Un guide d'aide à la conception de solutions de protection des communications sur les réseaux[1]

Maryline Laurent[2]
Télécom Bretagne
rue de la châtaigneraie - BP 78
35512 CESSON Cedex - France
Téléphone : 33.2.99.12.70.20, Télécopie : 33.2.99.12.70.30
E-mail : Maryline.Laurent@rennes.enst-bretagne.fr

1. Dans les actes de 1997 du Congrès «De Nouvelles Architectures pour les Communications» (DNAC'97); .Paris.
2. Ce travail est financé par la DRET

RESUME :

Cet article montre que pour protéger les communications sur une technologie de réseau donnée et y intégrer des services de sécurité, de nombreux facteurs sont à prendre en compte : les caractéristiques de la technologie considérée mais aussi les objectifs attendus de la solution de sécurité et les contraintes de développement.

Cet article propose un guide qui aide à concevoir des solutions de sécurité pour tout type d'environnements réseau. Il met en évidence quatre critères qui permettent, en fonction des objectifs et des contraintes fixés par la solution, d'identifier les différentes options de placement des services de sécurité au sein de la technologie réseau considérée. A titre illustratif, deux exemples de solutions de sécurité développées dans un environnement ATM par deux groupes de travail sont analysés. Il en ressort qu'à l'aide du guide, il est possible de retrouver les choix de placement des services de sécurité sélectionnés par les solutions de sécurité existantes.

Mots-clés : sécurité des réseaux, services de sécurité.

ABSTRACT :

As described in this paper, several factors need to be considered to protect communications over any given network technology and to introduce security services : the technology characteristics, but also the expected security solution objectives and development constraints.

This paper proposes a guide helping designing security solutions over any kind of network environments. The guide identifies four criteria allowing to determine the possible places where the security services should be introduced within the considered network technology depending on the solution's objectives and constraints. Two illustrative security solution examples developped by two working groups in the ATM environment are considered. They show that with the guide's help, it is possible to obtain the same security services placement choices as these obtained by the existing security solutions.

Keywords : network security, security services.

1. Introduction

Il est rare que les problèmes de sécurité soient pris en compte lors de la phase de conception d'un protocole réseau. Pour assurer la protection des communications sur de tels réseaux, il est donc bien souvent nécessaire d'introduire après coup des services de sécurité [11] dans les piles de protocoles réseau existantes.

De nombreuses solutions de sécurité ont ainsi été spécifiées. Très peu sont normalisées (TLSP, NLSP, IEEE 802.10). La plupart ont été développées à titre expérimental (SMDS, RNIS bande étroite, ATM) ou bien comme solutions propriétaires (X25) pour permettre aux opérateurs de protéger leur réseau en exploitation.

Face au besoin croissant de sécurité dans les réseaux et afin de faciliter l'élaboration de nouvelles solutions de sécurité, il s'avère intéressant de répertorier les différents facteurs mis en jeu lors de la conception d'une solution de sécurité, c.à.d. lors de l'introduction de services de sécurité dans la pile de protocoles réseau correspondante. Cet article présente ces facteurs et décrit en particulier un guide d'aide à la conception de solutions de sécurité.

Plus précisément, cet article s'interroge, à la section 2, sur la possibilité de réutiliser les normes de sécurité actuelles pour développer de nouvelles solutions de sécurité. Il présente à la section 3 un guide à suivre pour concevoir une solution de sécurité. A la section 4, il prend l'exemple du réseau ATM (*Asynchronous Transfer Mode*) et montre que les solutions de sécurité ATM conçues par différents groupes de travail (l'ATM Forum en particulier) peuvent être obtenues par l'application du guide de la section 3 en tenant compte de leurs objectifs et contraintes fixés. Enfin il résume à la section 5 les différents résultats obtenus.

La suite de cet article fait référence aux services de sécurité suivants :

- **la confidentialité** permet, grâce à des mécanismes de chiffrement, de protéger les données émises sur le réseau de telle sorte qu'elles ne soient compréhensibles que par les entités du réseau autorisées.
- **l'authentification** garantit à une entité que les données reçues proviennent de l'entité déclarée. En général, ce service consiste à adjoindre aux données émises une **signature digitale** calculée sur ces données à l'aide d'un algorithme de chiffrement et d'une **clé** cryptographique secrète.

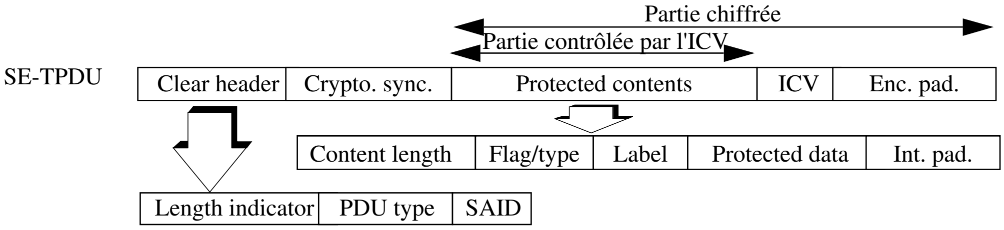

Figure 1 : La construction des TLSP PDUs de la norme TLSP

Lorsque le service de confidentialité est appliqué aux champs indiquant la source et la destination des données, ce service est appelé **anonymat**. Ce service permet de cacher l'identité (nom, adresse, etc.) des interlocuteurs vis à vis d'un observateur.

