SAND98-2226C 754

ATM Forum Technical Committee
ATM Forum/ 98-0647

****

TITLE: UNI Signaling 4.0 Security Addendum: Call for Straw Ballot

****

SOURCE:

Carter Bullard
Bay Networks
320 Park Avenue
New York, New York 10022
+1 212 317-4230
cbullard@baynetworks.com

Thomas D. Tarman*
Sandia National Labs
P.O. Box 5800, M/S 0806
Albuquerque, NM 87185-080
+1-505-844-4975
tdtarma@sandia.gov

****

DATE: October, 1998, Gold Coast, Australia

****

DISTRIBUTION: Control Signaling (CS) Working Group

****

NOTICE: This contribution has been prepared to assist the ATM Forum. This proposal is made by the authors as a basis of discussion. This contribution should not be construed as a binding proposal on the authors or their companies. Specifically, the authors and their companies reserve the right to amend or modify the statements contained herein.

****

This contribution is intended to assist the ATM Forum CS Working Group in the process of bringing BTD-CS-UNI-SEC-01.04 DRAFT and BTD-CS-PNNI-SEC-01.02 DRAFT to Straw Ballot.

* 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.

1. Introduction

The ATM Forum UNI 4.0 Security Addendum has undergone 4 revisions and has been without substantive modifications for 3 ATM Forum meetings. This contribution is intended to assist the ATM Forum CS Working Group in the process of bringing BTD-CS-UNI-SEC-01.04 DRAFT to Straw Ballot. This effort applies equally to its companion document, BTD-CS-PNNI-SEC-01.02 DRAFT.

BTD-CS-UNI-SEC-01.04 DRAFT is an addendum to UNI 4.0 Signaling that describes the additional procedures needed of ATM signaling to support the signaling-based security message exchange protocol, and its 4 basic security mechanisms, authentication, confidentiality, integrity and access control for ATM VC/VPs. These services are specified in detail in ATM Forum document **af-sec-0100.000**, which is currently in Final Ballot.

The remaining identified work for BTD-CS-UNI-SEC-01.04 DRAFT includes the resolution of the TBD items in the draft, and a review of the sections of the ATM Forum Security Specification V1.0 **af-sec-0100.000**, that are specifically referenced by BTD-CS-UNI-SEC-01.04 DRAFT.

In support of this effort, this contribution includes the relevant baseline text of the referenced sections of that Security Specification.

2. Motions

This contribution has two (2) motions, and two (2) supporting motions intended to advance BTD-CS-UNI-SEC-01.04 DRAFT and its companion document, BTD-CS-PNNI-SEC-01.02 DRAFT to straw ballot.

1. Move to resolve the **TBD** issues in BTD-CS-UNI-SEC-01.04 DRAFT.

    a. Move to acquire/allocate an Information Element code point for the Security Services Information Element (SSIE) described in BTD-CS-UNI-SEC-01.04 DRAFT.

    b. Move to acquire/allocate a Cause code point for the "Security Service Failure" condition.

This effort will resolve all TBD's in both BTD-CS-UNI-SEC-01.04 DRAFT and BTD-CS-PNNI-SEC-01.02 DRAFT.

2. Move to present to the closing plenary the UNI Signaling 4.0 Security Addendum, BTD-CS-UNI-SEC-01.04 DRAFT, and the PNNI Signaling Security Addendum, BTD-CS-PNNI-SEC-01.02 DRAFT, to be considered for Straw Ballot.

In support of primary motion #2, this contribution contains the relevant baseline text of the ATM Forum Security Specification V1.0 that is directly referenced in both the UNI Signaling 4.0 Security Addendum and the PNNI Signaling 1.0 Security Addendum.

