SAND2000-0885C

ATM Forum Technical Committee
ATM Forum/00-0161

****

TITLE: Sandia's Straw Ballot Comments on the Security Version 1.1 Specification

****

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: May, 2000 (San Francisco)

****

DISTRIBUTION: Security

****

ABSTRACT:

This contribution provides Sandia's straw ballot comments for the Security Version 1.1 specification, STR-SEC-02.01. Two major comments are addressed here that pertain to potential problems with the use of the Security Association Section digital signature, and potential inconsistencies with the allocation of relative identifiers in the initiating security agent.

****

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

This contribution provides Sandia's comments to the ATM Forum Security 1.1 straw ballot specification, STR-SECURITY-02.01. These comments are organized as follows – major comments indicate potential technical defects in the specification which, if not resolved, may preclude Sandia's vote in favor of the specification. Minor comments are technical comments which, if left unresolved, will not preclude Sandia's favorable vote. Finally, editorial comments are also provided.

* 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.

2. Major Comments

5.1.3.2.4: Transport Indicator

- Second paragraph: this paragraph states that intermediate or responding security agents may modify the transport indicator. If the Security Association Section (SAS) has an SAS digital signature, then the digital signature is broken. This indicates a need to clarify the role of the SAS digital signature (see section 7.4.6) -- is it a mechanism to protect the integrity of the SAS when it is **first generated**, or when it was **last modified**?

Section 5.1.3.2.8: Relative Identifier

- Editor's note: There is an inconsistency between the procedures for allocating new Security Association IDs and checking for "wrap around". Furthermore, it is not clear what "conditions exist where the next allocated Security Association ID" should be greater than one plus the largest one in the list. The stated example where a security agent is both an initiator and responder does not provide a clear example where this behavior is desired. Therefore, in the absence of a clear example, the following changes are proposed which will address the inconsistency. These changes are intended for the paragraph above the editor's note:

  - change "greater than all existing Security Association IDs." to "the largest Security Association ID plus 1."
  - delete that last two sentences of this paragraph.

  Note that if these changes are **not** desired, then the procedure for dealing with wrap-around of the 8-bit unsigned add operation needs to be re-worded to make consistent with this fact.

3. Minor Comments

Section 5: Support Services

- Paragraphs 3 and 4 : change "connection" and "call" to "security association"
- Paragraph 8: change "This method applies to SVCs and PVCs..." to "This method applies to SVCs, PVCs, and PVPs..."

Section 5.1.1: Security Message Exchange and Negotiation Protocols

- Paragraph 1: when calling out ISO/IEC 9594-8 and ISO/IEC 11770-2, include the following references in Section 1.2.1:
  [19] ISO/IEC 9594-8
  [TBD] ISO/IEC 11770-2, "Information Technology – Security Techniques – Key Management – Part 2: Mechanisms using Symmetric Techniques," 1996.
- Paragraph 4: change "connection" to "security association."
- Description of token Tx: the text that states "Because this time stamp wraps around..." should be a parenthetical note.
- Description of token SecNeg_: the text that states "Options **should** be presented in order of preference." should be changed to "Options **shall** be presented in order of preference."
- Description of token ConfPar_": is this consistent with the text in Section 5.2?
- Description of token Cert: change "In the three-way security message exchange protocol, ..." to "In the in-band security message exchange protocol, ..."

Section 5.1.1.2: Two-Way Security Message Exchange Protocol

- Paragraph 3: in its second occurrence, change "Section 5.1.4" to "Section 5.1.6."

Section 5.1.3: Security Services Information Element

- Paragraph 2: delete "along with support for other exchange mechanisms described in Section 5.2."

Section 5.1.3.2.2: Length of Security Association Section

- Heading: change to "Security Association Section Length"
- Table: change "Length of Security Association Section" to "Security Association Section Length."

Section 5.1.3.2.5: Flow Indicator

- Third paragraph: delete this paragraph because it is redundant.

Section 5.1.3.2.6: Security Association Section Discard Indicator

- First paragraph: change "...whether a security agent will discard..." to "... whether a peer security agent should discard..."
- Second paragraph: change "... SAS should be discarded after processing." to "... SAS should be discarded by the peer security agent after processing."

Section 5.1.3.2.7: Scope

- Throughout this section and subsections: text and headings imply that non-explicit addressing may only be used for addressing peer security agents (i.e., responders). However, the fourth example implies that it is permitted for an end system to use non-explicit addressing to address a proxy security agent. I believe that this usage is acceptable. Therefore, throughout this section and subsections, remove the word "peer", and state in the first paragraph that non-explicit addressing is used for peer (responder) addressing as well as addressing proxies.

Section 5.1.3.2.7.1: Explicit Security Peer Specification

- Second paragraph: add the following text to this sentence -- "..., and the Target Security Agent Identifier field is coded with the target security agent identifer for this SAS (Section 5.1.3.2.9)."
- Third paragraph: change "... an appropriate SSIE SAS type has been employed that provides..." to "... an appropriate SAS Authentication Section (Section 7.4) and the appropriate SA identifiers (Section 7.1) are employed that provide..."

