

- [SECM98]:** Network Management, Requirements and Logical MIB: ATM Security Services Phase 1, The ATM Forum Technical Committee. Avril 1998.
- [SKM97]:** System Security Management via SNMP, F. Stamatelopoulos, G. Koutepas, B. Maglaris, Proceedings of the 4th HPOVUA workshop. Avril 1997.
- [TCSEC83]:** Trusted Computer System Evaluation Criteria, Department of Defense Computer Security Center. Août 1983.
- [TIB95]:** Détection d'intrusions dans les réseaux de communication, K. Tibourtine, Thèse de doctorat. Université de Paris Sud. Février 1995.
- [UNI31]:** ATM User-Network Interface (UNI) specification. Version 3.1. The ATM Forum Technical Committee. Septembre 1994.
- [UNI40]:** ATM User-Network Interface (UNI) Signalling Specification. Version 4.0. The ATM Forum Technical Committee. Juillet 1996.
- [X263]:** Réseaux pour données et communication entre systèmes ouverts. Interconnexion des systèmes ouverts - identification des protocoles. Technologies de l'information - identification des protocoles dans la couche réseau. Recommandation ITU-T X263. Novembre 1995.

CI: Connection Identifier.
CN: Connected Number.
cPN: Calling Party Number.
CPN: Called Party Number.
cPSA: Calling Party Subaddress.
CPSA: Called Party Subaddress.
CS: Call State.
CSA: Connected Subaddress.
CSS: Connection Scope Selection.

NHLC: Narrowband High Layer Information.
NI: Notification Indication.
NLLC: Narrowband Low Layer Information.
OAMTD: OAM Traffic Descriptor.
pI: Priority Information.
PI: Progress Indicator.
QoS: QoS Parameters.
RI: Restart Indicator.
TNS: Transit Network Selection

Autres

ADTF: ACR Decrease Time Factor
BEI: Best Effort Indicator
CDF: Cutoff Decrease Factor
CDV: Cell Delay Variation
CLR: Cell Loss Ratio
FD: Frame Discard
SCR: Sustainable Cell Rate

ICR: Initial Cell Rate
MBS: Maximum Burst Size
MCR: Minimum Cell Rate
PCR: Peak Cell Rate
RDF: Rate Decrease Factor
RIF: Rate Increase Factor
SMI: Structure of Management Information

7 Références

- [**Atm97**]: ATM in Europe: The User Handbook. European Market Awareness Committee. Version 1.0. The ATM Forum. Juillet 1997.
- [**Atom98**]: Definitions of Supplemental Managed Objects for ATM Management, Faye Ly, Michael Noto, Andrew Smith, Kaj Tesink, Internet Draft. Mars 1998.
- [**AD97**]: The role of the Time Parameter in a network security management model, T. Apostolopoulos, V. Daskalou, Proceedings of the second IEEE symposium on computers and communications. Juillet 1997.
- [**BE98**]: Securing «classical IP over ATM Networks», Carsten Benecke, Uwe Ellermann, proceedings of the 7th USENIX security symposium. Janvier 1998.
- [**Darpa97**]: Architecture Design of a scalable Intrusion Detection System for the Emerging Network Infrastructure, Technical Report, Rome Lab. Avril 1997.
- [**FIPS188**]: Standard Security Label For Information Transfer, Federal Information Processing Standards Publication 188, NIST. Septembre 1994.
- [**H245**]: Audiovisual and multimedia systems. Line transmission of non-telephone signals. Control protocol for multimedia communication. ITU-T recommendation H245. ITU-T. Mars 1996.
- [**I610**]: Réseau numérique avec intégration des services, principes de maintenance. Principes et fonctions d'exploitation et de maintenance du RNIS à large bande. Recommandation UIT-T I610. UIT-T. Novembre 1995.
- [**Kar98**]: Integrated Access Control Management, Günter Karjoth. 1998.
- [**Pa098**]: Une analyse des MIBs du modèle ATM dans l'optique du contrôle d'accès. Olivier Paul. Juillet 1998.
- [**SEC98**]: ATM Security Specification Version 1.0, The ATM Forum Technical Committee. Juillet 1998.

Tableau 2 : Comparaison des informations de contrôle d'accès fournies par les deux méthodes.

Type d'information	Sous Type	Flux	MIBs
	FD	X	O
	BEI	X	X
	Icr, Nrm. Trm, Cdf, Rif, Rdf, Adtf, Crm	X	X
	CDV, CLR	X	O
	Descripteur d'équipement d'extrémité	X	O
Informations diverses	Informations de transit	X	O
	Informations horaires	O	X
	Routage	O	X

Note: X: information présente, x: information présente mais moins précise, O: information absente.

Les différences entre les informations fournies par les deux méthodes, bien que peu importantes, sont dues au décalage temporel existant entre la parution des spécifications concernant la signalisation et celles concernant les MIBs. Ainsi la prochaine version de l'ATM-MIB (IETF) [Atom98] contient la plupart des paramètres manquants dans la version actuelle (celle-ci datant d'août 1994).

On peut donc estimer que d'une part les informations majeures relatives à une connexion peuvent être trouvées dans les MIBs et d'autre part que les MIBs contiennent des informations synthétiques que l'on ne peut retrouver dans les flux de manière directe.

Cette constatation nous pousse à envisager dans de futurs travaux une architecture de contrôle d'accès utilisant les informations de gestion contenues dans les MIBs.

