générer.

Critères 2 – Examen du journal d'audit

Ces critères fournissent une base pour la sélection des informations contenues dans un ou plusieurs journaux d'audit de sécurité afin de recueillir des rapports de sécurité.

Paramètres d'entrée possibles:

- type d'enregistrement d'audit;
- type d'événement lié à la sécurité;
- heure de l'événement en cours d'examen;
- entité au sujet de laquelle l'information est demandée.

Paramètre de sortie possible:

- liste d'enregistrements sélectionnés.

Critères 3 – Critères d'analyse de journal d'audit

Les journaux d'audit seront analysés en évaluant l'apparition et la fréquence des événements avant de déterminer l'action à prendre.

Paramètres d'entrée possibles:

- type d'événement;
- nombre d'apparitions;
- intervalle de temps.

Paramètre de sortie possible:

- action à prendre.

NOTE – Les critères ne sont pas requis pour l'enregistrement d'audit de sécurité ou pour l'archivage d'audit de sécurité.

9 Mécanismes d'audit et d'alarmes de sécurité

Le service d'audit et d'alarmes de sécurité est différent des autres services de sécurité décrits dans la présente Recommandation | Norme internationale multiparties dans le sens où il n'y a pas un mécanisme unique spécifique qui pourra être utilisé pour fournir ce service. Les mécanismes d'audit peuvent être caractérisés comme des procédures basées sur plusieurs approches opérationnelles et de gestion. Pour cette raison, aucune présentation détaillée sur les mécanismes d'audit n'est incluse. Cependant, à titre d'exemple de type d'approches utilisées pour l'audit, les mécanismes pour la détection d'événement concernant la sécurité peuvent impliquer:

- la comparaison de l'activité d'une entité avec un profil connu; par exemple accès inhabituel basé sur l'heure ou la géographie, utilisation inhabituelle des ressources, etc.;
- la détection de l'accumulation d'un ou de plusieurs types d'événements durant un certain intervalle de temps;
- l'observation de l'absence d'un ou de plusieurs types d'événements durant un certain intervalle de temps.

La liste d'exemples ci-dessus n'est pas exhaustive.

10 Interaction avec d'autres services et mécanismes de sécurité

10.1 Authentification d'entité

Le transfert d'un journal d'audit de sécurité entre un *expéditeur d'audit* et un *collecteur d'audit* nécessite une authentification mutuelle pour que l'*expéditeur d'audit* délivre le journal de sécurité au *collecteur d'audit* supposé et que le *collecteur d'audit* reçoive le journal d'audit de sécurité de l'expéditeur supposé.

10.2 Authentification de l'origine des données

L'authentification de l'origine des données sert à connaître l'origine des messages d'audit de sécurité et des messages d'alarmes de sécurité. Elle est également utilisée par l'*analyseur d'audit* pour rejeter les messages reçus de générateurs d'événements ou d'analyseurs d'audit inconnus.

10.3 Contrôle d'accès

Les services de contrôle d'accès doivent être utilisés pour le stockage et le transfert des enregistrements de journal d'audit de sécurité. Le contrôle d'accès pourrait également être utilisé pour éviter un accès non autorisé à un journal d'audit de sécurité.

10.4 Confidentialité

Les services de confidentialité peuvent être utilisés durant la phase de transfert des journaux d'audit de sécurité, d'enregistrements sélectionnés d'audit de sécurité, de messages d'audit de sécurité et de messages d'alarme de sécurité. Le service de confidentialité peut également être utilisé pour protéger des enregistrements d'audit stockés.

10.5 Intégrité

Il est de première importance que toute modification d'un journal d'audit de sécurité, d'un ensemble d'enregistrements sélectionnés d'audit de sécurité, de message d'audit de sécurité ou d'un message d'alarme de sécurité soit détectée. Un service d'intégrité peut être utilisé pour cela.

10.6 Non-répudiation

Etant donné que le transfert des journaux de sécurité sera habituellement effectué au sein du même domaine de sécurité, un mécanisme de non-répudiation ne sera normalement pas utilisé.