- **l'intégrité** garantit à une entité que les données reçues n'ont subi aucune modification au cours de leur transfert. Il fait lui aussi appel à des mécanismes de signatures digitales en général.
- **le contrôle d'accès** permet de restreindre l'accès aux ressources d'un système - comme par exemple l'accès aux informations détenues sur une station - aux seules entités autorisées.
- **la négociation des services de sécurité** n'est pas un service de sécurité, mais elle permet à deux entités en communication de convenir de l'ensemble des services de sécurité à mettre en place avec des précisions sur les clés cryptographiques, les algorithmes de chiffrement, etc. à utiliser.

2. Les normes de sécurité

Pour développer rapidement une solution de sécurité dans un environnement de réseau donné, une solution simple consisterait à reprendre et à adapter à un environnement réseau particulier les normes de sécurité existantes [4] comme TLSP (*Transport Layer Security Protocol*) [10] ou NLSP (*Network Layer Security Protocol*) [9] définies par l'OSI ou encore l'IEEE 802.10 [6,7]. Cependant, comme le montrent les sous-sections suivantes, ces normes répondent toutes à un problème de sécurité bien précis et sont difficilement réexploitables dans la plupart des cas.

2.1. Les normes TLSP et NLSP

La norme TLSP (resp. NLSP) définit un protocole qui permet de protéger les échanges entre les couches transport (resp. réseau) du modèle OSI. La norme TLSP (resp. NLSP) définit un protocole de sécurité à intégrer dans les couches transport (resp. réseau) de ce modèle. Ces deux normes se déclinent en deux modes suivant qu'elles fonctionnent en mode connecté ou en mode sans connexion.

Avant de réaliser des échanges de données utilisateur protégés, les deux homologues de sécurité distants (TLSP ou NLSP) doivent convenir d'une association de sécurité commune, c'est à dire des services de sécurité à mettre en place, de la façon de les implémenter (type d'algorithmes de chiffrement) et des paramètres de sécurité à utiliser (clés de chiffrement). Cette association de sécurité est identifiée par un numéro SAID (*Secure Association IDentifier*). Elle peut être négociée par l'échange de PDUs de sécurité (non décrits ici) identifiés par un type de PDU particulier (*Secure Association PDU*).

Une fois l'association de sécurité négociée, les deux homologues de sécurité peuvent alors échanger des données utilisateur de façon protégée en encapsulant les données utilisateur dans un PDU de sécurité de type SE-TPDU (*SEcure Transport PDU*). Comme le montre la figure 1 qui décrit les encapsulations effectuées par le protocole TLSP (similaires à celles de NLSP), les données utilisateur sont chiffrées dans le champ *Protected data* avec l'association de sécurité indiquée dans *SAID* et, éventuellement, avec des informations de synchronisation spécifiées dans le champ *Crypto sync*. Suivant l'algorithme de chiffrement choisi, il peut s'avérer nécessaire d'aligner les données à chiffrer sur une certaine longueur. Dans ce cas, des bits de bourrage sont introduits dans le champ *Encrypted pad*ding.

Pour protéger en intégrité les données utilisateur et permettre au récepteur du SE-TPDU de s'assurer de l'identité de l'émetteur, il est nécessaire d'ajouter, dans le champ *ICV*, une signature digitale (calculée sur une partie du SE-TPDU) et, suivant l'algorithme de génération de signature choisi, d'introduire des bits de bourrage dans le champ *Integrity padding*.

Les normes TLSP et NLSP sont très liées aux couches du modèle OSI et souffrent de deux inconvénients majeurs qui les rendent quasiment inapplicables à des environnements réseau classiques. D'une part, les protocoles utilisés ne sont pas transparents. C'est à dire, seuls les équipements munis de la même pile de protocoles de sécurité de type TLSP (ou NLSP) peuvent communiquer entre eux. Pour les réseaux fonctionnant en mode connecté, ce problème peut être résolu en négociant à l'ouverture de connexion la possibilité de mettre en place l'un des protocoles TLSP ou NLSP pour assurer la protection des échanges de données utilisateur. Pour les autres types de réseaux, par contre, les normes TLSP et NLSP apparaîssent difficilement exploitables.

