ATM Security State of The Art[1]

Maryline Laurent[2]
Associate Professor at ENST de Bretagne
E-mail : Maryline.Laurent@rennes.enst-bretagne.fr

Pierre Rolin
Head of Scientific Evaluation, Survey and Skills Department at CNET-DS-SEV
E-mail : pi.rolin@cnet.francetelecom.fr

ABSTRACT :

We present a survey of existing solutions aiming to secure communications passed over ATM networks against malicious attacks that may be mounted on them such as hackings, eavesdroppings and traffic tamperings. Different solutions are analyzed and compared with emphasis on the ATM Forum draft specifications of September 1997 and the security solution developed in ENST de Bretagne (a French Graduate School of Telecommunications Engineering).

We give details about the security services offered by each ATM security proposition, their placement within the ATM Protocol Reference Model, the mechanisms to negotiate security services and the techniques to provide synchronization and dynamic key change during user data exchange.

Keywords : B-ISDN, ATM, network security, security services.

1. Introduction

ATM is a cell switching and connection-oriented technology which is usually represented as a three-plane model [I.321], as depicted in figure 1. The user plane is responsible for user data exchanges over the ATM networks ; the control plane monitors signaling information ; and the management plane maintains the network operational.

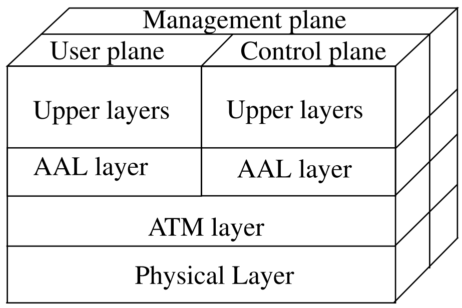

Figure 1 : The ATM protocol reference model

The control plane communicates over the ATM network by exchanging signaling messages [UNI3.1] such as : the SET UP message which is sent by the calling party over the network to request a connection set up ; the CONNECT message which is returned in response to SET UP by the called party to inform the connection initiator of the call acceptation ; the RELEASE message that causes a connection release. Signaling messages are organized into Information Elements (IEs), each of which includes a spe-

1. In proceedings of 1998 ATM Development; Rennes, France.
2. This work was supported by DRET

cific information type useful for control operations. For instance, SET UP messages contain IEs specifying the calling and called end-stations' ATM addresses which are respectively called *calling entity number IE* and *called entity number IE*. SET UP messages include also an IE informing of the application type requested by the connection's initiator and called BHLI IE *(Broadband High Layer Information IE)*.

The management plane communicates over the network by exchanging OAM (Operation And Maintenance) management cells making it possible mainly to monitor performance.

When an application needs to send user data over the ATM network, three lower layers are involved in ATM cells construction. The ATM Adaptation Layer (AAL) receives user data from the upper layers application (see figure 1) and segments these data into 48-byte blocks which are then sent to the ATM layer. The ATM layer appends to each block a 5-byte header thus obtaining 53-byte ATM cells. The 5-byte header encompasses routing information useful for the network to transport cells to the appropriate destination. ATM cells are then sent by the physical layer over the transmission medium.

With no security services being currently offered in ATM specifications, communications passed over ATM networks are vulnerable to the following attacks :

- eavesdroppings. A malicious person (later referred to as «an intruder») equipped with a traffic analyzer can position himself at a point on the network, observe the traffic exchanged over a communication and deduce information useful for mounting an attack later.
- traffic tamperings. An intruder can modify the traffic's content either by acting on the transmission medium or by introducing a traffic analyzer/generator in a network facility (e.g. switch).
- masquerades. An intruder can masquerade as another user when setting up a connection and thus retrieve confidential information for instance.

To secure ATM communications, it is necessary to introduce the following security services [X800] in ATM :

- **confidentiality** (against eavesdropping attacks) allows the sender to protect user data sent over the network using encryption mechanisms so that user data can only be understandable by the legitimate destination. Usually symetric keys algorithms [Sch94] are used. That is, the same secret cryptographic key is shared by both the partners of the connection. Because of its frequent use and since the more a key is used, the more vulnerable it is, this key later referred to as a **session key** must be updated frequently and securely. Session keys updating's security is usually ensured with asymetric keys algorithms. Asymetric keys algorithms are based on a pair of complementary keys. The **private key** should be known by only one entity and the **public key** should be widely broadcasted to network entities by means of a **public key certificate** generated by a **certificate authority**.

  If applied to origin and destination addresses fields, the confidentiality service is called **anonymity** [Sam96, p80] since it hides the connection partners' identities (names, addresses, etc.) from possible eavesdroppers.
- **traffic flow confidentiality** (against eavesdroppings) consists in introducing meaningless data into the user data flow so that the connection rate remains constant and thus no information relative to that connection (quantity of the user data being exchanged, its frequency, etc.) is deduced by flows analysis.
- **replay detection** (against masquerades) enables the receiver to be sure that the receiving data have not been previously played, i.e. received.

- **authentication** (against masquerades) guarantees the destination that the user data sender is as claimed. This is achieved by sending user data along with a **digital signature** usually calculated over these data with asymetric keys algorithms.
- **integrity** (against data tamperings) guarantees the destination that receiving data have not been modified during their transfer. Digital signature mechanisms are usually used.
- **access control** (against masquerades) limits the access to system resources to authorized entities only.

Since 1994/1995, the ATM Forum consortium and other working groups have been working on introducing security services - mainly the confidentiality, integrity and authentication services - into ATM. This does not consist in defining new security mechanisms, but in reusing existing security mechanisms such as encryption, digital signatures, etc. The difficulty is to choose the appropriate placement for these mechanisms within ATM, which is at the basis of most ATM security works' divergence.