3. Referenced Sections

BTD-CS-UNI-SEC-01.04 DRAFT explicitly references these sections of **af-sec-0100.000**:

1. **Section 2** *Top-Level Reference Model*s (1° reference in section 11.1)
2. **Section 4** *Security Services for the Control Plane* (1° reference in section 11.1.2)
3. **Section 5.1.3** *Security Services Information Element* (1° reference in section 11.2.3.1)
4. **Section 5.1.3.2** *Security Association Section* (1° reference in section 11.2.3.1)
5. **Section 5.1.4.4** *Security Agent Procedures for Signaling-Based Message Exchange* (1° reference in section 11. 3.1)
6. **Section 5.1.4.4.2.1** *Initiating Security Agent Procedures: Call/Connection Request* (1° reference in section 11.3.2.1.1)
7. **Section 5.1.5.1** *Security Message Exchange for Signaled Point-to-Point Connections* (1° reference in section 11.3.2.1.1)
8. **Section 5.1.3.2.10** *Security Service Data Section* (1° reference in section 11.3.2.1.1)
9. **Section 6.2** *SECURITY SERVICE DATA PRIMITIVES* (1° reference in section 11.3.2.1.1)
10. **Section 5.1.4.4.3.1** *Responding Security Agent Procedures: Call/Connection Request* (1° reference in section 11.3.2.1.1)
11. **Section 5.1.4.4.2.2** *Initiating Security Agent Procedures: Call/Connection Acceptance* (1° reference in section 11.3.2.1.2)
12. **Section 5.1.6** *Security Information Exchange Error Processing* (1° reference in section 11.3.2.1.3)
13. **Section 5.1.4.4.3.2** *Responding Security Agent Procedures: Call/Connection Acceptance* (1° reference in section 11.3.2.2.1)
14. **Informative Annex 7.3** *SECURITY SERVICES INFORMATION ELEMENT EXAMPLES* (1° reference in section A.4)

These references can be classified into three areas:

1. Concept Development.

   References 1, 2, 4, 7

2. Security Information Element Formats and Examples

   References 3, 8, 9, 14

3. Security Agent Procedures.

   References 5, 6, 7, 10, 11, 12, 13

The issues outstanding in the ATM Forum CS working group are focused primarily on Security Agent procedures within the control plane. To support this effort, this contribution focuses on the BTD-CS-UNI-SEC-01.04 DRAFT references that relate to the UNI 4.0 signaling entity procedures, by providing the baseline text of the ATM Forum Security Specification that address Security Agent Procedures for the control plane, and sections that describe diagnostic return codes. All of these references are in some measure also found in BTD-CS-PNNI-SEC-01.02 DRAFT, and so this effort should address the outstanding issues found in that document as well.

3.1 Security Agent Procedures

BTD-CS-UNI-SEC-01.04 DRAFT references specific subsections of **Section 5.1.4** . ***Message Exchange within UNI 4.0 Signaling*** and **Section 5.1.5.** ***Message Exchange within the User Plane*** of **af-sec-0100.000**. These sections describe the procedures of the ATM Forum Security Agent that are needed to process the Security Services Information Element (SSIE). Although the entire sections are of interest to the implementor, specific sections referenced in BTD-CS-UNI-SEC-01.04 DRAFT are of particular interest to implementors of signaling procedures in the control plane.

With regard to signaling entity procedures, BTD-CS-UNI-SEC-01.04 DRAFT references **Section 5.1.4.4.** ***Security Agent Procedures for Signaling-Based Message Exchange***, specifically the subsections **Section 5.1.4.4.2.1, Section 5.1.4.4.2.2, Section 5.1.4.4.3.1 and Section 5.1.4.4.3.2** of **af-sec-0100.000**. These sections specify the Initiating and Responding Security Agent procedures for Call/Connection Request and Call/Connection Acceptance.

The baseline text of these specific sections is included below.

[Begin included text from af-sec-0100.000]

5 Support Services

5.1 Security Information Exchange

5.1.4 Message Exchange within UNI 4.0 Signaling

5.1.4.4 Security Agent Procedures for Signaling-Based Message Exchange

5.1.4.4.1 General Procedures

The general security procedures shall apply for all procedures defined in Section 5.1.4.4.

Refer to Section 1.3 for definition of "Security Agent".