D'autre part, par l'ajout d'entêtes, les protocoles TLSP et NLSP provoquent l'accroîssement de la taille des paquets de données à transmettre, mais ils ne se soucient pas de la taille maximale autorisée par la couche inférieure (couche réseau pour TLSP ou couche liaison de données pour NLSP). L'implantation de ces protocoles dans une pile de protocoles ré-

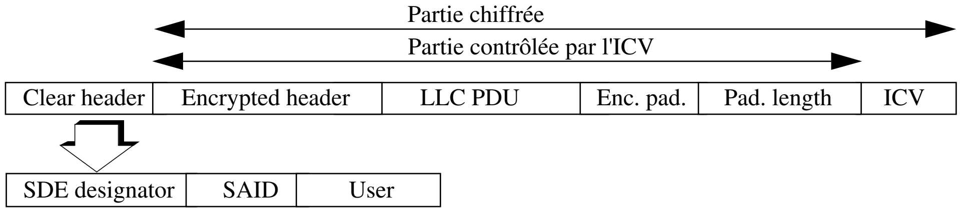

Figure 3 : La construction des SDE PDUs de la norme IEEE 802.10

seau particulière suppose donc d'intervenir en plus de la couche d'intégration du protocole de sécurité, dans certaines couches pour modifier les paramètres relatifs à la taille maximale des paquets admise. L'introduction de ces protocoles a donc un impact sur l'environnement de réseau à protéger.

2.2. La norme IEEE 802.10

La norme IEEE 802.10 [6, 7, 8] vise à assurer l'échange protégé de données sur les réseaux locaux de type IEEE 802. Elle définit pour cela une couche supplémentaire à introduire entre les couches MAC et LLC des modèles IEEE 802 (cf. figure 2). Cette couche appelée SDE [7] pour *Secure Data Exchange* encapsule les données issues de la couche LLC et les transmet à la couche MAC. Si la norme vise essentiellement à définir la couche SDE, elle définit en fait toute une architecture de sécurité [6] à intégrer au modèle IEEE 802, avec des modules de gestion de clés [8] et d'administration de la sécurité.

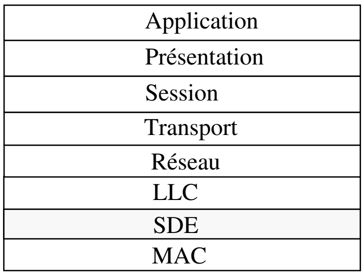

Figure 2 : Le modèle en couches IEEE 802.10 simplifié

La couche SDE effectue la double encapsulations décrite à la figure 3. Elle est proche de l'encapsulation réalisée par la norme TLSP. Elle chiffre les données utilisateur *LLC PDU* avec l'association de sécurité *SAID* précédemment négociée ainsi qu'avec d'éventuelles informations de synchronisation précisées dans le champ *User*. Le champ *Encrypted padding* avec sa longueur *Padding length* permet d'introduire les éventuels bits de bourrage utiles au calcul du chiffrement.

La couche SDE permet de protéger les données utilisateur par le biais d'un contrôle d'intégrité placé dans le champ *ICV*. Elle permet aussi d'assurer l'authentification des données en plaçant l'authentifiant de la machine émettrice dans le champ *Encrypted header*.

La couche SDE a la particularité intéressante de ne pas interdire les échanges avec des équipements ne disposant pas de couche SDE. En effet, la couche SDE définit un SDE PDU conforme, dans ses deux premiers octets, à la structure d'un LLC PDU. Le champ *SDE designator* du SDE PDU (resp. le LLC PDU) contient en effet dans ses deux premiers octets les adresses SAP (*Service Access Point*) source et destination de la couche SDE (resp. de la couche LLC). Ainsi, si un MAC SDU est reçu avec une adresse SAP de destination correspondant à une adresse SAP LLC, la couche SDE devient transparente pour ce datagramme et le MAC SDU est directement envoyé à la couche LLC.

La couche SDE apparaît donc comme une couche autonome qui est plus facilement applicable à d'autres environnements réseau que les normes TLSP et NLSP. En effet :

- elle est transparente et, suivant le type de réseau utilisé, cette propriété peut être conservée à condition que le champ *SDE designator* soit correctement adapté.
- la couche SDE résout elle-même le problème de l'extension de la taille des paquets à transmettre. Elle propose de fragmenter les paquets de telle sorte que la taille des paquets transmis à la couche inférieure ne dépasse jamais la taille maximale autorisée par cette couche. Il est clair que cette fragmentation réduit les performances du protocole, une réduction de performances qui est d'autant plus importante que la taille maximale autorisée par la couche inférieure est petite.

Du fait de ces caractéristiques, la couche SDE est reprise dans certaines solutions de sécurité pour protéger les échanges sur les réseaux ATM [12] (cf. section 4.3) ou SMDS (*Switched Multimegabit Data Service*) [3]. Cependant, elle n'est pas réutilisable telle quelle. Il est en effet nécessaire d'adapter ou de supprimer (cf. section 4.3) le champ *SDE designator* contenant les adresses SAP propres à la couche LLC du modèle IEEE 802.