This paper describes current works realized in the ATM security area. In particular, ATM Forum's works which are expected to define the first ATM security specifications in February 1998 are presented based on the BTD-SECURITY-01.04 document of September 1997 [AFSEC2]. Other works such as ENST-Bretagne's [Lau97b, Lau97c], Deng et al.'s [Den95], Stevenson et al.'s [Ste95] and Varadharajan et al's [Var97] are also presented. Since securing an ATM communication is based on firstly negotiating a security context and secondly applying negotiated security services on user data exchanges, the presentation of these works is divided into two corresponding sections 2 and 3. Finally, section 4 concludes with a general comparison between ATM security solutions.

2. Security services negotiation

ATM security solutions differ in that security services negotiation is done :

- during connection set up within control operations [AFSEC2, Den95],
- along the connection within management operations [AFSEC2],
- over an auxiliary channel dedicated to security operations [AFSEC2, Ste95].

Note that the ATM Forum uses all these schemes to exchange security information.

Along this paper, notations of table 1 are used.

Table 1 : Notations

A	calling entity
B	called entity
KAB	session key generated by A to protect flow from A to B
KsA {M}	encrypted M with A's private key
KpA{M}	encrypted M with A's public key
T_A	current timestamp generated by A
N_A	nonce generated by A
CA	certification authority entity
Cert_A	A's public key certificate generated by CA

Security IE Identifier	
	IE instr. field
Length	
Security Association Section(s)	

The security IE's fields include one or more *Security Association Sections* (see figure 4) specifying the security informations required to establish a security association between two security agents (for details, refer to [AFSEC2]).

Figure 3 : The ATM Forum's security IE

2.1. Negotiation within signaling operations

This approach is intuitive. Prior to user data exchanges over an ATM network, it is necessary to both set up a connection and negotiate the security services that will be used later to protect these user data. So it is possible to transfer security negotiation information via set up signaling messages - SET UP and CONNECT - as shown in figure 2. This approach consists in defining new IEs dedicated to security and is attractive since, besides services negotiation, it makes it possible to secure signaling messages exchanges.

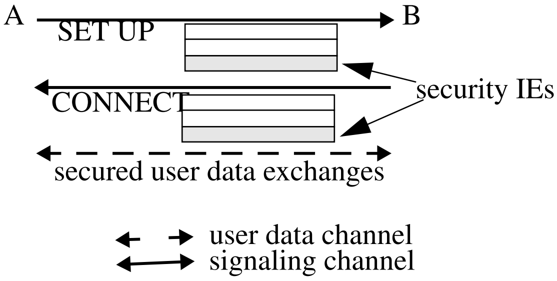

Figure 2 : The negotiation within signaling operations

2.1.1. The ATM Forum

The ATM Forum defines in its latest security specifications document [AFSEC2] of September 1997 one security IE whose format is given in figures 3, 4, 5 and 6 and which provides authentication, access control, unidirectional keys exchange and security context negotiation.

Security Association Section (SAS) ID			
SAS length			
Version	Transport Ind.	Flow Ind.	Discard
Scope			
Target Security Entity ID			
Relative ID			
Security Service Data Sections			

The *security associations section* includes :
- *Version* denotes the version to which the IE is compliant
- *Transport Indicator* indicates the transport method which will be used later to exchange security information (via signaling or via an auxiliary connection as described in section 2.3.2).
- *Flow Indicator* identifies the flow number of the security exchange (in the 2 or 3 way security protocol used).
- *Discard* indicates whether a security agent receiving this *security association section* should erase this *security association section* before forwarding the security IE over the network.
- *Scope* implicitly identifies the security agent responsible for the processing of the security association. It provides implicit identification of the target security agent : i.e., the region where the security agent is located (in the emitting or receiving ATM private network or the public network) and the agent's role (if it must be placed in an end-station, at the border of a private enterprise or in the public network).
- *Target Security Entity ID* explicitly identifies the agent.
- *Relative ID* identifies the security association.
- *Security Service Data Section(s)* indicates either a label (*Label Based Access Control* - cf figure 6), or a list of security parameters to be negotiated (*Security Message Exchange Data Section* - cf. figure 5).

Figure 4 : The *Security Association Section* of the ATM Forum's security IE

ID	Security Message Exchange Type
Security Entity ID	
Security Service Specifications Section (security services + algorithms)	
Confidentiality Section (keys)	
Authentication Section (timestamp + nonce + signature)	

The *Security Service Data Section* may be in the form of a *Security Message Exchange Data Section*. The latter is identified by the *ID* field and includes the following fields :
- *Security Message Exchange Type* specifies the (2-way or 3-way) security protocol type used.
- *Security Entity ID* identifies the security agents involved in security exchanges if an explicit agents identification is required.
- *Security Service Specifications Section* specifies the security services that need to be negotiated together with the security mechanisms to be used.
- *Confidentiality Section* is encrypted and allows security agents to exchange 3 keys : 2 session keys, one used to encrypt subsequent user data exchanges and the other one to generate a digital signature over these data and a master key $K_{m,AB}$ which will be used later for updating session keys during the connection. This section is obviously confidentiality protected by the algorithm indicated within the *Security Service Specifications Section*.
- *Authentication Section* includes a digital signature which is calculated over the *security association section* and the IEs required by the security protocol being used. The signature is also calculated over the timestamp and the nonce included within the *Authentication Section* thus allowing security IEs to be protected against any possible security IE replays.

