Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1550

(03/2017)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Echange d'informations sur la cybersécurité – Echange de politiques

Modèles de contrôle d'accès applicables aux réseaux d'échange d'informations sur les incidents

Recommandation UIT-T X.1550

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
Recommandations relatives aux infrastructures de clé publique	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1379
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	**X.1550–X.1559**
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

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

Recommandation UIT-T X.1550

Modèles de contrôle d'accès applicables aux réseaux d'échange d'informations sur les incidents

Résumé

La Recommandation UIT-T X.1550 présente les approches existantes pour mettre en oeuvre les politiques de contrôle d'accès applicables aux réseaux d'échange d'informations sur les incidents. Elle présente divers modèles de contrôle d'accès qui ont fait leur preuve, des modèles de partage d'informations ainsi que des critères pour évaluer les performances des réseaux d'échange d'informations sur les incidents. On considère que les solutions fondées sur les normes facilitent la mise en oeuvre de différents modèles de contrôle d'accès dans le cadre de divers modèles de partage d'informations sur les questions de cybersécurité et dans différents environnements de confiance.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1550	30-03-2017	17	11.1002/1000/13198

Mots clés

Contrôle d'accès, autorisation, CERT, CSIRT, CYBEX, IAM, réseau d'échange d'informations sur les incidents, intervention en cas d'incident.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) 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 développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

		Page
1	Domaine d'application	1
2	Références	1
3	Définitions	1
	3.1 Termes définis ailleurs	1
	3.2 Termes définis dans la présente Recommandation	2
4	Abréviations et acronymes	2
5	Conventions	3
6	Aperçu général	3
7	Classification des réseaux d'échange d'informations sur les incidents	4
	7.1 Environnements de fonctionnement	4
	7.2 Modèles d'échange d'informations sur les incidents	4
	7.3 Modèles de contrôle d'accès	4
	7.4 Niveau de confiance	6
8	Techniques facilitant la mise en oeuvre des politiques de contrôle d'accès	6
	8.1 Recommandations relatives à l'évaluation des langages d'expression des politiques	6
	8.2 Considérations relatives à la résolution de conflits de politique	7
	8.3 Recommandations sur l'évaluation des performances	8
Bibliographie		10

Recommandation UIT-T X.1550

Modèles de contrôle d'accès pour les réseaux d'échange d'informations sur les incidents

1 Domaine d'application

La présente Recommandation vise à exposer les approches existantes pour mettre en oeuvre les politiques de contrôle d'accès applicables aux réseaux d'échange d'informations sur les incidents. Elle présente divers modèles de contrôle d'accès éprouvés, des modèles de partage des informations ainsi que des critères pour évaluer les performances des réseaux d'échange d'informations sur les incidents. On examine les solutions fondées sur des normes visant à faciliter la mise en oeuvre de différents modèles de contrôle d'accès dans le cadre de différents modèles de partage des informations et dans différents environnements de confiance.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

[UIT-T X.1500] Recommandation UIT-T X.1500 (2011), *Techniques d'échange d'informations sur la cybersécurité.*

[UIT-T X.1570] Recommandation UIT-T X.1570 (2011), *Mécanismes de découverte pour l'échange d'informations de cybersécurité*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 contrôle d'accès [b-UIT-T X.1252]: procédure utilisée pour déterminer si l'accès à des ressources, fonctionnalités, services ou informations devrait être accordé à une entité, compte tenu des règles préétablies et des droits spécifiques ou de l'autorité associés à l'entité requérante.

3.1.2 autorisation [b-UIT-T M.3345]: modalités et conditions selon lesquelles les acteurs de la gestion de libre service peuvent utiliser des fonctions en libre service, et actions en libre service qu'ils sont autorisés à effectuer.

3.1.3 échange d'informations sur les incidents [UIT-T X.1570]: transfert d'informations de cybersécurité entre au moins deux entités de cybersécurité. Ce transfert peut être unidirectionnel, bidirectionnel ou multidirectionnel, c'est-à-dire multipoint à multipoint.

NOTE – Dans la présente Recommandation, les termes "échange d'informations sur les incidents" et "échange d'informations" sont considérés comme étant équivalents.