3. Un guide d'aide à la conception de solutions de sécurité

Comme le montre la section 2, il est difficile de baser de nouvelles solutions de sécurité sur les normes de sécurité actuelles. En fait, il est vain de vouloir définir une solution de sécurité générique qui s'applique à l'ensemble des environnements réseau car chaque réseau a ses caractéristiques et, au delà de la technologie utilisée, les solutions de sécurité dépendent de nombreux facteurs.

Par contre, il est possible de spécifier un guide d'aide à la conception de solutions de sécurité qui aide à déterminer, en fonction des besoins et contraintes de sécurité, :

- le placement des services de sécurité dans la pile de protocoles réseau utilisée,
- la façon de réaliser ces services de sécurité au sein de la couche de protocole choisie.

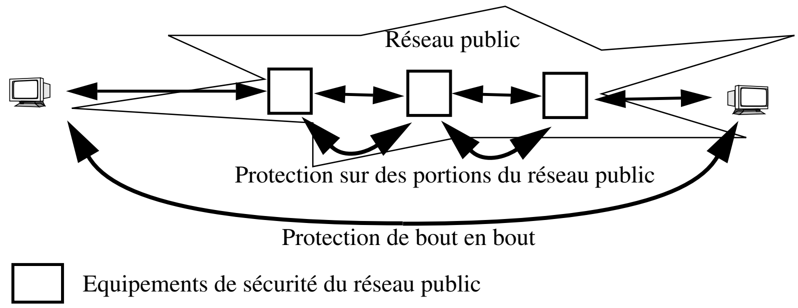

Figure 4 : Différents modes de protection : la protection de bout en bout et la protection sur des portions de réseau

Les deux sous-sections suivantes précisent, pour chacun de ces points, les différents facteurs mis en jeu et leur impact sur la solution de sécurité.

3.1. Le placement de services de sécurité dans une pile de protocoles réseau

Pour placer convenablement les services de sécurité dans une pile de protocoles réseau, deux facteurs sont à prendre en considération :

- (1) l'implication du réseau public dans la protection des communications [4]. Deux stratégies de protection des communications existent (cf. figure 4). L'une consiste, pour les utilisateurs en communication, à assurer eux-mêmes la protection de leurs communications. Dans ce cas, le réseau public n'intervient pas. Ce type de protection est appelé **protection de bout en bout**. L'autre stratégie consiste à déléguer en partie la protection d'une communication au réseau public qui doit alors assurer une **protection sur des portions de réseau**, chacune de ces portions étant comprise entre deux équipements de sécurité du réseau public.

  Une fois la stratégie adoptée, il suffit ensuite de déterminer, dans l'environnement réseau considéré, la couche en charge des opérations de routage pour obtenir la couche délimitant le placement des services de sécurité pour l'une ou l'autre des stratégies. Au-dessus de cette couche, il faudra placer les services de sécurité utiles à la protection de bout en bout, et en dessous, ceux servant à la protection sur des portions de réseau. Cette remarque est particulièrement évidente pour le service de confidentialité. Si des informations de routage sont envoyées chiffrées sur le réseau public, le premier noeud du réseau public rencontré doit nécessairement les déchiffrer pour acheminer correctement les données. Si par contre, elles sont en clair, le réseau peut directement router les données au travers du réseau, indépendamment du contenu des données (qui peut être chiffré ou pas). Ainsi, il est facile de constater que si le service de sécurité est rendu au dessous de la couche limite où s'effectue le routage, le réseau public doit nécessairement participer à la protection des communications.
- (2) les informations à protéger. Certaines informations telles que les informations de routage ou d'administration étant particulièrement sensibles, il peut s'avérer nécessaire de les protéger. Dans ce cas, des services de sécurité doivent être implémentés dans ou sous la couche traitant ces informations. Le point (2) permet d'affiner par rapport au point (1) le placement des services de sécurité dans une pile de protocoles.

Il faut également noter que bien souvent le choix du placement des services de sécurité au sein d'un modèle en couches est une affaire de compromis. En effet, plus les services de sécurité sont placés bas dans les couches, plus nombreux sont les équipements impliqués dans le traitement de la sécurité. Si les équipements sont fiables, le niveau de sécurité s'en trouve accru. En particulier, le chiffrement au niveau de la couche physique permet d'empêcher un observateur placé sur le réseau de distinguer les connexions entre elles et donc d'analyser le trafic échangé sur une connexion particulière. Par contre, il suffit qu'un équipement soit piraté pour que la confidentialité des connexions ne soit plus assurée. [15] qui traite plus particulièrement des problèmes d'intégrité des transferts de fichiers démontre que le placement du service d'intégrité dans le modèle en couches est un compromis entre le niveau de fiabilité du réseau et le coût en bande passante et en délais engendré par le placement du service d'intégrité dans les couches basses. En effet, plus le service d'intégrité est placé bas dans les couches, plus la rentabilité en terme de quantité d'informations de sécurité ajoutées (e.g. contrôle d'intégrité) comparativement à la quantité de données utiles est dégradée. D'autre part, plus ce service est placé bas, plus nombreux sont les équipements à vérifier l'intégrité des échanges. Ainsi en cas d'erreur d'intégrité, la reprise sur erreur est réalisée sur un segment du réseau d'autant plus petit que le service est placé bas. Si la ligne est particulièrement mauvaise, la perte de performances causée par le placement du service d'intégrité dans les couches basses peut être justifiée.