Figure 5 : The *Security Message Exchange Data Section* of the ATM Forum's security IE

Two main strategies to protect communications passed over the public network are available in [AFSEC2]. The first one expects the end-stations (or more generally end-sites in case of remote sites being interconnected) to protect their communications on their own (without the public network's help) and is referred to as «end-to-end» protection. The second strategy, called «hop-by-hop» protection, makes public operators secure communications over public network segments separated by security facilities. All intermediate strategies are also possible such as protecting communications between an end-station (or end-site) and one of the public network's security facilities.

Depending on the strategy, security agents (in charge of the communications' security) are placed in public network's security facilities or in end-stations. To protect a communication over the network segment in between, two security agents must negotiate a security context by appending a security association section (cf. figure 3) to the security IE.

The ATM Forum offers the following security services :

2.1.1.1. Authentication, integrity and replay detection services

The authentication service is achieved by introducing a digital signature in the security IE (in the *Authentication Section* field within the *Security Service Data Section*). Additionally to the authentication service, the digital signature ensures integrity of the *Security Association Section* and messages replay detection since it is calculated over a timestamp and a sequence number (cf. figure 4).

Label ID
Label Length
Label Type
Label-Specific Data

The *Security Service Data Section* may include a *Label Based Access Control* section which is identified by the *Label ID* field (cf. section 2.1.1.3).

Figure 6 : The *Label Based Access Control* of the ATM Forum's security IE

Figure 7 : The Démostène's context is typically a company's local networks interconnection proble

2.1.1.2. Security services negotiation and keys exchange

The *Security Service Specification Section* in the *Security Association Section* (cf. figure 5) allows the security agents to negotiate the confidentiality and integrity services (that will be used to protect subsequent user data), the authentication service (i.e. the digital signature generation algorithm) and keys exchange and session keys update services. More precisely, this section in SET UP messages includes security services to be negotiated together with security mechanisms (e.g. algorithms) supported by the emitting security agent. In the CONNECT message, it includes security mechanisms chosen by the receiving agent.

2.1.1.3. Access control service

The ATM Forum defines the *Label Based Access Control Section* (cf. figure 6) to specify the sensitivity level (e.g. public, confidential, etc.) of user data that need to be exchanged over the connection so that, for instance, the path selected over the network uses only links with appropriate sensitivity level.

The ATM Forum proposes that an access control service based on the calling and called entities' ATM addresses be introduced in ATM switches.

2.1.2. Solution SAFE proposed by ENST-Bretagne [Lau97b, Lau97c]

The ENST-Bretagne's solution was developed in the Démostène project. This project's aim is mainly to secure communications passed over the ATM public network between remote ATM sites. The solution proposed is called SAFE for Solution for an ATM Frequent communications Environment since it is mostly designed for ATM sites needing to frequently communicate (cf. section 2.1.2.2). SAFE defines a security module to be introduced in the ingress switch of each ATM site (cf. figure 7) so that any communications being set up between remote ATM sites be protected by security modules.

Although mostly developed before the ATM Forum's works, SAFE realizes security services negotiation within signaling messages as well, defining one security IE which is presented in figure 8. This security IE is organized into security elements, each of which supports security services being provided or negotiated to protect either signaling messages *(signaling)* or user data *(data)*. All these elements are optional in SAFE.

The security IE is exchanged between the ATM sites' security modules. That is, when a set up request originates from an end-station of its site and the SET UP message's destination is the remote site, the security module introduces an appropriate security IE into the SET UP message. After retrieving the security IE, the called security module processes it and, if the call is authorized (according to its site's security policy), it forwards the SET UP message without the security IE to the appropriate destination. Then the called security module sends back a security IE to the calling security module using the CONNECT message returned by the called end-station.

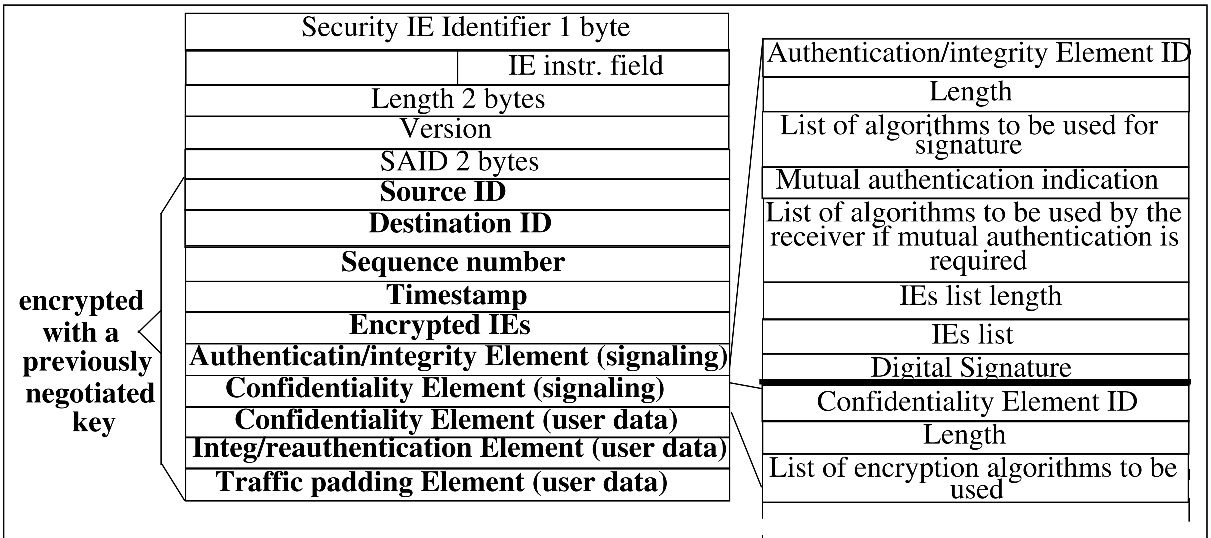

Figure 8 : SAFE's Security IE

Hereafter the security services offered by the IE are described :

2.1.2.1. Authentication, integrity and replay detection services

The digital signature placed in the *Digital Signature* field is computed over the security IE and all the «ordinary» IEs (not security-related) in the signaling message, whose identifiers are listed in the *IEs list* field.