3.1.4 domaine de confiance [b-UIT-T M.3410]: ensemble d'informations et de ressources associées composé d'utilisateurs, de réseaux, de répertoires de données et d'applications manipulant les données dans ces répertoires. Différents domaines de confiance peuvent utiliser en partage les mêmes composants physiques. En outre, un même domaine de confiance peut appliquer différents niveaux de confiance, en fonction de ce que les utilisateurs ont besoin de savoir et de la sensibilité des informations et des ressources associées.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 conflit de politique de contrôle d'accès: situation dans laquelle les actions relatives à deux règles se contredisent. L'entité qui met en oeuvre la politique ne sera pas en mesure de déterminer quelle action entreprendre.

NOTE – Cette définition repose sur la définition du terme "conflit de politique" donnée dans [b-UIT-T X.1036].

3.2.2 résolution dynamique de conflit de politique: stratégies de résolution des conflits appliquées pendant l'exécution.

3.2.3 réseaux d'échange d'informations sur les incidents: généralisation de l'infrastructure opérationnelle d'échange d'informations sur la cybsersécurité (CYBEX) fondée sur une gestion centralisée ou fédérée.

3.2.4 informations sur les incidents: sous-ensemble des informations sur la cybersécurité, des informations structurées ou des connaissances structurées concernant une analyse scientifique et technique se rapportant à des incidents ou des événements.

NOTE – Cette définition repose sur la description du terme "échange (d'informations de cybersécurité)" donnée dans [b-UIT-T X.1570].

3.2.5 résolution statique de conflit de politique: stratégies de résolution des conflits appliquées au stade de la conception.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ABAC contrôle d'accès basé sur les attributs (*attribute based access control*)

ACL liste de contrôle d'accès (*access control list*)

CERT équipe d'intervention en cas d'urgence informatique (*computer emergency response team*)

CSIRT équipe d'intervention en cas d'incident relatif à la sécurité informatique (*computer security incident response team*)

CYBEX échange d'informations sur la cybersécurité (*CYBersecurity information EXchange*)

DAC contrôle d'accès discrétionnaire (*discretionary access control*)

IAM gestion des identités et des accès (*identity and access management*)

IODEF format d'échange de description d'incidents en tant qu'objets (*incident object description exchange format*)

IT technologies de l'information (*information technology*)

MAC contrôle d'accès obligatoire (*mandatory access control*)

PBAC contrôle d'accès basé sur la politique (*policy based access control*)

PDP point de décision de politique (*policy decision point*)

PERMIS normes d'infrastructure de gestion de privilège et de rôle (*privilege and role management infrastructure standards*)

RAdAC contrôle d'accès adapté au risque (*risk-adaptive access control*)

RBAC contrôle d'accès fondé sur le rôle (*role based access control*)

RID défense en temps réel interréseaux (*real-time inter-network defense*)

RIDT transport de messages de défense interréseaux en temps réel (*real-time inter-network defense transport*)

STIX expression d'informations structurées sur les menaces (*structured threat information expression*)

TAXII échange sécurisé et automatisé d'informations sur les indicateurs (*trusted automated exchange of indicator information*)

TBAC contrôle d'accès basé sur la tâche (*task based access control*)

TBAM gestion d'accès basée sur les tâches (*task based access management*)

XACML langage de balisage extensible de contrôle d'accès (*eXtensible access control markup language*)

XML langage de balisage extensible (*extensible markup language*)

5 Conventions

Dans le cadre de la présente Recommandation, le terme "contrôle d'accès" désigne un mécanisme générique prenant en charge des procédures d'autorisation.

6 Aperçu général

L'atténuation des risques peut être nécessaire pour réduire les coûts financiers liés à l'atténuation des attaques informatiques, et fournir des garanties de sécurité au sein d'une organisation/collaboration ou d'un service/système. Les réseaux d'échange d'informations sur les incidents fonctionnent dans le but de prévenir ou d'atténuer les risques associés aux attaques informatiques. Les pratiques en matière d'échange d'informations sur les incidents dans le domaine de la cybersécurité font intervenir divers modèles de partage d'informations qui sont mis en oeuvre dans des environnements centralisés ou fédérés. Le partage d'informations sur les incidents repose sur un niveau de confiance déterminé qui est proportionnel aux risques associés et qui oblige à garantir que des informations confidentielles ou sensibles ne sont pas partagées de façon inappropriée. Par conséquent, certains modèles de contrôle d'accès sont plus efficaces que d'autres en matière de résultats, de mise en oeuvre et d'assurance de sécurité.