6 Annexe: Abréviations.

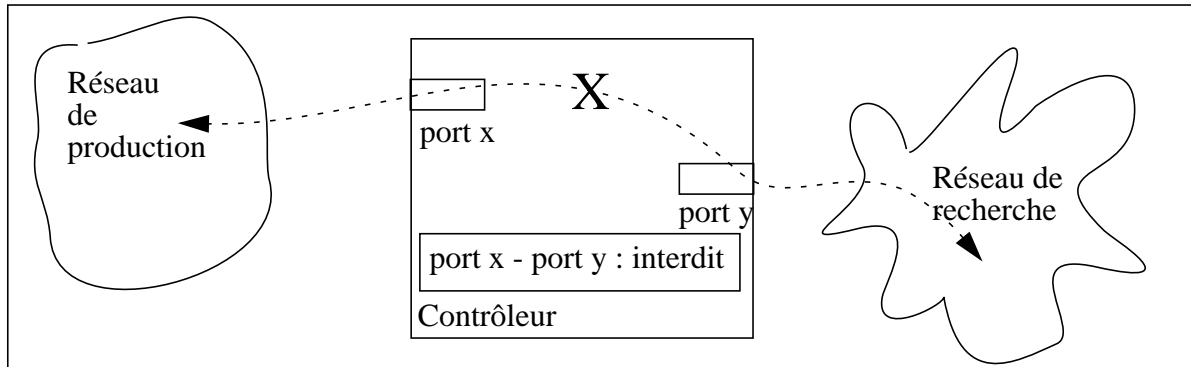
Eléments d'information

AALP: ATM Adaptation Layer Parameters.
 AAP: ABR Additional Parameters.
 AATD: Alternative Atm Traffic Descriptor.
 ASP: ABR Setup Parameters.
 ATD: ATM Traffic Descriptor.
 BBC: Broadband Bearer Capability.
 BHLI: Broadband High Layer Information.
 BLLI: Broadband Low Layer Information.
 BLS: Broadband Locking Shift.
 BRI: Broadband Repeat Indicator.
 BSC: Broadband Sending Complete.
 BTR: Broadband Type Report.
 C: Cause.

EQoSP: Extended QoS Parameters.
 ER: Endpoint Reference.
 ES: Endpoint State.
 ETD: End-to-End Transit Delay.
 F: Facility.
 GIT: Generic Identifier Transport.
 LIJCI: Leaf Initiated Join Call Identifier.
 LIJP: Leaf Initiated Join Parameters.
 LLCP: Link Layer Core Parameters.
 LLPP: Link Layer Protocol Parameters.
 LSN: Leaf Sequence Number.
 MATD: Minimum Acceptable Traffic Descriptor.
 NBC: Narrowband Bearer Capability.

les communications entre certains ports. La figure 7 montre un exemple où l'on interdit les trafics entre un réseau de recherche et un réseau de production dans une même entreprise au moyen de cette information.

Figure 7 : Contrôle d'accès par les informations de commutation



5 Conclusion

Nous avons analysé chapitre 3 en vue d'un contrôle d'accès les informations pouvant être obtenues par une analyse des flux produits par le modèle ATM. Dans le chapitre 4 nous avons analysé les informations pouvant être obtenues au travers des MIBs.

Afin de juger de la complétude des informations fournies par les MIBs, nous pouvons comparer les informations trouvées aux chapitres 3 et 4. Le tableau 2 synthétise les résultats obtenus.

Tableau 2 : Comparaison des informations de contrôle d'accès fournies par les deux méthodes.

Type d'information	Sous Type	Flux	MIBs
Type de flux		X	O
Identificateurs de connexion		X	X
Identificateurs d'équipements extrémité	Adresses	X	X
	Sous adresses	X	O
	Identificateurs d'extrémité	X	O
	Identificateur d'équipement extrémité	X	O
	Périmètre de validité	X	X
Information sur les flux	Couches adjacentes	X	x
	Applications	O	O
	Type d'AAL	X	X
	PCR, SCR, MBS, MCR	X	X

Information sur les flux

- atmTrafficDescrType, atmTrafficDescrParam[1-5], atmTrafficQoSClass, atmVccAalType (ATM-MIB), atmf[Vpc|Vcc][[Receive|Transmit][Type|TrafficDescriptorParam[1-5]|QoS-Class]][QoSCategory|BestEffortIndicator|ServiceCategory]], atmf[Vpc|Vcc]AbrTransmit[Icr|Nrm|Trm|Cdf|Rif|Rdf|Adtf|Crm] (ATM-FORUM-MIB), atmStatsSClass, atmHostSClass, atmMatrixSDSClass, atmMatrixDSSClass. Ces objets décrivent le type de trafic et la qualité de service associés à une connexion.
- atmVccAal5EncapsType. Cet objet décrit le type de protocole utilisé au dessus de l'AAL5.

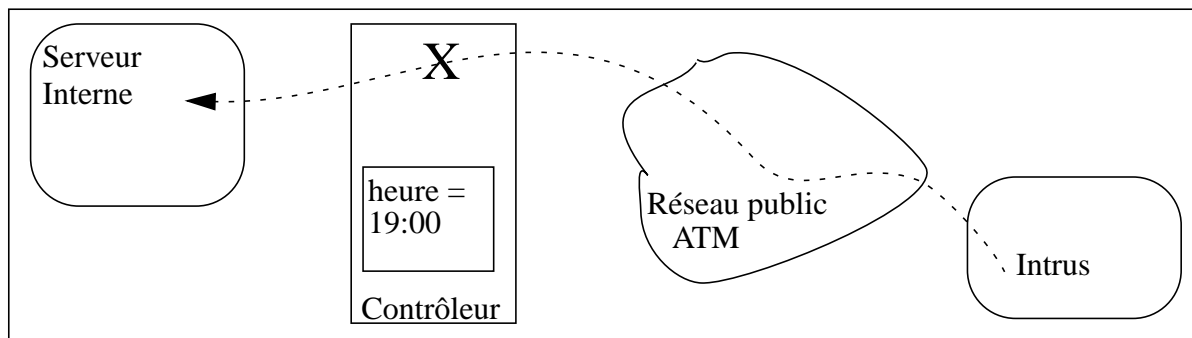
On peut également trouver, au niveau des informations de gestion, des informations plus synthétiques sur les connexions que celles pouvant être fournies par une analyse des flux.