Contrary to the ATM Forum's works, the signature algorithm to be used can be chosen by security modules. Indeed when the calling security module sends a security IE, it specifies a list of algorithms (with their respective information) ordered according to preferences within the field : *List of algorithms to be used for signature*. The first instance in the list is the algorithm code used to generate IE's signature. As such, if the called security module does not support that algorithm, it can choose another algorithm among the list and sends it back within a security IE. The calling security module will then use that algorithm to authenticate itself in other messages and may also specify available algorithms that the called security module should use to generate its signature in the security IE within the field *List of algorithms to be used by the receiver if mutual authentication is required*.

Contrary to ATM Forum's works, the calling security module may demand the called security module to authenticate by means of the field *Mutual authentication indication*. Also authentication based on both stations addresses and users is allowed since the fields - *Source ID* and *Destination ID* - may be used to carry specific users or user groups identifiers (alternative use of such fields is described below).

Replay detection is achieved by means of the signature calculated over the *Sequence number* and *Timestamp* fields.

2.1.2.2. Confidentiality and anonymity services

In the literature, the signaling confidentiality service has never been studied since this assumes that a security context (i.e. at least one session key and an encryption algorithm) has been previously negotiated. In the context where ATM security modules frequently communicate like in the Démostène project, we assume that a connection dedicated to security has already been set up between them to negotiate a list of session keys so that no keys exchanges are needed at connection set up. This security context is identified by a security association identifier (*SAID* field) so that when receiving such a security IE, the security module needs to retrieve the appropriate key within the SAID security context to decrypt the security IE.

SAFE enables to encrypt part of the security IE written in bold in figure 8, i.e. security parameters included within security services elements but also ordinary signaling IEs which can be moved to the security IE in the *encrypted IEs* field to be encrypted, on the sole obvious condition that they are not analyzed by the intermediate public network.

This confidentiality service may also be used to hide information within the security IE such as end-stations' addresses. This scheme appears suitable for companies wanting to keep their own addresses mappings secret while communicating over the network with their subsidiaries. This is realized by defining one global address common to all company's stations. Thus when setting up a connection with that company, the only clear address within the SET UP message (in the *called entity number IE*) is the global one and the real stations' addresses are encrypted within the *Source ID* and *Destination ID* fields of the security IE. This assumes that the receiving security module decrypts the security IE with the security association identified by the *SAID* field before forwarding the set up request to the appropriate station.

2.1.2.3. Security services negotiation

Once all the session keys useful for connections protection are exchanged between security modules in a a specific connection dedicated to security, as specified in section 2.1.2.2, four security elements in signaling messages allow security modules to negotiate mechanisms and session keys numbers to be used to provide confidentiality (signaling and user data), integrity/reauthentication and traffic flow confidentiality services for the signaling and user planes. The calling security module specifies a list of algorithms ordered according to preferences and the called security module returns its choice within the subsequent signaling message. Then choices are stored as the security context (identified by an SAID) to be applied on subsequent user data and signaling exchanges.

2.1.3. Deng et al. [Den95]

Deng defines twelve new IEs - six for each SET UP and CONNECT message - which allow entities A and B to authenticate mutually, exchange unidirectional session keys (2 IEs) and negotiate a security context (4 IEs).

Only confidentiality and integrity services to be applied on user data may be negotiated. The calling entity A proposes a set of security parameters to B within SET UP in four IEs (IEs #1 to #4 - see figure 9). Parameters include its desired protection QoS (Quality of Service) and the lists of available confidentiality and integrity parameters. B replies with its chosen protection QoS and parameters in CONNECT (IEs #5 to #8). Then A accepts or refuses the connection depending on B's choices. Both A and B store the security context in the form of a security association identified respectively by A and B 's identifier (IEs #1 and #5).

Authentication and keys exchange are based on X509 two-way authentication protocol. The first X509 message within SET UP includes A's public key certificate (IE#9) that allows B to retrieve A's public key and a token $KsA\{T_A, B, KpB\{KAB\}\}$ (IE#10) that allows B to authenticate A and retrieve A's session key KAB. The X509 message returned by B within CONNECT (IEs #11 and #12) is similar.

This scheme is rigid since the authentication protocol is imposed. Moreover using as many IEs as security parameters makes this scheme clear but not optimized in terms of modifications implied within UNI specifications.

Security IEs to be inserted by A into SET UP are:
IE#1: A's security association identifier
IE#2:Protection QoS: type of authentication, confidentiality and integrity levels
IE#3:Confidentiality operation parameters
IE#4: Integrity operation parameters
IE#9:A's certificate Cert_A = KsCA{serial number, validity period, A, KpA, CA}
IE#10: A's token = KsA{T_A, B, KpB{KAB}}

Security IEs to be inserted by B into CONNECT are:
IE#5: B's security association identifier
IE#6:Chosen protection QoS: chosen type of authentication, chosen confidentiality and integrity levels-
IE#7:Chosen confidentiality operation parameters
IE#8: Chosen integrity operation parameters
IE#11:B's certificate Cert_B = KsCA{serial number, validity period, B, KpB, CA}
IE#12:B's token = KsB{T_A, A, KpA{KBA}}

Figure 9 : Deng's IEs.