La croissance globale et l'intégration mutuelle des systèmes d'information mondiaux ont stimulé l'élaboration de modèles de contrôle d'accès évolués qui sous-tendent les processus d'autorisation. Les langages existants en matière de politique de contrôle d'accès facilitent la mise en place de politiques sécuritaires et pose des problèmes particuliers qui sont inhérents aux différents modèles d'accès et aux environnements d'exploitation.

Les approches et les mécanismes décrits dans la présente Recommandation peuvent servir de lignes directrices pour la mise en oeuvre des politiques de contrôle d'accès à la base de l'échange d'informations sur les formats de cybersécurité (CYBEX) et des protocoles de transport tels que: le format d'échange de description d'incidents en tant qu'objets (IODEF) [b-UIT-T X.1541]; la défense en temps réel interréseaux (RID) [b-UIT-T X.1580] et le transport de communications de défense interréseaux en temps réel (RIDT) [b-UIT-T X.1581]; l'expression structurée d'informations sur les menaces (STIX) [b-stix] et l'échange sécurisé et automatisé d'informations sur les indicateurs (TAXII) [b-taxii]; et autres.

7 Classification des réseaux d'échange d'informations sur les incidents

7.1 Environnements de fonctionnement

Les réseaux d'échange d'informations sur les incidents fonctionnent dans les environnements suivants:

– domaine de confiance unique (gestion centralisée);

– domaines de confiance fédérés (gestion décentralisée).

7.2 Modèles d'échange d'informations sur les incidents

Les modèles d'échange d'informations sur les incidents sont représentés comme suit:

– "Entre homologues" ("Peer-to-peer"). Echange d'informations unidirectionnel ou bidirectionnel entre deux participants.

– "Modèle en étoile" ("Hub-spokes"). Ce type de modèle a souvent un pivot central qui reçoit les données provenant des membres participants. Le pôle peut redistribuer les données d'entrée directement à d'autres membres ou bien fournir des services à valeur ajoutée et envoyer une information nouvelle (probablement plus utile) aux membres. Selon cette approche, le pivot fait fonction de centre d'échange qui peut faciliter le partage de l'information tout en protégeant les identités des membres. Le problème qui se pose alors est que le partage de l'information suivant ce modèle suppose un niveau élevé de confiance vis-à-vis du pivot [Modèles b-MITRE].

– "Envoyer à tous" ("Post-to-all"). Ce modèle permet à n'importe quel participant de partager les informations avec tous les membres de la liste complète, sans passer par un pivot central. Etant donné que les membres échangent directement l'information entre eux, la diffusion de l'information est rapide et peut être facilement transposée à plusieurs participants [Modèles b-MITRE].

Sur la base de ces trois modèles, les modèles orientés service suivants peuvent être mis en place:

– "Découverte-demande-réponse" ("Discovery-request-response"). Il s'agit d'un modèle en deux étapes: pendant la première étape (facultative), les mécanismes de découverte [UIT-T X.1570] sont utilisés pour identifier les sources centralisées ou distribuées des informations relatives aux incidents et, pendant la seconde étape, les consommateurs reçoivent des informations en interrogeant les bases de données et les décisions concernant les réponses sont fondées sur le modèle de contrôle d'accès.

– "Découverte-abonnement-notification". Il s'agit d'un modèle en deux étapes: pendant la première étape (facultative), les mécanismes de découverte [UIT-T X.1570] sont utilisés pour identifier les sources centralisées ou distribuées des informations relatives aux incidents et, pendant la seconde étape, les consommateurs reçoivent les données en s'abonnant et reçoivent des informations à partir de sources sélectionnées sous la forme de notifications.