3.2. La réalisation des services de sécurité

Le choix de l'implémentation des services de sécurité dépend des deux facteurs suivants :

- (3) l'importance des modifications autorisées. Ce facteur consiste à remarquer que les utilisateurs ayant fait l'effort financier de s'équiper dans une technologie risquent de faire pression pour que soient rejetées toutes les modifications de cette technologie (liées à l'introduction de services de sécurité) remettant en cause la pérennité de leurs équipements. En particulier, si après la phase de normalisation d'une technologie, certaines personnes décident d'y introduire de la sécurité, il est évident que toute modification de la technologie est à proscrire. Les solutions choisies consisteront plutôt à ajouter une couche supplémentaire dédiée à la sécurité du type IEEE 802.10 (cf. section 2.2). Plusieurs solutions ont été développées suivant ce concept pour protéger les échanges sur les réseaux ATM [12] (cf. section 4.3), SMDS [3] ou pour protéger l'interconnexion de réseaux Ethernet via l'utilisation de ponts sécurisés [14].

Si, par contre, des modifications du protocole sont autorisées, la solution peut tenir compte des particularités de la technologie, éviter l'encapsulation supplémentaire due à la couche de sécurité et résulter en de meilleures performances en bande-passante et délais. Par exemple, [14] présente une solution de protection des communications sur le RNIS bande étroite qui permet à deux abonnés de s'authentifier mutuellement en début de communication téléphonique. Pour cela, il utilise les éléments d'information de la signalisation RNIS [13] existants : l'élément *High Layer Compatibility parameter* pour transporter de bout en bout l'indication qu'il s'agit d'une communication où les abonnés doivent s'authentifier et l'élément *user-user* pour transporter l'authentificateur de chaque abonné au travers du réseau.

- 4 La technologie utilisée tient aussi une part importante dans la définition de la solution de sécurité.

  Si cette technologie fonctionne en mode connecté, la signalisation utilisée pour établir la connexion peut être exploitée pour transporter des informations de sécurité et permettre la négociation de paramètres de sécurité ou une première authentification des entités en communication. Cette technique est par exemple utilisée pour protéger les communications sur le RNIS bande étroite [14].

  En mode non connecté, par contre, des trames (ou paquets) doivent être identifiées comme porteuses de paramètres de sécurité. C'est le cas pour les réseaux IPv6 qui définissent une nouvelle entête pour l'échange de clés de sécurité [2] et pour la solution de protection de l'interconnexion de réseaux Ethernet [14].

  Pour une technologie à commutation de paquets, l'élaboration de la solution de sécurité varie suivant que les paquets sont de taille variable ou fixe. S'il s'agit de paquets de taille fixe encore appelés cellules, les possibilités de réalisation de certains services de sécurité comme le service d'intégrité sont plus limitées. En effet, les services qui aboutissent à l'accroîssement de la taille des données utilisateur (suite à l'introduction d'une signature digitale par exemple), risquent de provoquer des fragmentations supplémentaires en cellules s'ils sont effectués au niveau des cellules et risquent de conduire à un coût en bande passante inacceptable. Il faut donc les placer suffisamment haut dans le modèle en couches de la technologie. Pour l'ATM, par exemple, les services d'intégrité/authentification doivent être placés dans ou au dessus de la couche AAL (i.e. avant que les trames AAL ne soient segmentées en cellules ATM). Par contre, pour les technologies à commutation de paquets (de taille variable), ce problème ne se pose pas car les contraintes à observer sur la longueur des paquets sont plus flexibles.

4. L'exemple des réseaux ATM

Cette section montre comment le guide proposé à la section 3 peut être utilisé pour développer des solutions de sécurité. Pour cela, il prend l'exemple du réseau ATM et de deux solutions de sécurité développées dans cet environnement, l'une par l'ATM Forum et l'autre par l'ENST-Bretagne. Il montre qu'à partir des objectifs et contraintes fixés pour chaque solution, il est possible en utilisant le guide de retrouver les solutions obtenues par chacun des groupes de travail.

La section 4.1 présente les notions sur la technologie ATM (*Asynchronous Transfer Mode*) utiles à la compréhension des sections ultérieures. Les sections 4.2 et 4.3 portent sur les deux exemples de solutions de sécurité ATM.