2.2. Negotiation through management information

This scheme consists in injecting security information in-band within the user data channel by means of OAM cells (cf. section 1). This scheme has advantages over the previous approach since it ensures perfect synchronization between security information being exchanged and the user data stream.

2.2.1. The ATM Forum [AFSEC2]

The ATM Forum uses such a scheme when security information requires synchronization with the user data cells stream, that is when new session keys need to be exchanged during a connection. This session keys update is realized in two steps. Firstly, the new session key is transmitted over the network between security agents and secondly this key is activated so that subsequent user data cells being sent are encrypted with the new session key. Two corresponding OAM cells dedicated to security are defined. The OAM cell containing the new session key is obviously encrypted with the session key update algorithm negotiated at connection set up (see section 2.1.1.2) and the master key exchanged at connection set up (in the security IE's *Confidentiality Section* - cf. figure 5).

2.3. Negotiation through an auxiliary channel

Auxiliary channel notion is used here when security information is exchanged in the connection's content.

2.3.1. Stevenson et al. [Ste95]

Stevenson suggests to negotiate session keys at connection set up within the first data exchanged.

Figure 10 (a) depicts such a scheme in a proxies context. Proxies A and B are usually on line cryptographic units located at LAN boundaries whose function is to protect communications over the public network.

As shown in figure 10 (a), A sends a set up request to its proxy which in turn forwards it to proxy B. Before completing the connection set up between A and B, proxies A and B negotiate session keys by exchanging firstly their certificates and nonces and secondly their tokens which include unidirectional session keys and serve as authenticator. After keys negotiation, proxies complete the connection set up between A and B which are then allowed to exchange user data.

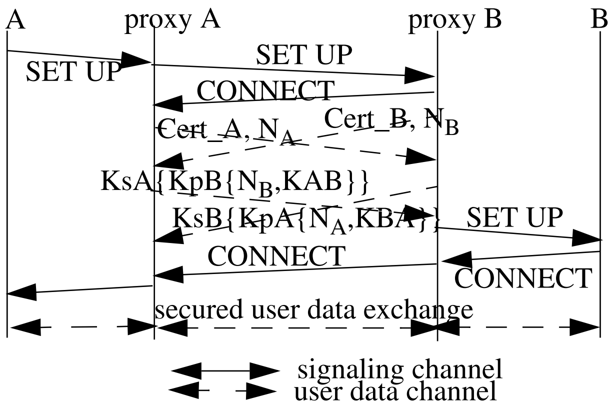

Figure 10 : (a) Session keys negotiation at connection set up via an auxiliary channel. Stevenson et al.'s solution.

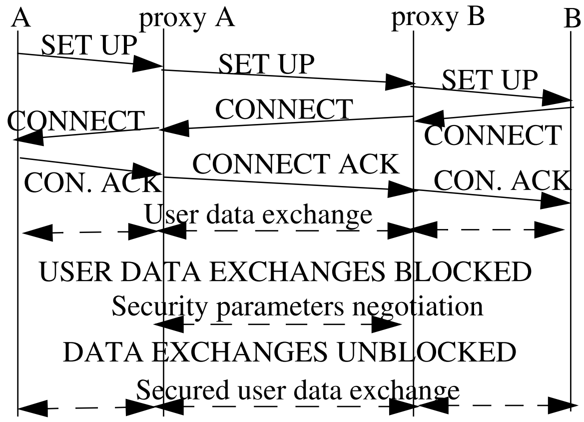

Figure 10 : (b) Parameters negotiation via the auxiliary channel. The ATM Forum's solution.

2.3.2. The ATM Forum [AFSEC2]

This solution is used in conjonction with the solution of section 2.2.1 to negotiate security parameters (security mechanisms). It may also be used to do mutual authentication during connection.

This solution applies in a proxies context like with the Stevenson's solution. However, as shown in figure (b), after the connection completion, proxies A and B may block the user data exchanges at any time during the connection in order to negotiate the security services that will be used to protect subsequent user data exchanges.

2.4. Comparisons of the solutions

As shown in table 3 (at the end of the paper), solutions may be compared in terms of modifications required within the ATM Forum's UNI specifications. Whereas Deng, the ATM Forum and SAFE introduce respectively twelve new IEs, one new IE and security OAM cells and one new IE, Stevenson requires no UNI modifications since modifications are transparent for the ATM network. Stevenson modifies only the connection's content.

Actually the ATM Forum at the beginning of its works defined as many security IEs as security services being used. [AFSEC1] of October 1996 specifies 7 security IEs. However, for the reasons mentionned above (see [Lau97a]), the ATM Forum decided to limit the number of its security IEs to one, as was defined in [AFSEC2].

All solutions include drawbacks listed hereafter.

The ATM Forum (section 2.1.1), SAFE and Deng's solutions expect intermediary public network facilities to transparently pass security information elements which may be used as covert channel (to pass data for free if signaling is free). As a consequence, operators are reluctant to introduce new security IEs in signaling messages.

Both in-band and auxiliary channel schemes include flaws. The former is unsuitable for unidirectional communications and real-time applications. Depending on the implentation considered, the latter scheme enables (ATM Forum) or disallows (Stevenson) security parameters to be renegotiated during a connection. However both of them offer advantages over the security IE definition based scheme since they allow security agents (or proxies/security modules) to negotiate security services with as many exchanges as necessary, thus allowing any security protocols - two-way or three-way exchange security protocols - to be used.