7.3 Modèles de contrôle d'accès

Les modèles de contrôle d'accès constituent la base de toute politique en matière de sécurité. Dans la pratique, ces modèles sont formalisés par des dialectes spécifiques du langage de balisage extensible (XML) (langages de la politique de contrôle d'accès).

Conformément aux Modèles NIST [b-NIST Models], les modèles de contrôle d'accès suivants sont présentés, depuis les modèles conservateurs (prenant en compte des politiques très peu détaillées) jusqu'aux modèles adaptatifs (prenant en compte des politiques plus détaillées et dépendantes de l'environnement):

– **ACL/DAC**. Le concept de listes de contrôle d'accès (ACL)/de contrôle d'accès discrétionnaire (DAC) est un concept où chaque ressource d'un système dont l'accès doit être contrôlé est définie en tant qu'objet, ayant sa propre liste de correspondances entre l'ensemble des entités demandant l'accès à la ressource et l'ensemble des mesures que chaque entité peut entreprendre concernant la ressource.

– **MAC**. Le contrôle d'accès obligatoire (MAC) est le plus souvent utilisé dans des systèmes où l'attention est accordée en priorité à la confidentialité des données. Le MAC consiste à attribuer une étiquette de classification à chaque ressource du fichier. Les classifications se font par catégorie d'information et niveau de sensibilité, tel que confidentiel, secret ou top secret. Il existe une classification similaire pour les sujets: chaque sujet se voit attribuer une autorisation d'accès. Lorsqu'un sujet tente d'obtenir l'accès à une ressource particulière, quelle qu'elle soit, le système vérifie les privilèges de ce sujet pour déterminer si l'accès sera autorisé; l'autorisation d'accès donnée au sujet dépend de la classification de la ressource.

– **RBAC**. Dans le modèle de contrôle d'accès basé sur les rôles (RBAC), l'accès à une ressource est déterminé sur la base des relations entre le demandeur et l'organisation ou la personne qui exerce un contrôle sur la ressource; le rôle ou la fonction du demandeur déterminera si l'accès sera autorisé ou refusé.

– **TBAC/TBAM**. Le contrôle d'accès basé sur les tâches (TBAC)/La gestion d'accès basée sur les tâches (TBAM) [b-IEEE TBAC] est une extension du modèle RBAC fondée sur la définition de tâches opérationnelles qui permettent une approche plus détaillée en matière de contrôle d'accès.

– **ABAC**. Le modèle de contrôle d'accès basé sur les attributs (ABAC) utilise des mécanismes tels que les listes de contrôles d'accès (ACL) qui contiennent les attributs des sujets ainsi que les opérations autorisées sur une ressource donnée. Lorsqu'un attribut correspond à celui figurant dans la liste ACL, le sujet se voit attribuer le droit d'effectuer sur la ressource les opérations mentionnées pour cet attribut dans la liste ACL.

– **PBAC**. Le contrôle d'accès basé sur la politique (PBAC) est une harmonisation et une normalisation du modèle ABAC au niveau d'une entreprise, à l'appui d'objectifs concrets de gouvernance. Le modèle PBAC combine les attributs de la ressource, de l'environnement et du demandeur et l'information relative à l'ensemble particulier de circonstances dans lesquelles la demande d'accès a été formulée, et utilise des ensembles de règles qui déterminent si l'accès est autorisé conformément à la politique de l'organisation concernant ces attributs et dans les circonstances données.

– **RAdAC**. Le modèle de contrôle d'accès adapté au risque (RAdAC) a été conçu dans le but de fournir un contrôle d'accès en temps réel, adapté et sensible au risque. Il élargit d'autres modèles d'accès précédents, en introduisant des conditions environnementales, ainsi que des niveaux de risque, dans le processus décisionnel relatif au contrôle d'accès. Il combine des informations sur la fiabilité d'une personne (ou d'une machine), des informations sur l'infrastructure des technologies de l'information des entreprises et des facteurs de risque liés à l'environnement, et utilise toutes ces informations pour établir une mesure globale quantifiable du risque. Ce modèle de contrôle intègre également des facteurs de situation dans le processus de prise de décision. Ces facteurs pourraient contenir des informations sur le niveau concret des menaces auxquelles une organisation est confrontée, sur la base des données provenant d'autres sources, telles que les équipes d'intervention en cas d'urgence informatique (CERT), les équipes d'intervention en cas d'incident lié à la sécurité informatique (CSIRT) ou les fournisseurs de systèmes de sécurité. (Voir [b-IEEE ARES], [b-NIST RADAC].)

