SAND98-1362C

ATM Forum Technical Committee
ATM Forum/98-xxxx

****

TITLE: Security Message Exchange Interoperability Scenarios

****

SOURCES:

Thomas Tarman[*]
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0806
USA
Phone: +1-505-844-4975
Fax: +1-505-844-2067
Email: tdtarma@sandia.gov

****

DATE: July, 1998 (Portland)

****

DISTRIBUTION: Security

****

ABSTRACT:

This contribution describes three interoperability scenarios for the ATM Security Message Exchange (SME) protocol. These scenarios include network-wide signaling support for the Security Services Information Element, partial signaling support where the SSIE is only supported in private or workgroup ATM networks, and the case where the SSIE is not supported by any network elements (except those that implement security services). Explanatory text is proposed for inclusion in Section 2.3 of the ATM Security Specification, Version 1.0.

****

NOTICE:

This contribution has been prepared to assist the ATM Forum. This proposal is made by Sandia National Laboratories as a basis of discussion. This contribution should not be construed as a binding proposal on Sandia. Specifically, the author and his company reserve the right to amend or modify the statements contained herein.

****

1 Introduction

At the Berlin meeting in April, some concern was expressed regarding the use of the Security Services Information Element (SSIE) to transport Security Message Exchange (SME) protocol messages in ATM signaling. Specifically, the concern was that ATM networks which do not implement the Signaling 4.0 Addendum for Security [1] would discard the SSIE since it is an unrecognized information element.

Early in the development of the ATM Forum Security Specification [2], this concern was expressed, and a protocol for the in-band exchange of SME protocol messages was developed. Since this protocol uses the

[*] This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible electronic image products. Images are produced from the best available original document.

user data connection for security message exchange between security agents, incompatibility issues with UNI and PNNI signaling are avoided. However, there exist instances where signaling-based security message exchange is useful. Therefore, a signaling-based approach was developed in parallel.

This contribution describes how the SME protocol can be used in three different UNI/PNNI signaling interoperability scenarios. These scenarios include the following:

1. The case where the entire network supports signaling-based SME
2. The case where private or workgroup ATM networks support SME, but must signal security messages across a network which does not provide SSIE transport, and
3. The case where no network elements (except security devices) support the SME protocol in signaling.

Descriptions for these scenarios are provided for inclusion in [2], Section 2.3 (Security Information Exchange), immediately following the first paragraph.

2 Specification Text

As stated earlier, signaling-based SME is used in networks that support the UNI 4.0 Security Addendum [***insert reference here***]. An example of SME usage in a network that supports the Security Addendum is shown in Figure 1 (where "UNI 4.0 + sec" and "PNNI 2.0 + sec" denote links that implement the UNI and PNNI security addenda). In this case, the end systems (with Security Agents) append the SSIE to the signaling message, and as the network establishes the call, the SSIE is passed without modification.

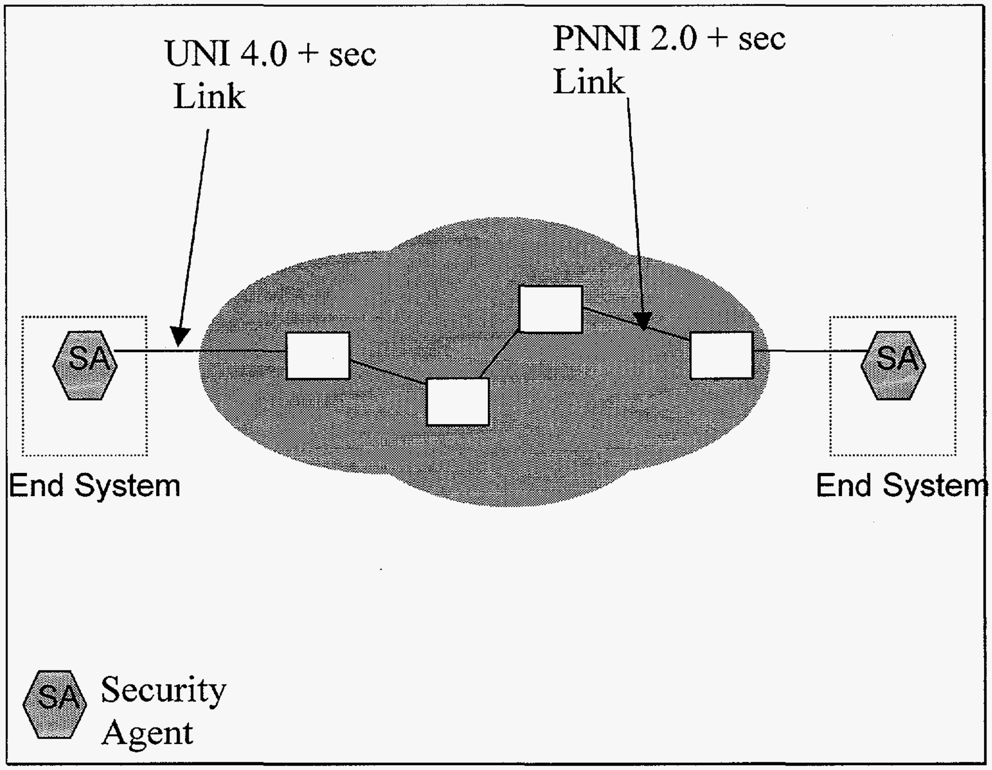

Figure 1: Entire Network Supports Signaling-Based SME

A more likely scenario is one that contains network elements that do not support signaling-based SME. An example of this scenario is shown in Figure 2.