Informations horaires

- atmVplLastChange, atmVclLastChange (ATM-MIB). Ces deux objets indiquent la date de création de la connexion.

Cette information peut être utilisée afin de restreindre l'accès à certains équipements à des horaires particuliers. La figure 6 montre comment ils peuvent être utilisés. Dans cet exemple, l'accès au serveur interne est interdit après 19 heures.

Figure 6 : Contrôle d'accès par information horaire.



- atmStatConnTime, atmHostInconnTime, atmHostOutconnTime, atmMatrixSDConnTime, atmMatrixDSConnTime (ATM-FORUM-MIB). Ces objets décrivent les durées des connexions.

Ils peuvent être utilisés pour faire du contrôle d'accès limitant la durée des connexions, soit pour des raisons budgétaires (afin de limiter le coût des communications), soit pour des raisons de sécurité (afin de limiter les risques d'intrusion).

Tables de brassage/commutation

- atmVpCrossConnect[LowIfIndex|LowVpi|HighIfIndex|HighVpi], atmVcCrossConnect[LowIfIndex|LowVpi|LowVci|HighIfIndex|HighVpi|HighVci]. Ces objets décrivent respectivement la table de brassage et la table de commutation de l'équipement si celui-ci est en mesure de fournir ces services.

Les informations fournies par ces tables peuvent servir à faire du contrôle d'accès en limitant

La station d'administration assure l'interface entre les informations de gestion et le gestionnaire du réseau. Pour cela, elle dispose d'une interface permettant de récupérer ou de fixer les informations de gestion auprès des agents. Elle possède aussi généralement un ensemble de logiciels permettant d'analyser les données recueillies. Ces données sont conservées dans une base de donnée propre à la station (MIB).

L'agent d'administration est l'autre élément actif du système de gestion. L'agent d'administration gère un ensemble d'objets au travers d'une représentation logique de ceux-ci. Cette représentation logique est codée au moyen d'une structure de gestion des informations (SMI) dans une base de donnée de gestion (MIB). Au travers de cette représentation logique, l'agent peut configurer ou surveiller les équipements qui lui sont rattachés. L'agent peut également fournir des informations à la station d'administration de manière asynchrone.

Ces deux éléments sont reliés au moyen d'un protocole d'administration. Le protocole utilisé est SNMP.

L'IETF et l'ATM-Forum ont spécifié un nombre de MIBs assez important. Celles-ci couvrent tous les domaines de normalisation:

- PNNI, émulation de LAN, CES, FUNI, ILMI, RMON, IMA, VTOA pour l'ATM-Forum.
- ATM et Classical IP over ATM (IPOA) pour l'IETF.

Parmi ces MIBs nous ne nous intéresserons qu'à celles qui se situent au niveau des couches analysées chapitre 3, c'est à dire les MIBs ILMI, RMON et ATM (ATM-FORUM-MIB, ATM-FORUM-ADDR-REG, ATM-FORUM-SRVC-REG, ATM-RMON-MIB, ATM-MIB). Le lecteur intéressé par une analyse des autres MIBs pourra se reporter à [Pa098].

On peut retrouver au niveau des informations de gestion une partie des informations pouvant être fournies par une analyse des flux. L'utilisation de ces informations se fait de la même manière que celles trouvées par l'analyse des flux.

Identificateurs de connexion

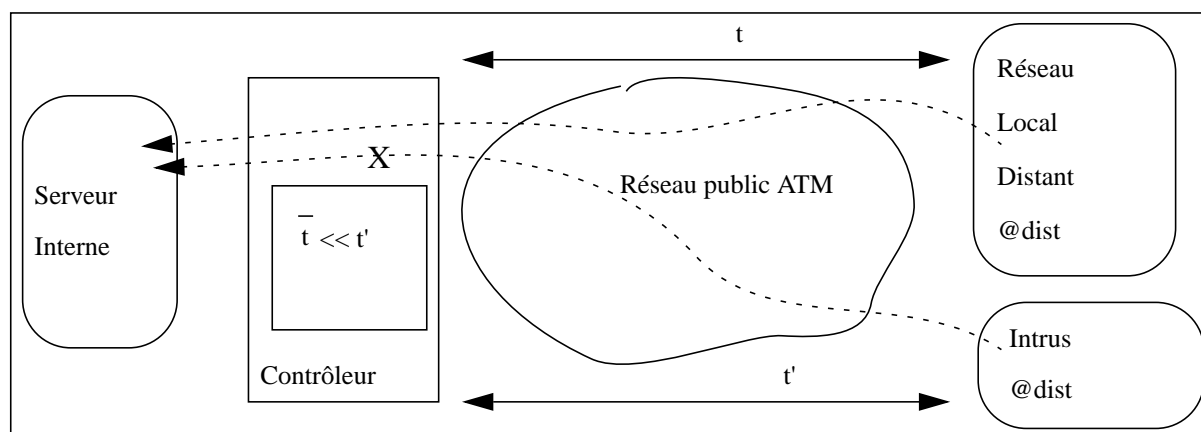
- atmVplVpi, atmVclVpi, atmVclVci (ATM-MIB), atmfVpcVpi, atmfVpcArbVpi, atmfVccVpi, atmfVccVci, atmfVccAbrVpi, atmfVccAbrVci (ATM-FORUM-MIB). Ces objets décrivent les identificateurs de connexion. Ces connexions peuvent être destinées à l'équipement local ou à un autre équipement (lorsque la MIB est sur un équipement fournissant des services de commutation ou de brassage).