7.4 Niveau de confiance

Afin de souligner la relation de dépendance entre les niveaux de confiance et les risques, il est recommandé d'utiliser les niveaux de confiance quantitatifs suivants pour les réseaux d'échange d'informations sur les incidents: **faible**, **moyen** et **élevé**. Il va de soi que plus le niveau de confiance est élevé, plus les exigences sont simples et moins le contrôle d'accès est détaillé. Par conséquent, le niveau de confiance influe directement sur le niveau de complexité des mécanismes de contrôle d'accès.

Les méthodes d'évaluation quantitative et qualitative des niveaux de confiance n'entrent pas dans le cadre de la présente Recommandation.

La corrélation suivante entre les niveaux de confiance et les modèles de partage est examinée:

– "Envoyer à tous" ("Post-to-all"): ce modèle nécessite généralement un degré de confiance **élevé** entre les participants.

– "Modèle en étoile" ("Hub-spokes"): ce modèle nécessite généralement un degré de confiance élevé ou moyen (dans la mesure où le pôle peut filtrer l'information).

– "Entre homologues" ("Peer-to-peer"): en général, ce modèle peut ne pas nécessiter un degré de confiance élevé, dans la mesure où le canal de communication unique peut être contrôlé au moyen de méthodes très diverses.

Les modèles de partage de niveau plus élevé ne dépendent pas explicitement du degré de confiance, mais dans les cas où les participants sont plus nombreux et les environnements plus complexes, il est possible que ces modèles nécessitent des modèles de contrôle d'accès plus évolués.

A cet égard, la classification suivante, indiquée dans la Figure 1, est examinée:

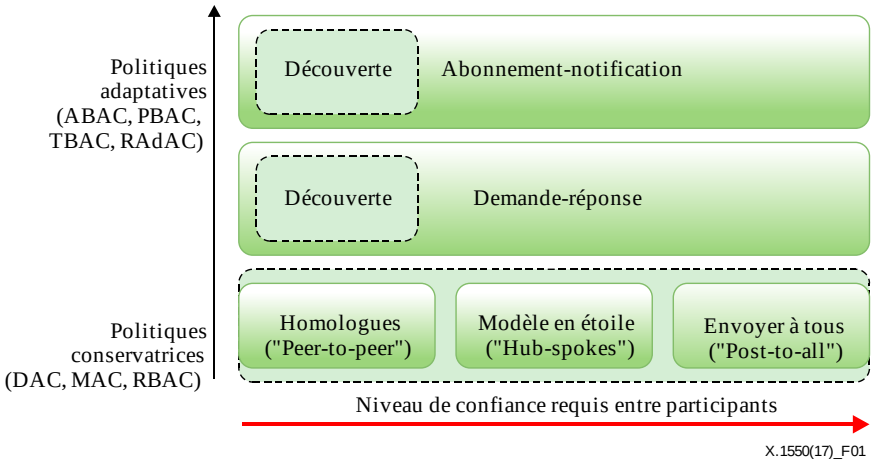

Figure 1 – Classification des modèles de contrôle d'accès, des modèles de partage des informations et des niveaux de confiance

8 Techniques facilitant la mise en oeuvre des politiques de contrôle d'accès

8.1 Recommandations relatives à l'évaluation des langages d'expression des politiques

Les langages suivants comptent parmi les langages de contrôle d'accès éprouvés qui sont utilisés afin de faciliter la mise en oeuvre des politiques de contrôle d'accès dans les systèmes de gestion d'identité et d'accès (IAM):

– Langage de balisage extensible de contrôle d'accès (**XACML**). Cette norme définit un langage de politique de contrôle d'accès déclaratif (pour le modèle ABAC), appliqué dans le langage de balisage, ainsi qu'un modèle d'application qui décrit comment évaluer les demandes d'accès conformément aux règles définies dans les politiques.

