ATM Forum Technical Committee
ATM Forum/97-0804

****

TITLE: Anonymity within the control plane

****

SOURCE:

Maryline LAURENT
Telecom Bretagne (ENST-B)
rue de la châtaigneraie - BP 78
35512 CESSON Cedex - France
Phone: 33 2 99 12 70 20
Fax: 33 2 99 12 70 30
E-mail: {Maryline.Laurent,Pierre.Rolin}@enst-bretagne.fr

Laurent STOFFEL
France Telecom
38-40 rue du General Leclerc
92131 Issy les Moulineaux - France
Phone: 33 1 45 29 62 02
E-mail : laurent.stoffel@Issy.cnet.fr

****

DATE: September 1997, Paris, France

****

DISTRIBUTION: SEC Working Group

****

ABSTRACT:

This contribution proposes a solution allowing communications between two private LANs to remain anonymous over the public network. This solution implies modifications to the SSIE (defined in the Phase I Security Specification BTD-SECURITY-01.04), which are described in this contribution.

We propose that this contribution be incorporated in the living list for phase II.

****

****

1 Introduction

As defined in [AFSEC], when a communication is set up between two end-stations, cleartext end-stations addresses are sent over the network. Thus the eavesdroppers positionned at a point on the network can know which end-stations need to communicate and, in case the mapping between users and stations is known, they may deduce end-users' identities. With such cleartext end-stations addresses, the eavesdroppers can easily select the connections to disrupt or to eavesdrop.

One solution to counteract this attack is to encrypt the end-stations addresses within the signaling messages so that end-users remain anymous along the path. However since end-stations addresses are useful for billing purpo-

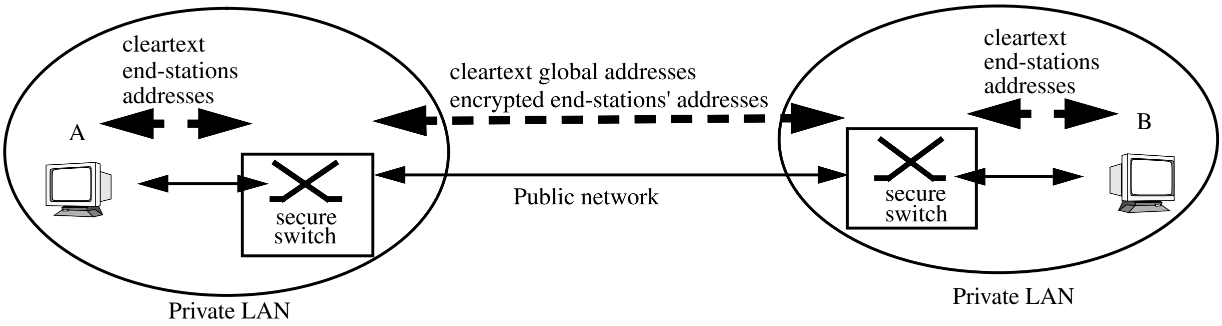

Figure 1 By defining one global address per private LAN and encrypting the stations addresses within the SSIE between the secure ingress switches, end-stations' addresses may be hiden over the public network. Thus only global addresses are in the clear over the public network.

ses and for the ATM network to establish communications between the appropriate end-stations, this solution is only possible for very specific examples. One of them is the case where two end-stations belonging to two remote private LANs need to communicate while remaining anonymous, as explained in section 2. In order to avoid billing disputes, it is necessary that each private LAN be considered as a unique subscriber entity by the public network.

2 The private LANs context where anonymity is of interest

As depicted in figure 1, it is possible for two end-stations located at two remote private LANs to communicate with anonymity guarantees through the public network. This is realized by defining one global address common to all the private LAN's stations. As described in figure 1, when setting up a connection, the only cleartext addresses indicated within the SET UP message (in the "called entity number" and "calling entity number" IEs) over the public network are the global ones. The real end-stations' addresses are encrypted within the SSIE (see section 3 for details). Anonymity is therefore guaranteed to the end-stations.

Actually, end-stations anonymity is ensured as follows : When setting up a connection with station B, station A needs to specify A and B's addresses in the clear within the SET UP message. The local ingress switch receiving the SET UP message should act as a secure proxy. It should replace end-stations addresses with the global private LANs addresses and build a new SSIE addressed to the remote private LAN's ingress switch with A and B's addresses encrypted inside. When receiving the SET UP message, the remote private LAN's ingress switch should decrypt the SSIE and forward the SET UP message with A and B's addresses in the clear.

Another solution that may be considered to obtain end-stations anonymity is for both the private LANs ingress switches to maintain an end-stations addresses mapping table update and secret so that the switches receiving a set up request consult their addresses mapping tables and replace the incoming message address with its corresponding address. With that solution, no encryption is required, thus saving the connection establishment time, but addresses mapping tables should be maintained up to date on both sides. This means that when a station is moved within a private LAN, it is necessary that the remote private LAN switch be informed of it and download up to date addresses mapping tables. Because of the tables updating problem, the encryption solution previously described seems easier to implement.