Identificateurs d'équipements d'extrémité

- atmfAddressAtmAddress, atmfAddressOrgScope, atmfAddressPort (ATM-FORUM-MIB), atmMatrixSDSrcAddress, atmMatrixSDDstAddress, atmMatrixDSSrcAddress, atmMatrixDSDstAddress (RMON-MIB). Ces objets décrivent des adresses. Dans le premier cas, il s'agit des adresses connectées au port d'un équipement de commutation ou de brassage ATM. Il est possible de faire le lien entre adresses et connexions au moyen du numéro de port. Dans le second cas, les connexions ne sont pas distinguées ; la seule connaissance est qu'il existe au moins une connexion entre les équipements identifiés par ces adresses.

Il faut noter que ces objets ne peuvent servir à faire du contrôle d'accès que si les deux équipements sont dans un même espace d'administration.

Figure 5 : Détection d'usurpation d'adresse



4 Informations provenant de l'analyse des MIBs

L'idée d'utiliser des données de gestion afin de rendre des services de sécurité n'est pas nouvelle. L'utilisation la plus courante de ces informations est la fourniture du service de détection d'intrusion. Ainsi [TIB95] présente une utilisation des valeurs fournies par les données de base spécifiées par l'IETF permettant de repérer des intrusions. [AD97] propose une adaptation du système de description des objets afin d'y introduire des notions temporelles, celles-ci permettant de rendre des services de détection d'intrusion. [Darpa97] présente l'intégration d'un système de détection d'intrusion avec le système de gestion spécifié par l'IETF. Les bases de données des systèmes de gestion ont également été utilisées afin de rendre des services de distribution d'éléments cryptographiques, d'audit [SECM98], de gestion du contrôle d'accès [Kar98] et de contrôle d'accès [SKM97].

Dans cette partie nous nous intéressons aux informations de gestion dans un objectif de contrôle d'accès. Pour cela nous recherchons dans ces informations les données pouvant être utilisées afin de réaliser un contrôle d'accès.

Nous considérons les informations qui ont été spécifiées afin de gérer les équipements ATM dans le cas de réseaux privés. Trois organismes ont établi des spécifications à ce sujet. Bien que les trois proposent des spécifications pouvant s'appliquer à la fois aux réseaux publics et privés, il est vraisemblable que seules les spécifications édictées par l'ATM-Forum et l'IETF seront appliquées au cadre des réseaux privés, les spécifications de l'ITU s'appliquant, elles, aux réseaux publics.

En ce qui concerne la gestion des réseaux privés, les modèles proposés par les deux organismes sont assez proches.

Les concepts principaux de ces deux modèles sont les suivants:

- Station d'administration.
- Agent d'administration.
- Base de donnée de gestion.
- Protocole d'administration.

Tableau 1 : Relations entre applications et classes de trafic.

Application/Type de trafic	CBR	rt-VBR	nrt-VBR	ABR	UBR
Interconnexion de LAN			x	X	x
Transport de données			x	X	x
Emulation de circuit (PABX)	X	x			
Vidéo conférence RNIS-BE	X				
Données audio compressées		X	x	x	
Video	X	x			
Multimedia interactif	X	X	x	x	
Données critiques	x		X		

Note 1: X Adéquation optimale, x Bonne adéquation.

Note 2: Relations entre AAL et classes de trafic:

CBR: AAL1, rt-VBR: AAL2, nrt-VBR ABR UBR: AAL3/4 AAL5.

Ces informations peuvent être utilisées pour obtenir des renseignements complémentaires sur les services utilisés. Comme le montre le tableau 1, il existe un lien entre applications et classes de service.

Cette relation peut être renforcée en utilisant les valeurs des contrats de trafic. Cependant comme ce lien n'est pas obligatoire, un intrus peut par exemple demander une connexion FTP sur AAL1 avec des paramètres de contrat de trafic correspondant à une connexion vidéo.

- GIT : Informations sur les équipements d'extrémité. Celles-ci fournissent des renseignements sur les capacités multimedia des équipements d'extrémité [H245].

Cette information peut être utilisée pour restreindre les possibilités de types de flux pouvant être échangés entre deux équipements en se basant sur leurs capacités communes.

Informations diverses

- TNS : Réseaux de transit. Cette information spécifie les réseaux traversés au cours d'une demande de connexion.

Cette information peut être utilisée d'une part pour vérifier qu'une demande de connexion ne traverse pas un réseau «sensible» du point de vue de la sécurité et d'autre part pour vérifier que la liste des réseaux traversés est compatible avec l'origine de l'appel.