Security Association Sections (SAS) within the SSIE are processed as 'atomic' entities, and so are processed to completion prior to processing of subsequent SASs.

Security agents, when modifying information elements in the signaled message shall conform to the procedures that govern the format and behavior of the object information elements. Specifically, the relevant procedures described in UNI 4.0 [3], Q.2931 [20], and Q.2971 [21] shall apply.

In the case where errors occur during processing and the security service cannot be performed or established, the VC must not be allowed to support the transmission of User Data. The VC should be cleared with appropriate cause codes and diagnostics.

5.1.4.4.2 Initiating Security Agent Procedures

5.1.4.4.2.1 Call/Connection Request

Upon receipt of a SETUP message by an initiating ATM security agent, all SSIE Security Association Sections that are present in the signaled message are parsed and the greatest Relative ID Security Association ID is noted. If there are no SSIE SASs present, the greatest Relative ID is zero.

Based on the security service that the security agent is to provide, the initiating security agent generates the appropriate Security Association Sections (SAS) for inclusion in the message, providing all mandatory fields that may be required. The initiating SA will ensure that:

1. The Version number for all ATM Forum Version 1.0 Security Services is zero.

2. The transport method is chosen and indicated in the Transport Indicator field, using the guidelines specified in Section 5.1.3.2.4 of this document.

3. The Security Message Exchange State is set to zero. This indicates that this SAS contains information for FLOW1 of the two-way or three-way message exchange protocol.

4. If the SAS is intended for only one security agent, then the **Discard** bit is set to 1. Generally, label based access control services can be intended for more than one target security agent, and so for these services the **Discard** bit may be set to zero.

5. If the security agent intends to use an explicit Target Security Agent Identifier to identify the intended target security agent, the **Explicit** Scope bit is set and an optional **Target Security Entity Identifier** is included in the SAS header.

   If the Target Security Entity Identifier is not used, then an appropriate **Scope** description is selected to identify the **Region** and **Role** of the intended target security agent. Details on the use of this field are specified in Section 5.1.3.2.7.

6. The security agent allocates a new **Security Association ID** value for the security services SAS, as described in Section 5.1.3.2.8. The Security Association ID is noted and is used to identify the corresponding SSIE SAS in the expected CONNECT message.

7. Each Security Association Section is given a **SAS Number** that specifies the precedence order for processing SASs within the same Security Association. SASs will be processed in descending order. The order of processing SASs with the same SAS Number is undetermined.

If an SSIE does not already exist in the SETUP message, an SSIE header is prepended to the SASs that are to be added to the message. The new SASs are then added to the signaled message accordingly.

If any error occurs in processing, the security agent should return the failure condition "Security Protocol Processing Error" (see Section 5.1.6), with an appropriate diagnostic for the condition that generated the error.

At this point, the message is returned to the signaling entity.

5.1.4.4.2.2 Call/Connection Acceptance

Upon receipt of a CONNECT message by an initiating ATM security agent, all SSIE Security Association Sections that are present in the signaled message are parsed and those SASs that have Relative ID Security Association IDs that match those being supported by this security agent are processed. If there are no SSIE SASs present that match any expected Relative ID Security Association IDs, then an error has occurred and the security agent will return the failure condition, "Missing Required Security Information Element" (see Section 5.1.6). If only a partial set of expected Relative ID Security Association IDs is present in the CONNECT message, then the initiating SA shall determine if the call should be in error. This decision is based on the SASs received and the initiating SA's security policy.

If there is no SSIE present then the initiating SA shall determine if the call should be in error. This decision is based on the initiating SA's security policy. If the SASs are unresolved or partially resolved the initiating SA can revert to in-band message exchange to establish the security service.

The initiating security agent processes all matching SASs, in descending order based on the 8 bit Relative ID. If an error occurs during processing, the security agent will return the failure condition "Security Protocol Processing Failure".