Section 5.1.3.2.9: Target Security Agent Identifier

- Editor's note: the Security Agent Distinguished Name is only used for explicit addressing (see section 7.1.3). Therefore, if FLOW-1 does not contain an identifier for "B" (e.g., three-way exchange), then the Target Security Agent Identifier field is coded according to the syntax in section 7.1.3. However, if FLOW-1 contains an identifier for "B", then B's ID is coded as a Responder Distinguished Name (section 7.1.2), and is contained in BOTH the Target Security Agent Identifier and the Security Agent Identification Section. Delete editor's note and add some text that clarifies this.

Section 5.1.3.2.10.2: Label-based Access Control Section

- Editor's note: this ed. note needs to be resolved, however, it's purpose is not clear.

Section 5.1.4.4.1: General Procedures

- Paragraph two: also refer to section 2.3 for definitions of SAsme, etc.

Section 5.1.4.4.2.1: Call/connection Request

- Step two: change "Security Message Exchange State" to "Flow Indicator."

Section 5.1.4.5: Endpoint Requests for Security Services

- Bulleted list of fields: insert the following section cross-references:
  - Security service declaration (Section 7.2.1)
  - Data confidentiality algorithm (Section 7.2.3.1)
  - Data integrity algorithm (Section 7.2.3.2)
  - Hash algorithm (Section 7.2.3.3)
  - Signature algorithm (Section 7.2.3.4)
  - Key exchange algorithm (Section 7.2.3.5)
  - Session key update algorithm (Section 7.2.3.6)
  - Access control algorithm (Section 5.1.3.2.10.2)

Section 5.2.3.1: Master Keys on Point-to-Point Connections

- Second paragraph: change second sentence to "The Master Key octet group is not required, and will not be included in the Confidential Parameters, and will be ignored if received." At the end of this paragraph, include pointer to section 8.6.4.1 (which describes Diffie Hellman procedures).

Section 7.1: Security Agent Identifiers

- First paragraph: this section is really describing the "Security Agent Identification Section" (see section 5.1.3.2.10.1). However, unlike other "sections", this section does not contain a section identifier. Nevertheless, these Distinguished Name fields need to be related to their appropriate sections in the SAS. Therefore, the Initiator Distinguished Name and Responder Distinguished Name descriptions should have pointers to Section 5.1.3.2.10.1: Security Message Exchange Data Section, and the Security Agent Distinguished Name should have a pointer to Section 5.1.3.2.9: Target Security Agent Identifier.

Section 7.2.2: Security Service Options Section

- First paragraph: add text that states that this section is used for negotiation.
- Second paragraph: no negotiation is possible with the two-way protocol (see section 5.1). In the two-way protocol, security service options are specified by the initiator, and the responder can only choose

to either accept the call, or reject it. Therefore, change this paragraph as follows:
"In the 2-way exchange, the initiator shall indicate which security services are required. The responder shall decide if the security services specification, and accept the call if the specification is suitable, or reject it if not."

- Third paragraph: change second sentence to read "For each service **required or** supported, ..."

Section 7.3: Confidentiality Section

- Description for "Confidential Data": make "encrypted data" bold.

Section 7.4.5.1.1: FLOW1-2WE

- Table entry for {ConfPara}: delete "formatted as."

Section 7.4.5.1.2: FLOW2-2WE

- Table entry for {ConfPara}: delete "formatted as."

Section 7.4.5.2.1: FLOW2-3WE

- Table entry for {ConfPara}: delete "formatted as."

Section 7.4.5.2.2: FLOW3-3WE

- Table entry for {ConfPara}: delete "formatted as."

Section 7.4.6: SAS Digital Signature

- Description of Digital Signature Value: see major comment on Section 5.1.3.2.4.

4. Editorial Comments

Section 5: Support Services

- Paragraph 5: space is needed in "... Section5.1.4..."
- Paragraph 9: space is needed in "... Section5.1.5..."

Section 5.1.1: Security Message Exchange and Negotiation Protocols

- Third and fourth paragraphs after box: put carriage returns after these paragraphs

Section 5.1.1.1: Three-way Security Message Exchange Protocol

- Step 5: change "Sig)" to "Sig(...)"

Section 5.1.1.2: Two-Way Security Message Exchange Protocol

- Figure 21: fix size of figure

Section 5.1.3.1: Security Services Information Element Format

- First paragraph: change "This specification defines the Security Services Information Element (SSIE)." to "This specification defines the contents of the Security Services Information Element (SSIE)."
- First paragraph: change "Octets 1-4 of this IE are ..." to "The header octets of this IE (octets 1-4) are ..."

Section 5.1.3.2.6: Security Association Section Discard Indicator

- Second and third paragraphs: need carriage return between these paragraphs.

Section 5.1.3.2.7.3: Relative ID Security Peer Specification

- First paragraph: change "... set to zero (0)." to "... coded as zero (0)."

Section 5.1.3.2.8: Relative Identifier

- Table: insert solid line between Relative ID and Security Association ID rows.
- SAS Number description and elsewhere: is "nibble" the standard terminology?
- Second paragraph: change "SAs" to "security agents", and insert space in "VCthere"
- Last paragraph: insert carriage return between this and the previous paragraph.

Section 5.1.4.4.2.1: Call/connection Request

- Editor's note: change "()" to "[]" for this and other relevant editor's notes. This aids in searching for outstanding ed. notes.

Section 5.1.4.4.3.1: Call/connection Request

- Third paragraph: delete stray "-" in front of "12 bit Relative ID numbers".

Section 7.1: Security Agent Identifiers

- First paragraph: needs space in "targetingsecurity."