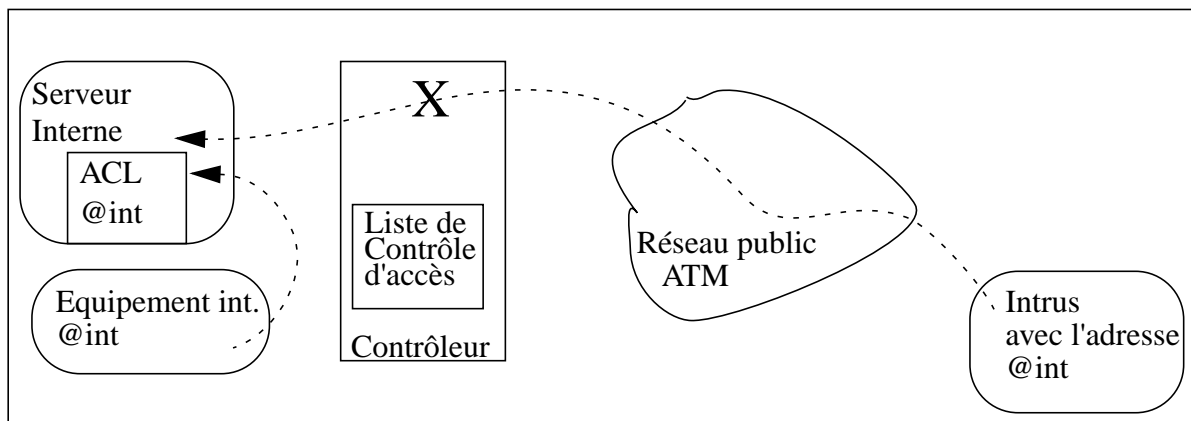
- ETD : Délai de transit. Cette information décrit le temps mis par un message de signalisation pour traverser le réseau entre les équipements d'extrémité.

La figure 5 fournit un exemple où le délai de transit est utilisé pour détecter une usurpation d'adresse. Celle-ci étant réalisée afin d'obtenir un accès privilégié à un serveur interne. Dans cet exemple le délai de transit à l'ouverture de connexion (t') est comparé avec le délai de transit moyen (\bar{t}) entre le contrôleur et l'entité distante. Si t' est significativement différent de \bar{t} , la demande de connexion est interrompue.

- CS: Périmètre de validité. Cette information est utilisée pour calculer la valeur des adresses de groupe.

Ces informations peuvent être utilisées afin de faire du contrôle d'accès sur les adresses. Il est par exemple possible d'utiliser ces identificateurs pour protéger un réseau privé d'éventuelles usurpations d'identité en provenance d'un réseau public. La figure 4 présente un exemple dans lequel un serveur fournit des services particuliers à des équipements internes à un réseau privé en se basant sur leurs adresses. Un intrus tente d'accéder au serveur interne en prenant l'adresse d'un équipement interne @int. Cette tentative d'accès non autorisée est interceptée par le contrôleur qui remarque une demande de connexion avec une adresse interne provenant de l'extérieur.

Figure 4 : Détection d'usurpation d'adresse



Information sur les flux

- BLLI, NLLC : Informations sur les couches adjacentes. Ces informations décrivent les protocoles au moyen d'identificateurs ISO ou SNAP [X263], les tailles de trames et de paquets, les tailles de fenêtres et les capacités de multiplexage.

Ces informations peuvent servir à restreindre l'accès à certains types de réseaux.

- BHLI, NHLI : Informations sur les applications. Ces informations en cours de normalisation décrivent les applications utilisées au dessus de la couche AAL de la même manière que les numéros de protocoles et de ports dans les réseaux IP.

Ces informations, lorsqu'elles seront normalisées, pourront être utilisées pour faire du contrôle d'accès par application.

- AALP, ATD, AATD, MATD, QoSP, BBC, ASP, EQoSP, AAP, LLCP, LLPP : Descripteurs de trafic. Les descripteurs de trafic donnent des informations sur le type d'AAL utilisé et les paramètres du contrat de trafic (PCR, SCR, MCR, MBS, FD, BEI, ICR, NRM, TRM, CDF, RIF, RDF, ADTF, CRM, CDV, CLR). Ces paramètres varient suivant le contrat de trafic (CBR, rt-VBR, nrt-VBR, ABR, UBR).

3.2 La couche AAL

Le but de la couche AAL est d'adapter le trafic ATM aux applications. Plusieurs types d'AAL ont été définis dans ce but, chacun correspondant à un type d'application particulier. Chaque AAL contenant des mécanismes qui lui sont propres, il en résulte des AAL-PDUs de structures différentes.

La structure de ces PDUs fournit donc une indication sur le type d'application utilisée au-dessus de la couche AAL. Cependant cette information est moins précise que celle pouvant être obtenue au moyen de la signalisation (cf chapitre 3.3).

Néanmoins dans le cas où la signalisation n'est pas utilisée (c'est à dire dans le cas des connexions permanentes), cette information peut être utilisée afin d'interdire l'utilisation de certaines applications reposant sur un type d'AAL particulier.

3.3 La signalisation

La partie signalisation est située dans le plan de contrôle du modèle ATM et dans la couche application au-dessus du modèle. Nous avons déjà présenté les caractéristiques de la signalisation au niveau de la couche ATM dans le chapitre 3.1. La couche AAL relative à la signalisation fournit une interface à une entité de signalisation appelée Q93B située dans la couche application. L'entité Q93B est responsable de la construction de messages de signalisation. Ces messages sont utilisés pour établir, contrôler et fermer les connexions ATM.

Dans cette section nous analysons les informations relatives au contrôle d'accès fournies par les messages de signalisation. Ces messages ont été spécifiés par deux organismes:

- L'ATM-Forum au travers de l'UNI4.0 [UNI40].
- L'ITU-T au travers de la série Q de recommandations (Q2931, Q2932, Q2933, Q2951, Q2959, Q2961, Q2962, Q2963, Q2971).

