CONF-951256--1

SAND95-2617C

ATM Forum Technical Committee
ATM Forum/95-1488

****

TITLE: Requirements for Signaling Channel Authentication

****

SOURCE: Thomas D. Tarman
Sandia National Laboratories*
P.O. Box 5800
Albuquerque, NM 87185-0451
Phone: (505)844-4975
Fax: (505)844-9641
E-mail: tdtarma@sandia.gov

* This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000

****

DATE: December 11, 1995

****

DISTRIBUTION: Security Working Group

****

ABSTRACT:

This contribution addresses requirements for ATM signaling channel authentication.

****

Notice:

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

****

Introduction

Signaling channel authentication is an ATM security service that binds an ATM signaling message to its source. By creating this binding, the message recipient, and even a third party, can confidently verify that the message originated from its claimed source. This provides a useful mechanism to mitigate a number of threats. For example, a denial of service attack which attempts to tear-down an active connection by surreptitiously injecting RELEASE or DROP PARTY messages could be easily thwarted when authenticity assurances are in place for the signaling channel. Signaling channel authentication could also be used to provide the required auditing information for accurate billing which is impervious to repudiation. Finally, depending on the signaling channel authentication mechanism, end-to-end integrity of the message (or at least part of it) can be provided. None of these capabilities exist in the current specifications.

Authentication for the signaling channel is unique from data authentication in that a signaling message has both end-to-end and hop-by-hop significance. The end-to-end nature of ATM signaling messages is obvious; a message is sent to a remote party indicating a request, a result, or an acknowledgment of an earlier message received. However, a signaling message also has hop-by-hop significance because each switch in an ATM network must examine the contents of the signaling message, make appropriate decisions, and if necessary, modify certain fields in the message. Since ATM signaling

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, makes 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 in electronic image products. Images are produced from the best available original document.

messages have hop-by-hop significance, end-to-end message integrity cannot be assured. This is true even for message fields that supposedly remain invariant, because the AAL 5 CRC is re-calculated at each hop (therefore, an intermediate system could modify a field in the message, re-calculate the CRC, and forward the message without detection of the modification). This property will have a significant impact on the design of a signaling channel authentication mechanism.

In addition to the technical constraints against signaling channel authentication, there are a number of political and organizational constraints as well. To formally document and implement security for an organization, a site security plan is typically drafted. This plan usually takes into account the assets to be protected, the expected threats against those assets, the strength of available protection mechanisms, and the performance requirements of the users to arrive at a security design which reduces risk to a satisfactory level. Since each organization has different security requirements, each site will likely want the opportunity to select from a variety of algorithms and/or protocols for their security designs. In addition to these organizational constraints, a number of political constraints exist as well. U.S. laws place restrictions on which encryption products may be exported. Although this applies to encryption and not authentication, certain authentication algorithms may be converted to encryption algorithms, making them subject to the same restrictions.

Requirements

The following requirements are the data channel authentication requirements that apply in the signaling channel case:

1. *The ATM signaling channel authentication framework shall protect against replay of earlier authenticated messages.*

2. *The ATM signaling channel authentication framework shall allow for the inclusion of service specific parameters in the message.*
   "Service specific parameters" include algorithm ID, key length(s), public parameters, etc. This addresses political and organizational constraints that were discussed in the introduction.

3. *The default ATM signaling channel authentication framework shall be based on asymmetric (public) key algorithms.*

4. *The ATM signaling channel authentication framework shall support end to end, switch to switch, and endpoint to switch authentication, even if intermediate entities do not support ATM security services.*
   This requirement implies the need for intermediate entities (such as switches) that do not implement ATM signaling channel authentication to pass authentication information anyway. This could be problematic if the default behavior for such devices does not allow this.

The following requirements are specific to signaling channel authentication:

5. *Upon receipt of a non-authentic message, a party that requires signaling channel authentication shall refuse any requested service and perform appropriate error reporting.*
   This is actually par of Requirement 1 of data channel authentication, but is broken out here. "Non-authentic" messages could be replayed messages, messages without authentication information, or messages that do not validate.

6. *The ATM signaling channel authentication framework shall support authentication algorithms in addition to the default.*
   These algorithms may be symmetric or asymmetric.

7. *The ATM signaling channel authentication framework shall allow injection of authentication information into a signaling message by any device that examines the message.*
   For auditing, route assurance, and perhaps debugging, it may be desired to have intermediates devices to "sign" the message after it is processed. The authentication framework shall not preclude this.

The following requirements are data channel authentication requirements that do not apply in the signaling channel case:

The ATM authentication framework shall provide an option for unilateral authentication. Authentication of signaling messages is inherently unilateral, so this requirement adds nothing.

The ATM authentication framework shall provide an option for mutual authentication. Again, signaling message authentication is inherently unilateral. If an endsystem requires that a response message contain authentication information, and the response is not authenticated, then the endsystem may reject the message and report an error (see Requirement 5).

If an instance of ATM authentication uses an existing signaling channel, then unilateral authentication shall be achieved with one signaling message, and mutual authentication shall be achieved with two signaling messages.
Once again, signaling message authentication is inherently unilateral.

The ATM authentication framework shall provide for the negotiation of optional mechanisms that use symmetric (private) key based algorithms.
While the use of other authentication algorithms is allowed (see Requirement 6), negotiation is outside of the scope of authentication of signaling messages.

The ATM authentication framework shall allow nested authentication.
This requirement is subsumed by Requirement 7.

The ATM authentication framework shall support authentication messaging in the signaling channel, and shall support additional authentication messaging in the data channel.
This contribution deals exclusively with the signaling channel.

Remarks

This contribution addressed the issue of requirements for signaling channel authentication. However, signaling channel authentication could also be used to provide *initial* authentication for the data channel, with additional measures needed for *data stream* authentication. As the Security Working Group begins to consider implementations, it may be worthwhile to investigate how leverage signaling channel authentication to avoid unnecessary duplication of (or worse yet, development of different approaches for) authentication mechanisms for each scenario.

Since signaling channel authentication mechanisms may be used to provide a portion of the data channel authentication service, it is suggested that the text currently in Section 5 (Security Services for the Signaling Channel) be located prior to the text which is currently located in Section 4 (Security Services for the Data Channel).

References

[1] T. Smith and J. Stidd, Xerox Corporation. "Requirements and Methodology for Authenticated Signaling." ATM Forum/94-1213. November 10, 1994.

[2] L. Pierson and T. Tarman, Sandia National Laboratories. "Requirements for Security Signaling." ATM Forum/95-0137. February 5 - 10, 1995.

[3] C. Kubic, J. Rutemiller, and G. Clark, U. S. Department of Defense. "Proposed Framework for ATM Security Services." ATM Forum/95-0783. June 5 - 9, 1995.