3 Modifications implied within the SSIE

The anonymity service introduction in [AFSEC] requires SSIE modifications, in particular the end-stations addresses encryption. The end-stations addresses may be encrypted either within the Confidentiality Section (see [AFSEC] section 6.2.4) or within the Extended Confidentiality Section in case contribution [AF-0803] is accepted. This implies the following modifications within [AFSEC] :

- **one additional security option indicating whether the anonymity service is supported** needs to be defined within the Security Service Specification Section. This is described in section 3.1.
- **a new field including the end-stations addresses** needs to be introduced either within the Confidentiality Section or within the Extended Confidentiality Section. Both of these solutions are described in sections 3.2 and 3.3.

Since the anonymity service applies only to the private LANs interconnection context, the SSIE needs only be considered by the private LAN ingress switches. Thus the SSIE should include the appropriate values for the following fields : scope and Target security entity ID.

3.1 The Security Service Specification Section

The Security Service Specification Section should indicate within the Security Service Specification Section whether the connection supports the anonymity service. To do that, the Anonymity Service Options section is defined and should be introduced in [AFSEC] as section 6.2.2.1.8 in case of contribution [AF-0803] acceptance, otherwise as section 6.2.2.1.7.

6.2.2.1.8. The Anonymity Service Options

This octet group indicates the presence of the End-stations addresses fields within the Confidentiality Section or the Extended Confidentiality Section.

Bits								
8	7	6	5	4	3	2	1	Octet(s)
1	0	0	1	1	0	0	0	
Anonymity Service Option Identifier								x.1
Anonymity Service Options								
x	x	x	x	x	x	x	x	x.2

Anonymity Service Options (Octet x.2)

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**Meaning**
0	0	0	0	0	0	0	0	Not Supported
0	0	0	0	0	0	0	1	Supported

3.2 The Confidentiality section

In case [AF-0803] is not accepted by the ATM Forum, the end-stations addresses need to be encrypted within the Confidentiality Section as the End-stations addresses field.

A section describing the End-stations addresses field needs to be inserted in [AFSEC] as section 6.2.4.5.

Bits								
8	7	6	5	4	3	2	1	Octet(s)
1	1	0	0	0	1	0	0	
Confidential Parameters Identifier								x.1
Master Key								x.2 etc
First Data Confidentiality Session Key								x.3 etc
First Data Integrity Session Key								x.4 etc
End-stations addresses								x.5 etc

6.2.4.5. End-stations addresses

This octet group contains the end-stations addresses.

Bits								
8	7	6	5	4	3	2	1	Octet(s)
1	1	0	0	1	0	1	1	
End-stations addresses Identifier								x.1
Length of End-stations addresses								x.2
Calling end-stations addresses Value								x.3
Called end-stations addresses Value								x.4

End-stations addresses Length (Octet x.2)

A binary number indicating the length in octets of the End-stations addresses Value contained in octets x.3, x.4, etc.

End-stations addresses Value (Octet x.3, x.4)

These fields contain the addresses of both the calling and called end-stations.

3.3 The Extended Confidentiality section

In case [AF-0803] is accepted by the ATM Forum, the end-stations addresses need to be encrypted within the Extended Confidentiality Section in the Confidential data field [AF97-0803] as the End-stations addresses field.

A section describing the End-stations addresses field needs to be inserted in [AFSEC] as section 6.2.5.2.

6.2.6.2. End-stations addresses

This octet group contains the end-stations addresses.

Bits								
8	7	6	5	4	3	2	1	Octet(s)
x	x	x	x	x	x	x	x	
Anonymity Service Identifier								x.1
Length of End-stations addresses								x.2
Calling end-stations addresses Value								x.3
Called end-stations addresses Value								x.4

End-stations addresses Length (Octet x.2)

A binary number indicating the length in octets of the End-stations addresses Value contained in octets x.3, x.4, etc.

End-stations addresses Value (Octet x.3, x.4)

These fields contain the addresses of both the calling and called end-stations.

4 Conclusion

In order to provide the anonymity service between two private LANs over the ATM public network, we propose that one global address per private LAN be defined and that end-stations addresses be encrypted either in the Confidentiality Section (see [AFSEC] section 6.2.4) or in the Extended Confidentiality Section in case of contribution [AF97-0803] acceptance. To do that, a new field indicating whether the connection considered supports the anonymity service should be introduced in the Security Service Specification Section ([AFSEC] section 6.2.2).

Besides end-users anonymity, the anonymity service allows to keep secret the private LANs' addresses mapping.

5 References

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

[AF97-0803] Maryline Laurent, Pierre Rolin, Laurent Stoffel, «Signaling Confidentiality», ATM Forum/97-0803, September 1997, Paris, France.