Bien que ces deux normes soient proches, il existe des différences mineures au niveau de la spécification des messages et de leur composition.

Les messages sont structurés au moyen d'une unité d'information appelée IE (Elément d'Information). Chaque IE traite d'un seul sujet. Plusieurs IEs peuvent néanmoins traiter du même sujet.

Tous les éléments d'information n'ont pas la même utilité en terme de contrôle d'accès. En effet certains messages ne sont échangés qu'entre deux éléments adjacents du réseau. Les IEs propres à ces messages n'ont donc qu'une signification locale. Cette analyse nous a conduits à sélectionner un ensemble d'IEs ayant une signification globale, c'est à dire apportant des informations sur les équipements terminaux faisant partie d'une connexion. Afin d'analyser les IEs nous grouperons ceux-ci en catégories. Tous les IEs sont présentés sous une forme abrégée dont la signification est donnée en annexe.

Identificateurs d'équipements extrémité

- CPN, cPN, CPSA, cPSA: Adresses et sous adresses des équipements appelant et appelé.
- CN, CSA: Adresses et sous adresses connectées. Ces informations peuvent différer des précédentes lorsqu'un service tel que la redirection d'appel est utilisé.
- ER,LIJCI: Identificateurs d'extrémité. Ces informations identifient un équipement d'extrémité dans le cas de connexions point à multipoint.
- CI: Identificateur d'équipement d'extrémité. Cette information permet de distinguer des équipements utilisant la même adresse ATM et la même pile de signalisation.

3 Informations provenant de l'analyse des flux

Dans cette partie, nous analysons le modèle ATM de manière systématique afin d'y trouver les informations pouvant être utilisées pour fournir ou améliorer le contrôle d'accès. Nous jugerons de l'utilité des informations recueillies par analogie avec les informations utilisées pour réaliser le contrôle d'accès dans les réseaux actuels. Afin d'analyser le modèle nous suivrons la structure présentée figure 1 à savoir la couche ATM, la couche AAL et la signalisation, celle-ci étant à la fois dans le plan de contrôle du modèle et dans la couche application.

La couche la plus basse du modèle ATM est la couche physique. Le but de cette couche est d'adapter le flux ATM à un type particulier de support physique. Nous ne nous intéresserons pas à cette couche car elle ne transporte pas d'informations de bout en bout. Une analyse des informations fournies par cette couche ne peut donc pas donner de renseignements sur les entités extrémité.

3.1 La couche ATM

Toutes les informations fournies dans ce chapitre proviennent des spécifications UNI3.1 [UNI31] de l'ATM-Forum qui sont les plus récentes dans ce domaine.

Les PDUs échangés par les entités ATM sont appelés cellules et peuvent être décomposés en deux parties : une partie de contrôle et une partie utilisateur.

La partie de contrôle

La partie de contrôle a une taille de 5 octets. Elle contient :

- Le type de flux. Celui-ci est codé au moyen d'une combinaison de bits. Cette information peut être utilisée pour distinguer certains flux. Il peut ainsi être intéressant de bloquer les flux de signalisation en dehors des heures de travail afin d'empêcher des connexions dynamiques de s'établir.
- Les champs VPI/VCI qui sont utilisés pour identifier une connexion. Cette information peut être utilisée en association avec d'autres renseignements tels que la date, l'heure ou des informations administratives. Ainsi, dans le cas de connexions permanentes, il est possible d'associer une connexion à un service. Dans ce cas, les champs VPI/VCI peuvent être utilisés pour interdire l'accès au service pendant des périodes de temps particulières.

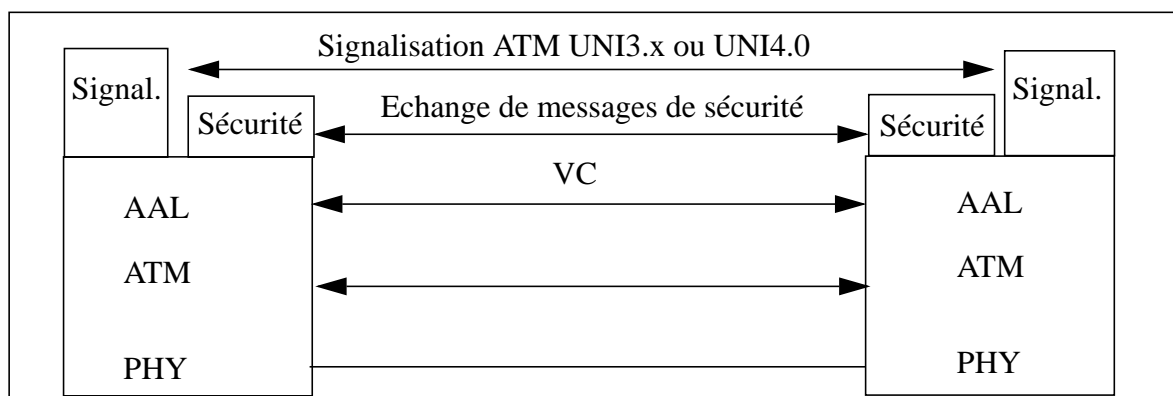
La partie utilisateur

Au niveau du plan utilisateur et du plan de contrôle, aucune information sur la structure des données échangées n'est fournie par les spécifications au niveau ATM.