3. User data protection

User data exchanges may be protected with the security services negotiated in section 2. Since the user plane is responsible for processing user data (cf. section 1), these services must be placed within that plane.

Solutions differ in that user data encryption is performed :

- at the ATM layer [Ste95, AFSEC2],
- within the AAL layer [Den95],
- above the AAL layer [Lau97b, Lau97c].

3.1. Confidentiality at the ATM layer

This scheme consists in encrypting user data on the cell-by-cell basis. However encryption algorithms are more or less error-extension sensitive. That is, cell loss occurrence may cause for instance at most one 64-byte block loss when encrypted with DES ECB (Electronic Code Book) and much more data loss when encrypted with DES CBC (Cipher Block Chaining) [Sch94], since in the ECB mode, blocks of data are encrypted independently whereas in the CBC mode, an encrypted block of data is dependent on the plaintext block that generated it but also all the previous encrypted blocks. To avoid too many losses to occur, encrypting/decrypting devices need to be frequently resynchronized. Hereafter each solution's synchronization mechanism is specified.

3.1.1. Stevenson et al. [Ste95]

Stevenson defines cryptographic units (proxies of section 2.3.1) which encrypt ATM cells with one session key per connection. He studies the «key agility» problem, i.e. the problem of switching keys quickly enough so that ATM cells streams from various connections can be encrypted independently. He also solves the synchronization problem by injecting synchronization information in-band within OAM cells or user data cells.

3.1.2. The ATM Forum [AFSEC2]

The ATM Forum supports user data confidentiality and integrity (with two independent keys) and optionally reordering/replay detection. Confidentiality may be realized end-to-end or hop-by-hop (cf. section 2.1.1) whereas integrity is only ensured end-to-end.

The integrity and optional reordering/replay detection are supported at the AAL layer by means of fields appended to the AAL SDU to protect : a signature computed over the AAL SDU, a timestamp and a sequence number. As mentioned in section 2.2.1, synchronization together with keysupdate are realized in-band within OAM cells.

3.1.3. Varadharajan et al. [Var97]

Varadharajan introduces a new security layer between the ATM and AAL layers. This layer provides confidentiality, integrity and AAL-PDUs emittor's authentication.

This solution is suitable for the AAL3/4 layer since the AAL3/4 (realizing user data frames segmentation) is the only AAL where a *Segment type* field is defined indicating the segment position - beginning, continuation or end of user data frame - within the user data frame being segmented. With the *Segment type* field, it is possible to define new AAL PDUs dedicated to encrypting/decrypting devices synchronization. In order not to confuse them with user data AAL PDUs, the se-

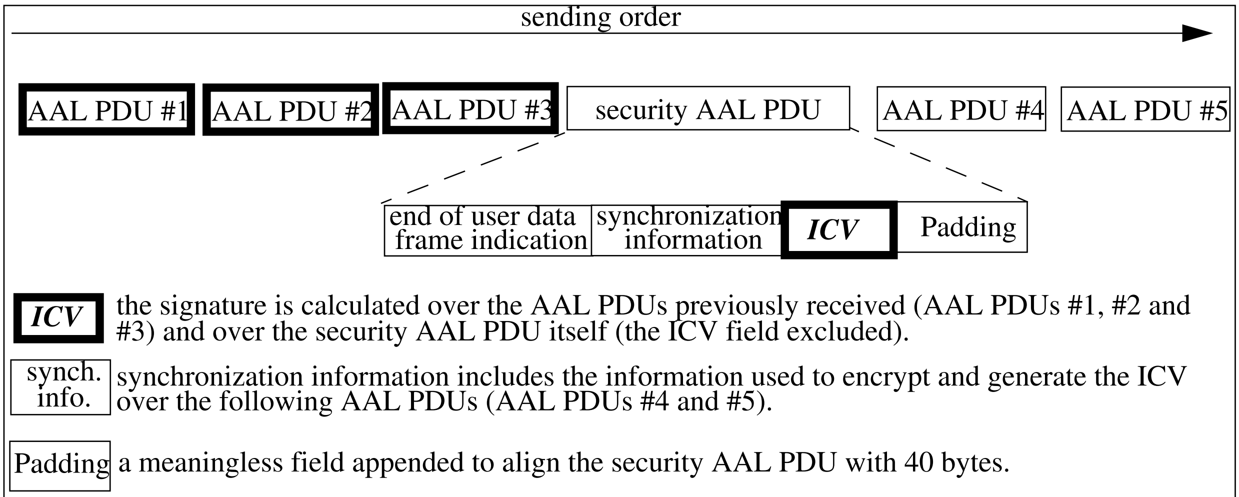

Figure 11 : The security AAL PDU construction
The Varadharajan et al.'s solution

curity AAL PDU is identified with the «end of user data frame» indication being present in the previous AAL PDU and with itself bearing the «end of user data frame» indication. Indeed, no consecutive AAL PDUs with the «end of user data frame» indication are allowed since an AAL PDU corresponding to an entire user data frame bears the «single segment» indication.

As depicted in figure 11, the security AAL PDU includes synchronization information useful for the receiving device to decrypt the user data AAL PDUs following the security AAL PDU (AAL PDU #4 and #5).

The security AAL PDU is also used to carry an ICV *(Integrity Checksum Value)* authenticator calculated over the user data AAL PDUs previously emitted and belonging to the same user data frame (AAL PDUs #1, #2 and #3 in figure 11).

The Varadharajan's solution also uses OAM cells to carry synchronization and ICV information through the network. The use of OAM cells allows other AALs than AAL 3/4 to be supported and allows synchronization to be done at any time during a connection and not only at the end of user data frames.