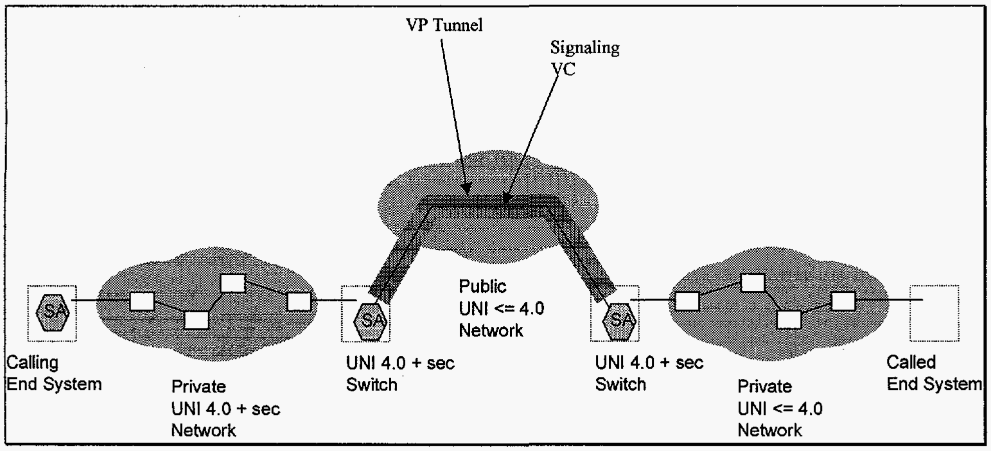

Figure 2: Portion of Network Does Not Support Signaling-Based SME

In this scenario, the calling endpoint is attached to a network that supports signaling-based SME. The security agent in this endpoint supplies security information along with the signaling message, and the message traverses the public network. When the message reaches the boundary UNI 4.0 + sec switch, it is signaled through a Virtual Path tunnel to the remote switch, which also supports signaling-based SME. Although the public network does not support signaling-based SME, the VP tunnel allows the two border switches to signal each other directly, and hence, allows SME to traverse the public network.

Since the remote switch contains a security agent that terminates the security association, the remaining network elements do not need to support signaling-based SME.

If none of the network elements are expected to support signaling-based SME, then the Inband SME protocol introduced earlier can be used instead. An example where this protocol should be used is illustrated in Figure 3.

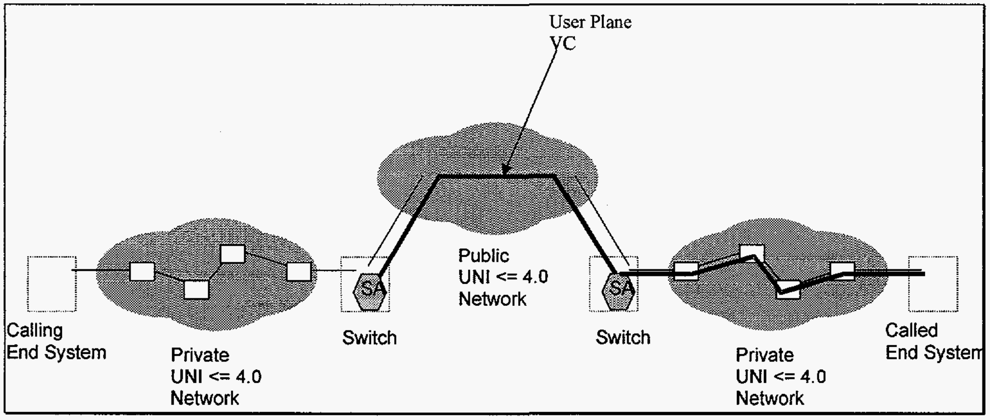

Figure 3: Using the Inband SME Protocol in Networks that do not Support Signaling-Based SME

In this case, the calling end system initiates the connection setup request, and the request propagates to the called end system as usual. As the call setup request progresses, the Security Agents do not augment the signaling messages with security information. As the connection confirmation signal propagates back from the called end system to the calling end system, the user plane virtual circuit is constructed along the way. When the user plane VC connects the two security agents, data transfers from the end systems are blocked, and the SAs perform the SME protocol within this virtual circuit. This protocol is described in more detail in Section 5.1.5.

Regardless of the SME method used, after the SME is completed, … [existing text from specification, section 2.3]

3 Motion

The motion is to incorporate this text in the ATM Security Specification, Section 2.3, immediately following the first paragraph.

4 References

1. The ATM Forum Technical Committee, Baseline Text for the UNI Signaling 4.0 Security Addendum, ATM Forum btd-cs-sec-01.02, Sept, 1997.
2. The ATM Forum Technical Committee, ATM Security Specification, Version 1.0 (Straw Ballot), ATM Forum str-sec-01.03 July, 1998.