Annexe A

Principes généraux d'audit et d'alarmes de sécurité pour l'interconnexion OSI

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

Il est recommandé que les types suivants d'événements liés à la sécurité soient toujours vérifiés:

- opérations liées à la gestion des informations de sécurité;
- opérations qui changent l'ensemble des événements à vérifier;
- opérations qui changent l'identification des objets vérifiés.

Cette annexe spécifie les événements OSI qui donneront potentiellement naissance à un événement lié à la sécurité. Il peut s'avérer nécessaire de vérifier aussi bien les conditions normales que les conditions anormales, par exemple chaque demande de connexion peut être sujette à un enregistrement de journal d'audit de sécurité, que cette demande soit ou non anormale et indépendamment du fait qu'elle ait été acceptée ou non.

Les événements suivants peuvent être, parmi d'autres, sujets à l'audit. Cette liste n'est pas exhaustive; elle est seulement fournie à titre d'indication.

Evénements liés à la sécurité relatifs à une connexion spécifique:

- demandes de connexion;
- connexion confirmée;
- demandes de déconnexion;
- déconnexion confirmée;
- statistiques sur la connexion.

Evénements liés à la sécurité relatifs à l'utilisation de services de sécurité:

- demandes de service de sécurité;
- usage des mécanismes de sécurité;
- alarmes de sécurité.

Evénements liés à la sécurité relatifs à la gestion:

- opérations de gestion;
- notifications de gestion.

La liste des événements vérifiables devrait inclure au moins:

- dénier accès;
- authentifier;
- changer attribut;
- créer objet;
- détruire objet;
- modifier objet;
- utiliser privilège.

Les événements suivants liés à la sécurité sont importants, en termes de services individuels de sécurité:

- authentification: vérifier succès;
- authentification: vérifier échec;
- contrôle d'accès: décider succès de l'accès;
- contrôle d'accès: décider échec de l'accès;
- non-répudiation: création non répudiable de message;
- non-répudiation: réception non répudiable de message;

– non-répudiation: répudiation sans succès d'événement;
– non-répudiation: répudiation avec succès d'événement;
– intégrité: utilisation de protection;
– intégrité: utilisation sans protection;
– intégrité: valider succès;
– intégrité: valider échec;
– confidentialité: utilisation de dissimulation;
– confidentialité: utilisation de révélation;
– audit: sélectionner événement pour audit;
– audit: désélectionner événement pour audit;
– audit: changer critère de sélection d'événement d'audit.

NOTE – Lorsque le contrôle d'accès est utilisé comme la base des mécanismes d'intégrité ou de confidentialité, les enregistrements d'audit associés avec «décider échec d'accès» peuvent être convertis en une indication explicite de tentatives de violations de la confidentialité ou de l'intégrité.

Tous les enregistrements de journal d'audit appartenant à une instance particulière de communication devraient être identifiés de façon non ambiguë pour garantir que les enregistrements peuvent être tracés.

Les services de la Rec. X.734 du CCITT | ISO/CEI 10164-5 peuvent être utilisés pour gérer le service d'envoi d'événement et pour configurer les filtres d'envoi d'événement spécifiant les critères de sélection pour les événements liés à la sécurité qui ont une importance pour l'audit de sécurité.

Le service de rapport de journal d'audit de sécurité de la Rec. X.740 du CCITT | ISO/CEI 10164-8 peut être utilisé par des entités pour générer des messages d'audit de sécurité.

Les services de la Rec. X.735 du CCITT | ISO/CEI 10164-6 peuvent être utilisés pour spécifier la sélection de messages d'audit de sécurité stockés dans des journaux d'audit de sécurité.

Le service de signalisation des alarmes de sécurité de la Rec. X.736 du CCITT | ISO/CEI 10164-7 peut être utilisé par une application de journal d'audit de sécurité pour générer des alarmes de sécurité.