The main shortcoming of this solution is that the security layer is in charge of part of the AAL layer's processing since it analyzes the AAL PDU's *Segment type* field for security AAL PDUs detection. Thus the layers independence principle is not respected in the ATM model.

3.2. Confidentiality within the AAL layer

User data encryption is provided within the AAL layer prior to their segmentation into cells.

3.2.1. Deng et al. [Den95]

Deng defines an additional layer called DPL (Data Protection Layer) which is placed between two AAL sublayers and supports confidentiality and integrity services and optional reordering. DPL SDUs are independently encrypted and signed with the keys negotiated at connection set up and the Initialization Vector (IV) specified within the DPL SDU's clear header. As a consequence no synchronization is needed.

During connection the DPL layer may update session keys by halting data transmission and sending repeatedly one DPL SDU containing a new session key (encrypted with its private key) until

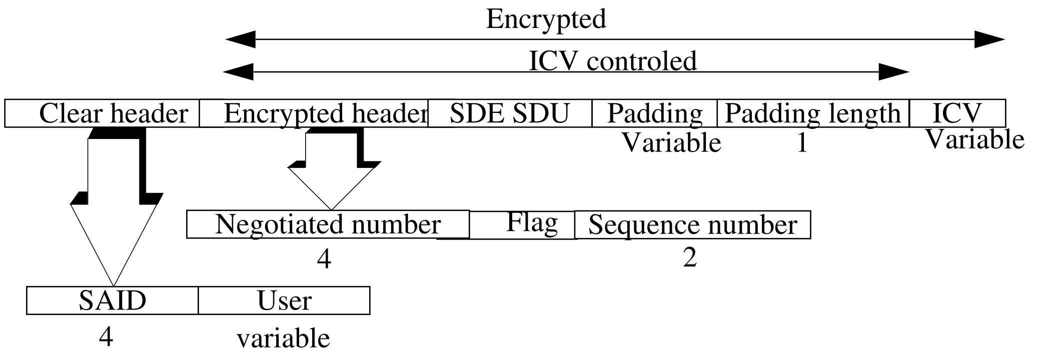

Figure 12 : SDE PDU construction.
Solution SAFE

reception of a positive acknowledgement. This scheme appears unsuitable for unidirectional communications and real-time applications and is unsecure since no strong authentication protocols are used to exchange session keys.

3.3. Confidentiality above the AAL layer

User data encryption is done on the AAL SDUs basis.

3.3.1. Solution SAFE proposed by ENST-Bretagne [Lau97b, Lau97c]

SAFE is close to Deng's solution (section 3.2.1) and the IEEE 802.10 model [IE802.10a, IE802.10b] since all user data security services are introduced into one additional layer. This layer is placed above the AAL layer and called Secure Data Exchange (SDE) layer in reference to IEEE 802.10.

As depicted in figure 12, the ATM Secure Data Exchange layer encapsulates user data (*SDE SDU*) with one clear header and one encrypted header.

SDE offers the following security services:

- user data confidentiality. The *SAID* field identifies the security context (negotiated in section 2.1.2) used to encrypt user data (SDE SDU). *Padding* and *Padding length* fields are used to align data to be encrypted with a length suitable for the encryption algorithm.
- user data integrity/authentication. The Integrity Control Value (*ICV*) computed over the SDE PDU encrypted part may be used to both authenticate and check integrity. However if the confidentiality service is offered, the ICV may be a simple Cyclic Redundancy Check (CRC) and the authentication service may be a secret number negotiated within the security IE and placed in the *Negotiated number* field.
- user data traffic flow confidentiality. Cells with no meaningful content may be injected into user data cells flow and recognized by means of the *Flag* field.
- user data replay detection. User data unicity is ensured with the *Sequence number* field.

Like with Deng's solution, synchronization is realized on each SDE PDU by inserting into the *User* field synchronization information such as session keys numbers and initialization vectors to be used for encryption or ICV generation.

3.4. Solutions comparisons

Solutions may be compared in terms of services supported. Stevenson's solution only supports the confidentiality service whereas all other solutions support confidentiality and integrity services at least.

We should note that the integrity service when offered is always placed at the AAL layer or above in order to avoid additional cells segmentations. The Varadharajan's solution which does not respect the layers independence principle supports the integrity service at the ATM layer although it is logically supported at the AAL layer (with introduction of security AAL PDUs). The confidentiality service is placed either at the ATM layer or above (in the AAL layer or above in SAFE).

Encrypting user data in the ATM layer brings simplicity since realized on fixed-size blocks (48-byte cells payloads) and high encryption speeds since implemented in the hardware.

Benefits result also from encrypting user data at the AAL layer or above. Modifications within the ATM layered model are restricted to one layer : the AAL layer for Deng's solution and the SDE layer for SAFE. Because of encryption realized on long-size block of data (up to 65535 bytes for DPL SDUs), no key agility problems arise. In Deng's and SAFE solutions, with the DPL SDUs and SDE SDUs being independently encrypted, the synchronization is naturally obtained. For Deng's solution, only session keys change requires synchronization with the user data flow.

However placing confidentiality at the AAL layer or above is less reliable than at the ATM layer since DPL PDUs and AAL PDUs' headers remain in clear.

It should be noticed that, contrary to the ATM Forum and SAFE solutions, the integrity and confidentiality services are not independent in Deng's and Varadharajan's solutions (cf. table 3) since both services use the same key. This results in algorithms choice restrictions and a weaker security level since in case the key being used is broken, user data exchanged may be decrypted but also corrupted user data may be generated and signed.