  NOTE 1 – La version XACML 2.0 a été adoptée en tant que [b-UIT-T X.1142].

  NOTE 2 – La version XACML 3.0 a été adoptée en tant que [b-UIT-T X.1144].

– Les normes pour les infrastructures de gestion des privilèges et des rôles (**PERMIS**). Il s'agit d'un système d'autorisation complexe basé sur la politique qui applique une version améliorée du RBAC (semblable à l'ABAC). La politique du système PERMIS est fondée sur XML et assure une interaction avec XACML, ce qui permet à PERMIS et XACML d'échanger entre eux de façon transparente des points de décision de politique (PDP).

Il est recommandé d'évaluer l'applicabilité des modèles de contrôle d'accès dans divers environnements et de déterminer les exigences minimales concernant leur application avec des langages de politique tels que [b-UIT-T X.1142], [b-UIT-T X.1144] ou [b-UKENT PERMIS].

Le Tableau 1 fournit un exemple d'évaluation.

Tableau 1 – Application des modèles de contrôle d'accès dans divers environnements dans des langages de définition des politiques

Modèle/ environnement	ACL/ DAC	MAC	RBAC	ABAC	TBAC/ TBAM	PBAC	RAdAC
Centralisé	[b-UIT-T X.1142]; PERMIS	XACML expérimental	[b-UIT-T X.1142]; PERMIS	[b-UIT-T X.1142]; PERMIS*	Expérimental	[b-UIT-T X.1142]; PERMIS*	[b-UIT-T X.1142]; PERMIS*
Fédéré	[b-UIT-T X.1144]; PERMIS	XACML expérimental	[b-UIT-T X.1144]; PERMIS	[b-UIT-T X.1144]; PERMIS*	Expérimental	–	[b-UIT-T X.1144]

NOTE 1 – Les versions XACMLv2 [b-UIT-T X.1142] et XACMLv3 [b-UIT-T X.1144] sont séparées depuis l'apparition de la "délégation", qui est requise pour la plupart des environnements fédérés, dans la version XACMLv3.

NOTE 2 – Les applications MAC connues nécessitent une extension XACML.

NOTE 3 – A l'heure actuelle, les mises en oeuvre TBAC/TBAM nécessitent une extension XACML considérée comme expérimentale.

NOTE 4 – Par définition, le modèle PBAC ne s'applique que dans des environnements centralisés; dans des environnements fédérés, il peut être nécessaire d'utiliser le modèle RAdAC.

NOTE 5 – L'astérisque (par exemple, PERMIS*) indique que certaines restrictions concernant la mise en oeuvre PERMIS d'ABAC (PBAC et RAdAC, s'ils sont considérés comme une extension du modèle ABAC) sont indiquées dans [b-UKENT PERMIS].

8.2 Considérations relatives à la résolution de conflits de politique

Un conflit de politique de contrôle d'accès entraîne des actions contradictoires relatives à deux ou plusieurs règles de politique. Le mécanisme de base permettant de résoudre les conflits de politique consiste à élaborer des règles de politique claires (résolution statique du conflit). Une autre approche est fondée sur l'évaluation des politiques pendant l'exécution (résolution dynamique du conflit) [b-UKENT PERMIS].

Si la résolution statique du conflit, dans le cas de systèmes centralisés, est considérée comme possible [b-USB CONFLICT], [b-SPIIRAN POLICY], dans un environnement fédéré et dynamique l'utilisation de méthodes de résolution statique d'un conflit peut s'avérer problématique.

Les stratégies de base de résolution statique d'un conflit comportent les caractéristiques suivantes:

– Refus prioritaire ("Deny-override"). Les règles conflictuelles sont associées; l'action "refuser" est préférée à l'action "autoriser".

– Autorisation prioritaire ("Permit-override"). Les règles conflictuelles sont associées; l'action "autoriser" est préférée à l'action "refuser".

– Le premier s'applique ("First-applicable"). La première action parmi les règles conflictuelles est exécutée.