En ce qui concerne le plan de gestion, on peut distinguer trois types de flux produits au niveau ATM :

- ILMI. Ce flux n'est pas très intéressant car il n'existe qu'entre deux équipements physiquement adjacents. Il est utilisé pour la gestion et la configuration automatique des équipements.
- Les flux F4 et F5. Ces deux flux ont une structure similaire. En ce qui concerne le contrôle d'accès, deux champs (OAM type, fonction type) peuvent être utilisés afin d'affiner le contrôle d'accès réalisé au moyen des informations provenant de la partie de contrôle qui précisent le type et la fonction des flux de gestion.

Figure 3 : Placement des mécanismes de contrôle d'accès dans le plan utilisateur.



Le placement dépend du réseau utilisé et de sa capacité à supporter une signalisation sécurisée. De manière pratique, ce contrôle d'accès pourrait s'effectuer :

- Soit au niveau des équipements extrémité.
- Soit au niveau d'équipements spécialisés.

Bien que le service de contrôle d'accès spécifié par l'ATM-Forum soit intéressant par sa généralité, il possède néanmoins un certain nombre de défauts :

- L'utilisation d'étiquettes de sensibilité suppose l'utilisation d'équipements (équipements de commutation mais également équipements terminaux) capables d'interpréter ces étiquettes. Ce n'est pas le cas de la majorité des équipements actuels. Les équipements ne supportant pas les étiquettes de sensibilité devront utiliser des passerelles.
- Les spécifications ne prennent pas en compte que des données de niveaux de sensibilité différents peuvent être échangées sur une même connexion.
- Le service de contrôle d'accès dans son sens traditionnel (c'est à dire de la manière dont il est réalisé dans les réseaux TCP/IP ou X25, en utilisant les informations présentes dans les flux échangés afin de contrôler l'accès aux services) est volontairement laissé en dehors du champ de normalisation.

Ces défauts ont été perçus au niveau des constructeurs de matériel qui proposent certaines solutions destinées à traiter le troisième point. En particulier [BE98] montre comment réaliser du contrôle d'accès à partir d'équipements ATM standards (Cisco LS 1010). Le contrôle d'accès offert par ce type d'équipement est du même type que celui offert par les routeurs filtrants dans le monde IP mais ne tient compte au niveau ATM que des informations d'adressage. Les seules informations aujourd'hui utilisées étant les informations d'adressage, il est clair qu'il existe un gros potentiel de progression dans la finesse du contrôle d'accès vis à vis de celui qui peut être implémenté aujourd'hui.

Comme nous l'avons montré précédemment, que l'on désire rendre le service de contrôle d'accès en utilisant les spécifications de l'ATM-Forum ou en utilisant des mécanismes semblables à ceux utilisés dans les réseaux actuels, il est nécessaire d'analyser les informations disponibles sur les connexions ATM, que cela soit pour construire des étiquettes de sensibilité ou pour filtrer les données directement.

Le moyen le plus utilisé pour obtenir des informations sur une connexion est l'analyse de flux.

Le contrôle d'accès pour les réseaux ATM spécifié par l'ATM-Forum dans [SEC98] est de type «label based», il se base sur une classification des données échangées afin de réaliser le contrôle d'accès. Cette classification se fait d'une manière analogue à celle qui est effectuée dans les systèmes classés B et A selon le classement de l'orange-book [TCSEC83]. Elle est effectuée au moyen d'un paramètre appelé niveau de sensibilité. Ce paramètre est défini au moyen de deux composantes :

- Une structure hiérarchique (par exemple : non classifié, confidentiel, secret, très secret ...).
- Un ensemble de catégories d'accès (par exemple : recherche, production, administratif ...).

La classification des données se fait au moyen de deux relations d'ordre :

- Une relation d'ordre total portant sur la structure hiérarchique.
- Une relation d'ordre partiel portant sur l'ensemble des catégories d'accès.

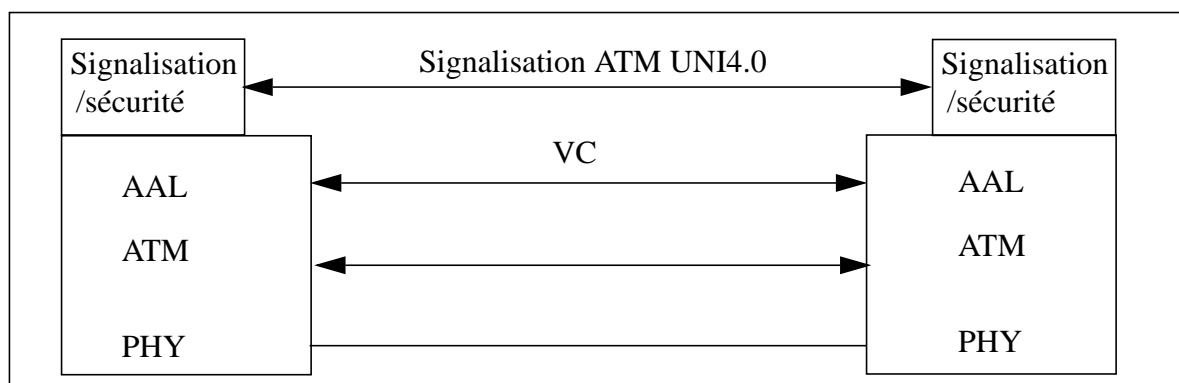
Le test de contrôle d'accès se fait en comparant les composantes du niveau de sensibilité cible avec les composantes d'un niveau de sensibilité repère au moyen des deux relations d'ordre.

En pratique, à chaque donnée est associée une étiquette de sensibilité représentant le niveau de sensibilité des données. La norme choisie pour la représentation des étiquettes de sensibilité est spécifiée par [FIPS188].