4.1. Les concepts des réseaux ATM

L'ATM est une technologie à commutation de cellules qui offre aux utilisateurs un service orienté connexion. Le modèle de référence ATM [5] comprend donc plusieurs plans (cf. figure 5) :

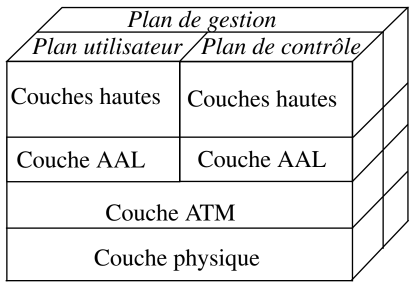

Figure 5 : Le modèle de référence ATM

- le plan utilisateur qui permet d'échanger des données utilisateur sur le réseau ATM,
- le plan de contrôle qui traite les informations de signalisation pour établir, superviser et libérer les connexions,
- le plan de gestion chargé de maintenir le réseau ATM opérationel par l'échange de cellules de gestion.

Le plan de contrôle communique au travers du réseau ATM en échangeant des messages de signalisation. Chaque message de signalisation est structuré en éléments d'information (IEs), chacun contenant un type d'information particulier utile aux opérations de contrôle. Toutes les informations sont échangées sur le réseau sous forme de cellules ATM de 53 octets composées d'une entête (contenant des informations de routage) et d'une charge utile (les données utilisateur).

Le modèle ATM comprend trois couches basses : une couche physique principalement responsable de la transmission sur le réseau, une couche ATM essentiellement chargée des fonctions de multiplexage et de commutation et une couche AAL (*ATM Adaptation Layer*) qui permet entre autre d'adapter les besoins des applications aux flux ATM en effectuant par exemple des segmentations/réassemblages de cellules ATM.

4.2. La version draft 5 des spécifications de sécurité de l'ATM Forum [1] :

Les objectifs et contraintes de l'ATM Forum :

- A le but de la solution ATM Forum est de s'assurer de l'identité des partenaires d'une connexion (authentification), de refuser au besoin une communication en fonction de l'identité déclinée (contrôle d'accès) et de garantir au récepteur des données utilisateur la confidentialité/intégrité des données et l'identité de leur émetteur.
- B la solution développée doit permettre d'assurer à la fois une protection de bout en bout et une protection sur des portions de réseau (voir point 1).
- C les modifications apportées à l'ATM sont autorisées (point 3) du fait que la technologie ATM est toujours en cours de spécifications.
- D la solution doit proposer le maximum de techniques d'implémentation possibles.

Préambule sur les possibilités de protection des réseaux ATM :

Comme le décrit la section 4.1, l'échange d'informations de sécurité au travers du réseau ATM peut se faire de trois façons différentes : les IEs des messages de signalisation, les données utilisateur et les cellules de gestion. Chacun de ces supports a ses avantages.

La signalisation offre l'avantage de permettre d'échanger à l'ouverture de connexion des informations de sécurité avant tout échange de données utilisateur. Elle peut donc servir à négocier les services de sécurité et les paramètres (e.g. clés) qui serviront ultérieurement à protéger les données utilisateur. C'est aussi à l'ouverture de connexion, que le terminal appelé ou le réseau public accepte ou refuse d'établir une connexion. Les échanges de signalisation à l'ouverture de connexion peuvent donc servir à transporter les authentificateurs des partenaires d'une connexion et ainsi permettre au réseau public et aux partenaires de la connexion de réaliser un contrôle d'accès efficace.

La signalisation permet de gérer une connexion : l'ouverture de connexion mais également sa libération, l'ajout de partenaires à une connexion point-à-multipoint, etc. Il est donc nécessaire de protéger certains messages de signalisation sensibles en assurant au minimum l'authentification de l'émetteur et leur intégrité.

L'avantage des cellules de gestion est qu'elles permettent d'échanger des informations de sécurité à tout moment au cours de la connexion et de façon synchronisée avec les données utilisateur.

Il est aussi possible d'échanger dans le flux de données utilisateur des informations de sécurité au cours d'une connexion. Cependant, pour que le récepteur puisse distinguer les informations de sécurité des données utilisateur, il est nécessaire de l'informer de l'envoi d'informations de sécurité, par exemple par le biais de cellules de gestion.

Application du guide d'aide à la conception de solutions de sécurité :

L'ATM Forum autorise tout type de modifications (contrainte C). Il est donc possible de modifier la signalisation et les cellules de gestion pour introduire des informations de sécurité (point 3). De plus, la signalisation et les cellules de gestion sont visibles à la fois par le réseau public et par les terminaux d'une connexion. Une solution utilisant ces deux moyens de communication et satisfaisant la contrainte B peut donc être définie.

L'introduction d'informations de sécurité dans la signalisation consiste à définir de nouveaux IEs (cf. section 4.1) de sécurité dans les messages de signalisation. L'ATM Forum en définit sept dans la version 5 de ses spécifications de sécurité. Ils permettent d'authentifier les partenaires d'une connexion et aussi de négocier des services et paramètres de sécurité.