Les stratégies [b-UKENT PERMIS] en matière de résolution dynamique de conflit de politique font appel à des algorithmes pour sélectionner la stratégie statique la mieux adaptée, compte tenu du contexte de la demande d'accès en cours.

Il est recommandé d'évaluer les stratégies de résolution de conflit du point de vue de leur performance et de leur compatibilité avec les modèles de contrôle d'accès dans divers environnements.

Compte tenu de l'évaluation des performances des méthodes statiques de résolution de conflit de politique [b-IJCSIT XACML] lorsqu'elles sont utilisées conjointement avec les méthodes dynamiques de contrôle d'accès tel que [b-FUSCAT RADAC], il est recommandé de réduire au minimum le nombre de politiques, sans nuire au niveau d'assurance de sécurité ou de recourir à des stratégies dynamiques de résolution de conflit.

Le Tableau 2 fournit un exemple d'évaluation.

Tableau 2 – Résolution de conflits de politique pour les modèles de contrôle d'accès dans divers environnements

Modèle/ environnement	ACL/ DAC	MAC	RBAC	ABAC	TBAC/ TBAM	PBAC (Note)	RAdAC
Centralisé	Statique	Statique	Statique	Statique	Statique	Statique	Dynamique
Fédéré	Dynamique	Dynamique	Dynamique	Dynamique	Dynamique	–	Dynamique
NOTE – Par définition, le modèle PBAC peut être appliqué uniquement dans des environnements centralisés.							

8.3 Recommandations sur l'évaluation des performances

Bien que les langages de balisage (tels que [b-W3C XML] et [b-ECMA JSON]) soient censés être lisibles par l'homme, l'existence d'un grand nombre de règles d'accès bien établies et évoluées peut poser problème pour le profilage et le débogage des politiques mises en oeuvre.

Du fait de la complexité des services d'échange d'informations sur les incidents dans les réseaux d'échange d'informations sur les incidents, il peut être nécessaire d'utiliser des modèles de contrôle d'accès évolués. Dans le cas d'un fonctionnement dans des environnements fédérés, il peut en résulter une dégradation de la qualité de fonctionnement des réseaux d'échange d'informations sur les incidents, et, par voie de conséquence, des problèmes d'assurance de sécurité.

Pour évaluer la qualité/la performance/la conformité des politiques, les paramètres correspondants peuvent être calculés. Les mécanismes d'évaluation de ces paramètres dans le cadre des réseaux d'échange d'informations sur les incidents ne relèvent pas de la présente Recommandation. Toutefois, un ensemble de critères et d'indicateurs pour de telles évaluations est recommandé [b-KIT PERFIAM] et [b-NIST METRICS]:

– **Temps de réponse**. Le temps de réponse pour les composants de l'infrastructure IAM et les composants du partage d'information permet l'évaluation des paramètres de base des performances.

– **Décisions de contrôle d'accès incorrectes**. L'évaluation du nombre de décisions d'authentification ou d'autorisation dans des situations tendues fournit des informations sur la robustesse de l'infrastructure IAM sous-jacente.
– **Composantes de confiance**. Le contrôle d'accès est une tâche sensible qui nécessite un certain niveau de confiance entre les entités coopérantes. De fait, une liste des composants de confiance dans le cadre d'une décision de contrôle d'accès est utile en vue de déterminer d'éventuelles pertes de données.
– **Distribution de la politique**. Permet d'évaluer les capacités et la performance de la distribution de la politique dans des systèmes de contrôle d'accès centralisés ou fédérés.
– **Facilité d'attribution des privilèges**. Détermine le nombre d'étapes nécessaires pour attribuer/changer/supprimer les capacités d'un sujet ou d'un groupe, ou pour en hériter.
– **Qualité de l'expression de la politique**. Détermine si le contrôle d'accès pourrait être défini au moyen d'expressions logiques et programmables.
– **Capacités de délégation**. Détermine si un système de contrôle d'accès est capable de déléguer des privilèges aux sujets.
– **Combinaison de politiques et résolution**. Détermine les stratégies de combinaison de politiques qui sont utilisées pour résoudre des conflits (le cas échéant).
– **Contournement**. Détermine si telle ou telle composante contourne la politique de contrôle d'accès.
– **Sécurité**. Détermine les possibilités existantes pour contrôler le respect de la sécurité, par exemple l'imposition de restrictions aux règles de contrôle d'accès afin d'éviter tout relèvement des privilèges.
– **Niveau de détail**. Détermine le niveau de détail qu'un système de contrôle d'accès peut contrôler. Cela pourrait correspondre à un ensemble d'attributs du sujet qui sont évalués lors de la procédure de contrôle d'accès.
– **Intégration de l'authentification**. Détermine si un système de contrôle d'accès est capable de s'intégrer aux systèmes d'authentification.