Annexe B

Réalisation du modèle d'audit et d'alarmes de sécurité

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

Les fonctions du modèle d'audit et d'alarmes de sécurité sont indiquées sur la Figure 1. La procédure complète peut être distribuée sur plusieurs systèmes ouverts séparés, chaque système étant responsable d'un ou de plusieurs aspects de la procédure. Un exemple est donné sur la Figure B.1.

Un exemple d'événement de sécurité pourrait être une tentative de connexion à un système moyennant l'utilisation d'un mot de passe invalide sur un compte. L'analyse du journal d'audit pourrait révéler qu'il s'agissait d'une tentative parmi une série de tentatives de connexion sur le compte avec un mauvais mot de passe et une alarme pourrait être envoyée lorsqu'un seuil est atteint.

S1 est en mesure de détecter des événements liés à la sécurité et de les analyser en fonction de critères définis (critères 1) mais n'a aucune capacité de journal d'audit de sécurité, ses alarmes de sécurité sont donc envoyées à S2 et ses messages d'audit de sécurité sont envoyés à S3 pour inclusion dans le journal d'audit de sécurité.

S3 est responsable de la mise à jour du journal d'audit de sécurité. S3 fournit également à S6 l'accès au journal d'audit de sécurité et aux archives de journal d'audit de sécurité de façon à ce que les enregistrements de journal d'audit de sécurité puissent être sélectionnés en fonction de critères définis (critères 2) et rassemblés dans un rapport de sécurité.

S4 est responsable de l'archivage et de la recherche des enregistrements de journal de sécurité.

S5 contient une application qui analyse les enregistrements d'audit de sécurité (et les enregistrements archivés) en fonction de critères définis (critères 3) et envoie les alarmes à S2 lorsque les limites du seuil sont franchies ou lorsque les conditions d'alarmes sont détectées.