L'ATM-Forum propose de spécifier le niveau de sensibilité des données échangées au moment de l'ouverture de connexion, ce niveau devant être constant pendant toute une connexion. Pour réaliser le contrôle d'accès, il est proposé de placer les mécanismes de contrôle d'accès :

- Soit dans le plan de contrôle au niveau de l'entité de signalisation, les étiquettes de sensibilité étant placées dans le flux de signalisation (cf. figure 2). Cette méthode nécessite l'utilisation d'une signalisation conforme à l'UNI 4.0.

Figure 2 : Placement des mécanismes de contrôle d'accès dans l'entité de signalisation.



- Soit dans le plan utilisateur au niveau de la couche application, les étiquettes de sensibilité étant échangées avant tout transfert de données des utilisateurs (cf. figure 3). Cette méthode peut s'appliquer à n'importe quel type de connexion (permanentes ou dynamiques) et à n'importe quel type de signalisation.

dard à partir des avancées dans ce domaine. Au niveau de l'ATM-Forum, des spécifications concernant certains services de sécurité ont été publiées en juillet 1998. Les services de sécurité pris en compte sont la confidentialité des données, l'authentification des données, l'intégrité des données ainsi qu'une certaine forme de contrôle d'accès.

Dans cet article, nous présentons d'abord dans le chapitre 2 un état de l'art sur les mécanismes et les informations utilisées aujourd'hui afin de réaliser le contrôle d'accès dans les réseaux ATM. Nous montrons en quoi le service de contrôle d'accès proposé par l'ATM-Forum est différent du service de contrôle d'accès généralement implémenté dans les réseaux traditionnels (IP, X25) et nous décrivons également les travaux qui ont été menés afin de rendre le service de contrôle d'accès «traditionnel».

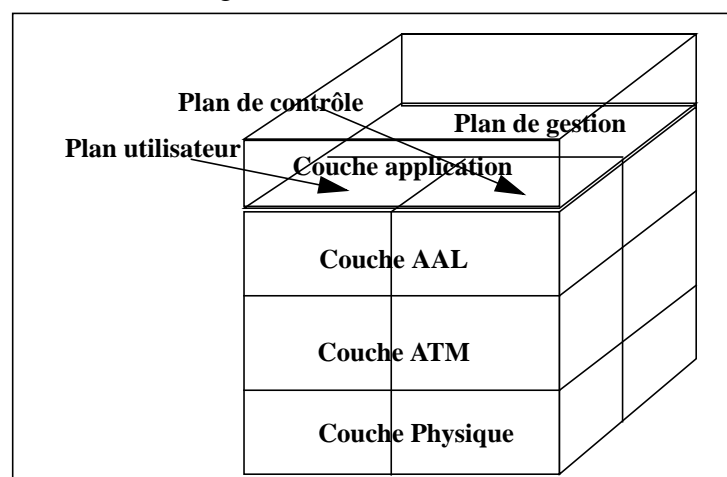
Ce service de contrôle d'accès se base généralement sur un ensemble d'informations extraites des flux échangés. Nous montrons que dans le cas de l'ATM ces informations peuvent être obtenues par la méthode classique d'analyse des flux mais également au travers des informations de gestion fournies par les MIBs. Nous exposons chapitres 3 et 4 les informations sur lesquelles peut se baser le contrôle d'accès et montrons comment ces informations peuvent être utilisées.

En conclusion nous étudions la complétude de la méthode basée sur l'analyse des informations de gestion afin de juger de sa viabilité et montrons qu'elle peut constituer une alternative intéressante.

2 Le contrôle d'accès dans l'ATM

Avant de présenter les travaux concernant le contrôle d'accès dans l'ATM, nous présentons rapidement le modèle ATM. Comme le montre la figure 1, le modèle ATM peut être divisé en trois couches (couches physiques, ATM et AAL) et en trois plans (plans utilisateur, de contrôle et de gestion).

Figure 1 : Le modèle ATM.



Où trouver les informations de contrôle d'accès dans le cas des réseaux ATM ?

Olivier PAUL^{}, Maryline LAURENT*

ENST de Bretagne

rue de la châtaigneraie - BP 78

35512 CESSON Cedex - France

Email: {paul/mlaurent}@rennes.enst-bretagne.fr

Résumé

Cet article s'intéresse aux moyens de récupérer des informations de contrôle d'accès dans le cas des réseaux ATM. Le but étant de protéger des sites ATM par filtrage des appels. Pour cela, nous présentons deux approches pouvant être complémentaires ou concurrentes. La première se base sur la méthode classique d'analyse des flux. La seconde utilise les informations fournies par les bases de données de gestion (MIBs). Nous montrons que la seconde méthode présente une alternative intéressante en terme de complétude de l'information obtenue.

Mots clef

Contrôle d'accès, Réseaux ATM, Analyse de flux, MIBs, Sécurité des réseaux.

Abstract

This paper presents various means to get access-control information in ATM networks. Two approaches are described that can be used together or alone. The first method uses the classical flows analysis mechanism. The second approach is based on the information provided by the Management Information Bases (MIBs). As a conclusion we show that the second method is a more complete alternative solution.

Keywords

Access Control, ATM Networks, Flow Analysis, MIBs, Network security.

1 Introduction

Le développement de services de sécurité pour les réseaux ATM (Asynchronous Transfer Mode) est un sujet qui a engendré beaucoup de travaux depuis quelques années. Des groupes de travail ont été formés au sein des organismes de normalisation dans le but de créer un stan-

*. Ce travail est financé par une bourse DRET