Bibliographie

[b-UIT-T M.3345] Recommandation UIT-T M.3345 (2009), *Principes de la gestion de libre service.*

[b-UIT-T M.3410] Recommandation UIT-T M.3410 (2008), *Lignes directrices et prescriptions pour les systèmes de gestion de la sécurité en gestion des télécommunications.*

[b-UIT-T X.1036] Recommandation UIT-T X.1036 (2007), *Cadre applicable à la création, au stockage, à la distribution et à la mise en vigueur des politiques de sécurité de réseau.*

[b-UIT-T X.1142] Recommandation UIT-T X.1142 (2006), *Langage de balisage extensible de contrôle d'accès (XACML 2.0).*

[b-UIT-T X.1144] Recommandation UIT-T X.1144 (2013), *Langage de balisage extensible de contrôle d'accès (XACML) 3.0.*

[b-UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité.*

[b-UIT-T X.1541] Recommandation UIT-T X.1541 (2012), *Format d'échange de description d'objet incident.*

[b-UIT-T X.1580] Recommandation UIT-T X.1580 (2012), *Défense interréseaux en temps réel.*

[b-UIT-T X.1581] Recommandation UIT-T X.1581 (2012), *Transport de messages de défense interréseaux en temps réel.*

[b-IEEE TBAC] IEEE IET Software (2008), *Types for task-based access control in workflow systems*.

[b-IEEE ARES] IEEE (2011), *Sixth International Conference on Availability, Reliability and Security (ARES), An Attribute Based Framework for Risk-Adaptive Access Control Models*.

[b-ECMA JSON] ECMA International (2013), *The JSON Data Interchange Format.*

[b-FUSCAT RADAC] Federal University of Santa Catarina (2014), *A Dynamic Risk-based Access Control Architecture for Cloud Computing*.

[b-IJCSIT XACML] International Journal of Computer Science and Information Technology (IJCSIT) (2010), *Design and evaluation of XACML conflict policies detection mechanism*.

[b-KIT PERFIAM] Karlsruhe Institute of Technology (2009), *Performance Evaluation of Identity and Access Management Systems in Federated Environments*.

[b-MITRE Models] The MITRE Corporation (2012), *Cyber Information-Sharing Models*.

[b-NIST METRICS] NIST Internal Report 7874 (2012), *Guidelines for Access Control System Evaluation Metrics*.

[b-NIST Models] NIST Computer Security Division (2009), *A survey of access control models*.

[b-NIST RADAC] NIST Computer Security Division (2009), *Risk-adaptable access control (RAdAC).*

[b-SPIIRAN POLICY] SPIIRAN (2006), *Conflict Detection and Resolution in Security Policies of Computer Networks*.

[b-stix] OASIS CTI TC (2017), *A structured language for cyber threat intelligence*. <https://oasis-open.github.io/cti-documentation/>

[b-taxii] OASIS CTI TC (2017), *A transport mechanism for sharing cyber threat intelligence*. <https://oasis-open.github.io/cti-documentation/>

[b-UKENT PERMIS] The University of Kent (2013), *Adding privacy protection to policy based authorisation systems*.

[b-USB CONFLICT] IEEE First AESS European Conference on Satellite Telecommunications (ESTEL) (2012), *Conflict detection in security policies using Semantic Web technology*.

[b-W3C XML] W3C (1997), *Extensible Markup Language (XML)*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
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	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; 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 et mesures et tests associés
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, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2017