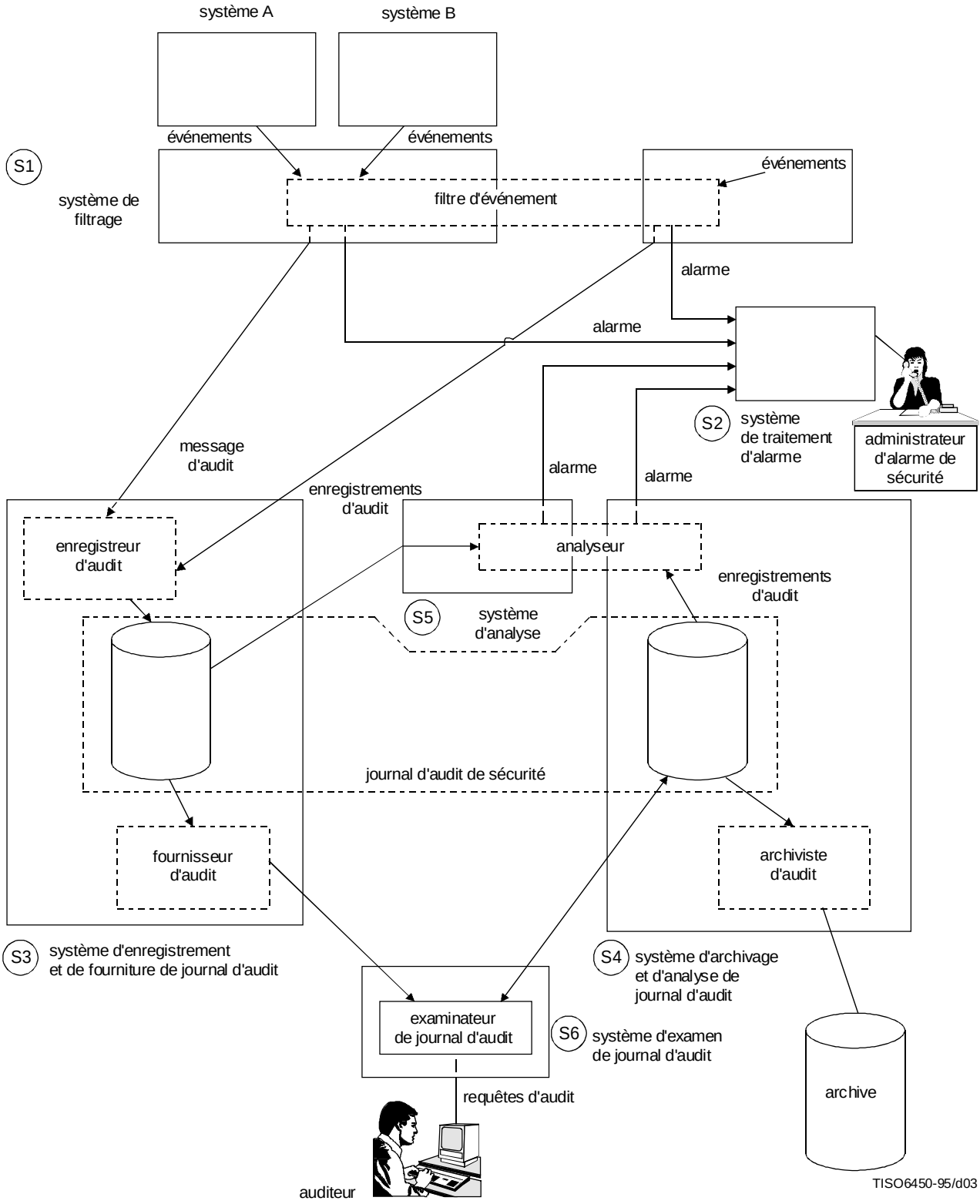

Figure B.1 – Exemple de réalisation d'un service distribué d'audit et d'alarmes de sécurité

Annexe C

Grandes lignes des fonctionnalités d'audit et d'alarmes de sécurité

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

<table>
<tr><td colspan="2" rowspan="4">Grandes lignes des fonctionnalités de sécurité</td><td rowspan="3">Eléments</td><td colspan="3">Entités: autorité d'audit; administrateur d'alarme; auditeur de sécurité.</td></tr>
<tr><td colspan="3">Fonctions: filtre d'événement; enregistreur d'audit; processeur d'alarmes; analyseur d'audit; examinateur de journal d'audit; fournisseur d'audit; expéditeur d'audit; collecteur de journal d'audit.</td></tr>
<tr><td colspan="3">Objets info: messages d'audit de sécurité; enregistrements d'audit de sécurité; rapports de sécurité.</td></tr>
<tr><td colspan="4">But du service: assurer que l'information liée à la sécurité des systèmes ouverts est enregistrée et, lorsque cela est approprié, signalée.</td></tr>
<tr><td rowspan="7">FONCTIONNALITÉS</td><td>Entité</td><td colspan="4">Autorité d'audit</td></tr>
<tr><td>Fonction</td><td colspan="4">Détermination et analyse des événements liés à la sécurité</td></tr>
<tr><td>Activité liée à la gestion</td><td colspan="4">Critère 1: filtrage d'événement
Critère 2: examen de journal d'audit
Critère 3: analyse de journal d'audit</td></tr>
<tr><td>Entité</td><td colspan="2">Administrateur d'alarme</td><td>Auditeur de sécurité</td><td>Initiateur/cible sujet/objet</td></tr>
<tr><td>Fonction</td><td colspan="2">Filtre d'événements
Processeur d'alarmes
Analyseur d'audit</td><td>Filtre d'événements
Analyseur d'audit
Enregistreur d'audit
Examinateur de journal d'audit
Fournisseur d'audit
Archiviste d'audit</td><td></td></tr>
<tr><td>Fonctionnalités opérationnelles apparentées</td><td colspan="2">Générer INFO.
Collecter INFO.
(INFO. signifie alarme)</td><td>Générer INFO.
Collecter INFO.
Analyser INFO.
(INFO. signifie message d'audit)</td><td></td></tr>
<tr><td rowspan="4">INFORMATION</td><td rowspan="2">Elément de données géré par une autorité d'audit</td><td colspan="2">Critères 1
– type d'événement
– temps
– entité</td><td>Critères 2
– type d'enregis-trement
– type d'événement</td><td>Critères 3
– type d'événement
– nombre d'apparitions
– intervalle de temps</td></tr>
<tr><td colspan="2">– Action à prendre
– Information de sécurité à générer</td><td>– Listes d'enregistrement</td><td>– Action à prendre</td></tr>
<tr><td>Type d'information utilisé dans l'opération</td><td colspan="4">– Type de message/information
– Identificateur caractéristique des éléments
– Cause du message
– Identificateur caractéristique de filtre d'événement, fournisseur d'audit et/ou enregistreur d'audit</td></tr>
<tr><td>Information de contrôle</td><td colspan="4">– Temps, apparitions</td></tr>
</table>