For each SAS, the initiating security agent processes the contents of the SAS to completion. If the processing completes successfully, then the initiating security agent may perform additional processing, depending on the value of the Transport Indicator field. If the Transport Indicator is Signaling-Based messaging, then no additional processing is performed. If the Transport Indicator is In-Band Messaging, then the initiating security agent performs the In Band Security Message Exchange as outlined in Section 5.1.5. If an error occurs during extended SME processing, the security agent will return the failure condition "Security Protocol Processing Failure". Upon successful completion of the extended SME, the initiating security agent processes the next appropriate SAS.

At this point, the message is returned to the signaling entity.

5.1.4.4.3 Responding Security Agent Procedures

5.1.4.4.3.1 Call/Connection Request

Upon receipt of a SETUP message by a responding security agent, if an SSIE is present, all SSIE Security Association Sections that are present in the signaled message are parsed and the SASs that are intended for this security agent are collected. The security agent selects all the appropriate SSIE SAS's based on either the explicitly specified **Target Security Entity Identifier** or based on the **Region** and **Role** bits of the SAS **Scope** field, using the procedures described in Section 5.1.3.2.7. From this collection, SASs that have a **Security Service Identifier** that match a security service that can be provided by this security agent are retained. All other SASs are left unmodified. If the SETUP message does not contain a required SSIE or a required SAS, the security agent, based on policy, will either revert to in-band message exchange to establish the security service or reject the call and return an appropriate error condition and the signaling entity will clear the call with the failure condition "Missing Required Information Element" (see Section 5.1.6).

The responding security agent processes all matching SASs, in descending order based on the SAS's 8 bit Relative ID. If an error occurs during processing, the security agent will return the failure condition "Security Protocol Processing Failure".

For each new Security Association ID number encountered in the collection of appropriate SASs, a new security association is allocated, and subsequently referenced by Security Association ID number. All SASs with the same Security Association ID are processed within the same security association context, and are processed in descending order based on SAS number. SASs with identical 8 bit Security Association ID numbers are processed in undetermined order.

Each SAS is processed to completion, before processing can proceed to the next SAS.

Any subsequent flows or responses to processed SASs are held, pending the arrival of the appropriate CONNECT message for this VC.

If the **Discard** bit in the Scope field is set (1), the security agent removes the SAS from the SSIE, the security agent adjusts the SSIE length. If no other SASs remain, the SSIE is removed from the signaled message. If the **Discard** bit is zero (0), the SAS is retained, unmodified, in the signaled message.

At this point, the message is returned to the signaling entity.

5.1.4.4.3.2 Call/Connection Acceptance

Upon receipt of a CONNECT message by a responding security agent, all SSIE Security Association Sections that are present in the signaled message are parsed and the greatest Relative ID Security Association ID is noted. If there are no SSIE SASs present, the greatest Relative ID is zero. The security agent determines that the Relative ID of any pending second (2nd) flow or response SASs are not less than the greatest observed Relative ID in the current message. Once this is done, the security agent builds one or more SASs (with the Flow Indicator set to 1 to indicate a FLOW2 message), and adds or appends the pending SASs to the SSIE. If any processing errors occur, the security agent will return an appropriate error condition and the signaling entity will clear the call with the failure condition "Security Protocol Processing Failure" (see Section 5.1.6).

At this point, the message is returned to the signaling entity.

5.1.4.5 Endpoint requests for security services

An endpoint or host that does not provide security services may (as an option) request security services from a downstream security agent as follows:

1. Insert a Security Services Information Element into the SETUP message on the signaling channel.

2. Set the security message exchange protocol to the unspecified codepoint ('0 0').

3. Insert any combination of the following optional fields, indicating the desired service(s) and/or algorithm(s):
   - Security service declaration
   - Data confidentiality algorithm
   - Data integrity algorithm
   - Hash algorithm
   - Signature algorithm
   - Key exchange algorithm
   - Session key update algorithm
   - Access control algorithm
   - Multiple algorithms may be inserted in preference order for each requested security service

Upon receipt of such a request, the security agent replaces the Security Services Information Element with one of its own choosing, based on its security policy. A security agent is under no obligation to use the options requested by the endpoint or host. It should be noted that this process is not secure, and that a trusted link between the endpoint and security agent is assumed.