Une autre alternative peut aussi être envisagée pour négocier des services de sécurité et réaliser de l'authentification/contrôle d'accès à l'ouverture de connexion. Elle est utilisée par l'ATM Forum (objectif D). Il s'agit d'utiliser le flux de données utilisateur, c.à.d. de bloquer les échanges de données utilisateur une fois la connexion établie, de négocier des services de sécurité via le flux de données utilisateur et d'autoriser à nouveau les échanges de données utilisateur une fois la négociation réalisée. Cette alternative a l'avantage de permettre une négociation de services à tout moment au cours de la connexion. Par contre, elle nécessite de bloquer tout échange de données utilisateur durant la négociation. Pour une négociation de services de sécurité qui ne se produit que rarement, cette alternative est envisageable (à condition que l'application utilisée ne soit pas temps-réel) mais pour une mise à jour fréquente de paramètres de sécurité (e.g. le renouvellement de clés de chiffrement), les cellules de gestion apparaîssent plus adaptées.

Les cellules de gestion sont d'autant plus intéressantes à utiliser qu'elles permettent de communiquer, en cours de connexion, des informations de sécurité en parfaite synchronisation avec le flot de données utilisateur. Cet aspect synchronisation est surtout nécessaire pour assurer le renouvellement des clés de chiffrement en cours de chiffrement et ainsi éviter que le récepteur ne perde des données utilisateur suite à l'utilisation d'une clé de déchiffrement inappropriée. L'ATM Forum fait appel aux cellules de gestion pour renouveler les clés de chiffrement.

Les cellules de gestion pourraient aussi être utilisées pour négocier des services de sécurité. Cependant, le trafic de cellules de gestion supplémentaire engendré risquerait d'être très important et de perturber les échanges de données utilisateur - surtout dans le cas de connexions à débit garanti (*Constant Bit Rate*) - du fait que les informations de gestion introduites sont comptabilisées en tant que données utilisateur. Pour cette raison-là, l'ATM Forum n'exploite pas cette possibilité.

La protection des données en confidentialité (objectif A) ne peut se faire que sur la couche ATM par chiffrement du contenu des cellules ATM. En effet, la solution développée par l'ATM Forum doit permettre la protection des communications de bout en bout et aussi sur des portions de réseau. Comme le mentionne le point 1, il est donc nécessaire de placer le service de confidentialité sur la couche réalisant la fonction de routage des cellules, c'est à dire sur la couche ATM. Plusieurs possibilités de chiffrement existent sur la couche ATM. L'une consiste à chiffrer les cellules ATM en entier (entête + charge utile), mais elle nécessite que les commutateurs déchiffrent les cellules ATM pour avoir accès à l'entête des cellules ATM et pour réaliser correctement le routage des cellules. Elle n'est donc pas applicable à une protection de bout en bout. C'est pourquoi, l'ATM Forum a choisi une autre possibilité qui consiste à limiter le chiffrement au contenu même des cellules.

Comme le spécifie le point 4, pour des raisons de performances il est nécessaire que les services d'intégrité/authentification des données utilisateur soient rendus au dessus ou dans la couche AAL. De ce fait, il s'avère impossible de définir une solution intégrant les services d'intégrité/authentification et réalisant la protection des communications sur des portions de réseau. L'ATM Forum s'est donc trouvé contraint de distinguer la solution de protection de bout en bout intégrant les services d'intégrité/authentification des données utilisateur qui sont à placer dans la couche AAL et une solution de protection sur des portions de réseau qui ne garantit pas l'intégrité/authentification des données utilisateur.

4.3. La solution SAFE de l'ENST-Bretagne [12]

Les objectifs et contraintes de la définition de la solution SAFE :

- A le but de cette solution est sensiblement le même que celui de l'ATM Forum. Elle vise en plus à garantir l'anonymat aux partenaires de la connexion et à protéger en confidentialité l'ensemble des paramètres de sécurité sensibles de la connexion (services de sécurité et paramètres de sécurité à négocier).
- B la solution développée doit uniquement permettre d'assurer une protection de bout en bout (point 1).
- C les modifications apportées à l'ATM sont autorisées (point 3) mais doivent être réduites pour simplifier l'implémentation au sein d'un logiciel ATM existant.
- D toutes les clés de chiffrement sont prédistribuées avant l'ouverture de connexion.
- E les services de sécurité doivent tous être placés au dessus de la couche AAL. Cette contrainte provient de considérations purement matérielles. La solution devait initialement être implémentée mais, comme tout développement en *hardware* était impossible, il ne restait que la solution de placer les services de sécurité au dessus de la couche AAL.