4. Conclusions

In this paper, we present and compare solutions proposed by Stevenson et al., Deng et al., ATM Forum, Varadharajan et al. and SAFE (ENST-Bretagne) to secure ATM networks. Thus, contrary to the ATM Forum which meets both operators and users' security needs, Stevenson, SAFE, Varadharajan and Deng focus on users' needs. That is, their philosophy is to ensure end-to-end communications security over an ATM public network considered as unsecure.

The ATM Forum and SAFE's solutions are the most complete solutions in terms of security services offered (cf. table 2), parameters possible to negotiate and implementation details level obtained (messages structures).

SAFE is the only one solution proposing confidentiality of part of signaling. Thus, contrary to the ATM Forum's and Deng's solutions, this allows security services to be negotiated via signaling while maintaining the exchanged security parameters confidential. This service is also used when interconnecting remote ATM sites to guarantee communicating entities' anonymity and ATM sites' addresses mappings secret (cf. section 2.1.2.2).

The ATM Forum's solution offers the biggest choices in terms of methods to be used for security services negotiation and renegotiation. However the ATM Forum's solution is also the most complicated solution to implement. Today no implementation of the ATM Forum's solution is available. SAFE is the only one solution being partly implemented [Pau96]. The Varadharajan's solution is currently being implemented.

Table 2 : Recapitulation of the security services offered by ATM security solutions

a	Stevenson et al.	Deng et al.	Varadharajan et al.	ATM Forum	SAFE (ENST-Bretagne)
security services established through signaling		A, KE, RD, SN:I+C		A, I, AC, KE, RD SN:I+C+KE+A for all signaling messages	(A, I, C, RD, SN:C+I+A+P+RD) for all signaling messages
security services established through management cells				KE	
security services established through the auxiliary channel	EC, A, RD			SN, A, KE	
user data security services	C within ATM S with OAM or user data cells	C, I, and (RD) within AAL S done for each DPL-PDU KE	C and I between ATM and AAL S with OAM cells or security AAL PDUs	C rather within ATM I, A and (RD) within AAL S with OAM cells	(C, I, A, RD, P) above AAL layer S on each secure SDE PDU

a. Notations used:

A Authentication	KE Keys Exchange
AC Access Control	P Padding
C Confidentiality	RD Replay Detection
I Integrity	SN:XX Negociation of service XX
(XX) Optional service XX	

Table 3 : recapitulation of the ATM security solutions

	Stevenson et al.	Deng et al.	Varadharajan et al.	ATM Forum	SAFE (ENST-Bretagne)
security parameters renegotiation	no	yes, keys exchange through DPL PDUs	no	yes, with management information	yes, via a secure auxiliary connection
authentication and/or keys negotiation protocol	protocols based on asymetric algorithms	X509 two-way protocol		within the signaling flow: two-way protocols within the auxiliary channel: not defined	two-way protocols
modifications required within UNI	none (unless synchronization is realized through security OAM cells)	12 new IEs		2 new IEs and new security OAM cells	one new IE
distinction between confidentiality and integrity services		no, mechanisms are different but keys are similar	no	yes	yes, mechanisms, keys and IVs are different

References

[AFSEC1] ATM Forum Security Working Group, (Draft) «ATM Forum 95-1473R5, Phase I ATM security specification», October 1996.

[AFSEC2] ATM Forum Security Working Group, (Draft) «Phase I Security Specification», BTD-SECURITY-01.04, September 1997.

[Den95] Deng R.H., Gong L., Lazar A.A., «Securing data transfer in Asynchronous Transfer Mode networks», Proceedings of Globecom'95, Singapore, November 1995, pp. 1198-1202.

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

[IE802.10a] IEEE 802.10 «Standard for Interoperable Local Area Network (LAN Security (SILS) - Part A - The Model», draft, décembre 1989.

[IE802.10b] IEEE 802.10 «Standard for Interoperable Local Area Network (LAN Security (SILS) - Part B- Secure Data Exchange», draft, janvier 1990.

[Lau97a] Laurent M., Rolin P., Stoffel L., «Security mechanisms within control plane», Contribution ATM Forum/97-0040, February 1997, San Diego, California.

[Lau97b] Laurent M., Paul O., Rolin P., «Securing communications over ATM networks», IFIPSEC'97, Copenhagen, Denmark, May 1997.

[Lau97c] Laurent M., «Protection des communications sur les réseaux ATM», Ph.d. thesis, Université de Rennes I, July 1997.

[Pau96] Paul O., «Conception et implémentation d'un module de sécurité pour les réseaux ATM», Rapport ME-96001, Télécom Bretagne, septembre 1996.

[Sam96] Samfat D., «Architecture de sécurité pour réseaux mobiles», Ph.d. thesis, Ecole Nationale Supérieure des Télécommunications, January 1996.

[Sch94] Schneier B., «Applied cryptography : protocols, algorithms, and source code in C», Volume ISBN 0-471-59756-2, John Wiley & Sons, 1994.

[Ste95] Stevenson D., Hillery N. et Byrd G., «Secure Communications in ATM Networks», Communications of the ACM, Vol. 38, N°. 2, February 1995, pp. 45-52.

[UNI3.1] ATM Forum, «ATM User-Network Interface Specification», version 3.1, 1994.

[X800] UIT-T X.800, «Data communication networks ; open systems interconnection (OSI) ; security, structure and applications. Security architecture for open systems interconnection for CCITT applications», 1991.

[Var97] Varadharajan V., Shankaran R., Hitchens M., «Security issues in Asynchronous Transfer Mode», ATMWORKS'97, New Zealand, February 1997.