5.1.4.6 Acknowledgements to endpoints requesting security services

A security agent shall acknowledge a security request received from an endpoint as follows:

1. Insert a Security Services Information Element into the CONNECT message on the signaling channel.

2. Set the security message exchange protocol to the unspecified codepoint ('0 0').

3. Indicate which service(s) and/or algorithm(s) were negotiated by the security agents, for only those instances where a specific request was made.

The endpoint or host would then have the option of rejecting the call if it did not get the service(s) and/or algorithm(s) it desired.

[End included text from af-sec-0100.000]

3.2 Diagnostics

BTD-CS-UNI-SEC-01.04 DRAFT references specific subsections of section 5.1.6 in **af-sec-0100.000.** This section specifies error-processing procedures for the security agent. The baseline text is included below.

[Begin included text from af-sec-0100.000]

5.1.5 Message Exchange within the User Plane

5.1.6 Security Information Exchange Error Processing

The following text applies when security message exchange occurs in UNI 4.0 signaling, in-band, or both.

When errors occur in establishing or maintaining a security service on a specific VC, the VC must be put into a state where User Data transport is not supported. For establishing or established VC's this is accomplished by clearing the call. When clearing a call based on failure of a security agent to establish or maintain a security service, an appropriate Cause code will be chosen by the security agent that is involved with the fault, and a diagnostic is provided that provides adequate information of the peer security agent to understand the nature of the fault condition.

Security diagnostics are specific to the types of error conditions that can happen within a security agent and are limited to 28 bytes in length. The amount of information that is disclosed in a security agent diagnostic may have a security impact, and as such each diagnostic has a mandatory section and optional sections that provide more detail on the condition that generated the error.

1. Missing Required Security Information Element.

   When this error condition occurs, the call is cleared with Cause code # 96 "Mandatory Information Element Missing" (see Q.2931 **[20]**), and the diagnostic will be at most 28 bytes of a valid SSIE. A 4 byte SSIE header is mandatory. Optionally, the diagnostic can contain valid SAS segments that will declare to the originator, the type of security service that is required by the security agent. When providing SASs, the security agent can use existing fields to provide additional information, such as the security agents region and role bits.

2. Security Protocol Processing Error.

   When this error condition occurs, the call is cleared with Cause code # **TBD** "Security Services Failure" (see Q.2931 **[20]**), and the diagnostic will be at most 28 bytes of a valid SSIE. A 4 byte SSIE header is mandatory. Optionally, the diagnostic can contain valid SAS segments which will indicate which SAS was being acted on when the processing error occurred. The SAS may include the Relative ID of the SAS that generated the error.

3. Security Policy Violation

   When this error condition occurs, the call is cleared with Cause code #**TBD** " Security Services Failure", and the diagnostic will be at most 28 bytes of a valid SSIE. This diagnostic should contain valid SAS segments which indicate the service that is not allowable based on the security policy that was violated. The SAS may include the Relative ID of the SAS that generated the error.

   Reporting this specific error condition is optional, as local policy may want to minimize the amount of information disclosed when a security error occurs. When reporting this specific error condition is not possible, a general "Security Protocol Processing Error" should be reported.

[End included text from af-sec-0100.000]

4.0 References

ATM Forum Technical Committee, "B-ICI Specification, Version 2.0".

[3] ATM Forum Technical Committee, “User-Network Interface (UNI) Signalling Specification”, Version 4.0, April 1996.

[20] ITU-T Recommendation Q.2931, "B-ISDN DSS2 User-Network Interface Layer 3 Specification for Basic Call/Connection Control", February, 1995.

[21] ITU-T Recommendation Q.2971, "B-ISDN DSS2 User-Network Interface Layer 3 Specification for Point-to-Multipoint Call/Connection Control", 1995.