Application du guide d'aide à la conception de solutions de sécurité :

Tout comme la solution de l'ATM Forum, les modifications étant autorisées, il est possible de réaliser la négociation de services de sécurité et l'authentification/contrôle d'accès par le biais de la signalisation en définissant de nouveaux IEs de sécurité. Cependant, comme les modifications sont autorisées de façon limitée (objectif C), la solution SAFE ne définit qu'un seul IE de sécurité. Du fait que l'ensemble des clés de chiffrement sont prédistribués (contrainte D), il est possible de satisfaire la contrainte A en chiffrant dans cet IE certaines informations sensibles comme la liste des services de sécurité à négocier et divers paramètres de sécurité.

Contrairement à l'ATM Forum où deux solutions de négociation de paramètres de sécurité sont préconisées, seule la solution de définir un IE de sécurité est exploitée par l'ENST-Bretagne car elle est la seule à satisfaire l'objectif A et car les modifications engendrées par la solution choisie doivent être limitées (contrainte C).

La solution SAFE envisage uniquement de protéger les communications ATM de bout en bout (objectif B). Les services de sécurité doivent donc être placés au dessus de la couche ATM (cf. point 1). Avec la contrainte supplémentaire E, seul un placement des services de sécurité juste au dessus de la couche AAL est envisageable.

Avec l'objectif C de limiter les modifications à introduire dans le modèle ATM (cf. point 3), la solution la mieux adaptée consiste à définir une couche de sécurité du type IEEE 802.10 (cf. section 2.2) à placer au dessus de la couche AAL. Cette couche met en place les services de sécurité négociés à l'ouverture de connexion. Ainsi, si aucun service de sécurité n'a été négocié, cette couche devient alors transparente pour la connexion.

5. Conclusions

Cet article montre qu'il est impossible de définir une solution de sécurité générique qui permette de protéger les communications sur tout type d'environnements réseau. Il montre en particulier, que les normes de sécurité actuelles ne sont que très rarement réutilisables sur des environnements réseau particuliers.

A défaut de solutions génériques, cet article présente un guide qui aide à concevoir de nouvelles solutions de sécurité. C'est à dire, en fonction des contraintes et objectifs fixés - du type d'informations à protéger, du choix de l'intervention ou non du réseau public dans la protection des communications et des limitations fixées quant à l'impact de l'introduction de la sécurité sur la technologie réseau - il détermine les différentes options de placement des services de sécurité au sein de la technologie réseau considérée. Finalement, il examine deux solutions de sécurité développées dans un contexte de réseau ATM et montre qu'en appliquant le guide et en tenant compte des objectifs et contraintes de chaque solution, il est possible de retrouver les choix de placement des services de sécurité sélectionnés par les solutions de sécurité.

Références

[1] ATM Forum, «ATM Forum 95-1473R5, Phase I ATM security specification», octobre 1996.

[2] Aziz A., Markson T. et Prafullchandra H., «Simple Key-Management For Internet Protocols (SKIP)», draft IPSEC, août 1996.

[3] Fulchignoni P., Marrota G. et Wiley A.J., «Applying security to SMDS: a pratical example», IEEE Infocom 93, San francisco, CA, mars 1993, pp. 1414-1421.

[4] Hebrard P., «Sécurité dans les couches basses de l'OSI», CFIP'95, Rennes, mai 1995, pp. 110-129.

[5] CCITT I.321, «B-ISDN Protocol Reference Model and its applications», 1991.

[6] IEEE 802.10 «Standard for Interoperable Local Area Network (LAN Security (SILS) - Part A - The Model», draft, décembre 1989.

[7] IEEE 802.10 «Standard for Interoperable Local Area Network (LAN Security (SILS) - Part B- Secure Data Exchange», draft, janvier 1990.

[8] IEEE 802.10 «Standard for Interoperable Local Area Network (LAN Security (SILS) - Part C - Key management», draft, septembre 1993.

[9] ISO/IEC IS 11577, «Network Layer Security Protocol», 1994.

[10] ISO/IEC IS 10736, «Transport Layer Security Protocol», 1993.

[11] ISO 7498-2, «Systèmes de traitement de l'information : Interconnexion de systèmes ouverts, Modèle de référence de base. Partie 2 : Architecture de sécurité», septembre 1990.

[12] Laurent M., Paul O. et Rolin P., «Une solution de protection des communications sur les réseaux ATM», CFIP'97, Liège, Belgique, septembre-octobre 1997.

[13] ITU-T Q.931, «Digital Subscriber Signaling System N^{o}.1, Network Layer -ISDN User-Network Interface layer 3 specification for basic call control», mars 1993.

[14] Recacha F., Melus J.L., Simon X., Soriano M. et Forné J., «Secure data transmission in extended Ethernet environments», IEEE Journal on selected areas in communications, Vol. 11, N^{o}. 5, juin 1993, pp. 794-803.

[14] Sailer R., «Integrating authentication into existing protocols», 5th open workshop high speed networks, Paris, mars 1996.

[15] Saltzer J.H., Reed D.P. et Clark D.D., «End-to-end arguments in system design», ACM Transactions on Computer Systems», Vol. 2, N^{o}. 4, novembre 1984, pp. 277-288.