Annexe D

Heure d'enregistrement des événements d'audit

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

Une synchronisation parfaite entre les différents générateurs d'événements ou enregistreurs d'événements n'est pas, en pratique, possible. Dans un tel cas, un moyen de corréler le temps dans un domaine de sécurité est nécessaire. Un enregistrement d'audit de sécurité est créé à partir d'un message d'audit de sécurité qui peut ou non contenir une date. S'il contient une date, un enregistrement d'audit de sécurité est créé en utilisant l'indication de temps fournie dans le message d'audit de sécurité. Dans le dernier cas, l'enregistrement de sécurité créé sur réception de l'événement de sécurité lié à l'audit contient une date utilisant la référence de temps de l'*enregistreur d'audit*. Dans les deux cas, un enregistrement d'audit de la relation de temps entre le générateur d'événement et l'*enregistreur d'audit* doit être créé.

Dans le premier cas, une évaluation de la différence entre la référence de temps du générateur d'événement et la référence de temps de l'*enregistreur d'audit* doit être effectuée. L'enregistrement d'audit doit inclure l'identification du générateur d'événement, la référence de temps du générateur d'événement, la référence de temps de l'*enregistreur d'audit*, le retard entre les références de temps et la marge de tolérance sur le retard. Dans le dernier cas, l'enregistrement d'audit doit indiquer l'identification du générateur d'événement, la référence de temps de l'*enregistreur d'audit* et l'estimation du retard entre le générateur d'événement et l'*enregistreur d'audit* et la marge de tolérance sur le retard.

Il ne serait pas pratique de créer de tels enregistrements pour chaque événement. En fonction de la nature de la liaison ou de l'écart entre les références de temps, de tels enregistrements peuvent être créés. Si après une période d'observation il apparaît que le retard est négligeable, alors de tels enregistrements peuvent être omis. Une interpolation linéaire peut être utilisée lorsque les mesures de retard font défaut.

Le même type de problème peut intervenir entre la référence de temps d'un *enregistreur d'audit* et la référence de temps d'un *expéditeur d'audit* localisé sur un autre système. Cependant, dans ce cas les deux systèmes auront une référence de temps. Les mesures de la différence de temps peuvent être réalisées à tout instant entre les deux correspondants ou au moment du transfert d'un journal d'audit de sécurité. L'enregistrement devra inclure l'identification du générateur d'événement, l'identification de l'*expéditeur d'audit*, la référence de temps de l'*enregistreur d'audit*, l'estimation du retard entre l'*enregistreur d'audit* et l'*expéditeur d'audit*, et une marge de tolérance sur le retard.

La détermination de l'événement qui, parmi deux événements, est apparu en premier peut être effectuée en ajoutant ou en retranchant les retards entre une série de références de temps et en ajoutant toutes les marges de tolérance. Si le retard résultant est plus petit que la marge de tolérance alors la distinction ne peut pas être faite.

Le même argument s'applique également lorsqu'un rapport d'audit de sécurité doit être créé. En utilisant l'information fournie dans le journal d'audit de sécurité, il est possible de trier les événements en fonction des différentes références de temps. Cependant, l'ordonnancement d'un événement peut être uniquement garanti si la marge de tolérance du retard est plus courte que la différence de temps plus la marge de tolérance du prochain événement. A cette fin, il doit être possible de calculer pour chaque événement une marge de tolérance cumulative.