ATNP/WG3

WP/15-38

17/01/99

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL(ATNP)

WORKING GROUP 3 - APPLICATIONS AND UPPER LAYERS

Honolulu, 19-22 January 1999 (fifteenth meeting)

Agenda Item 5.4 : Ground-Ground Post Package 1work

WP/15-38 : AMHS Security operation using Security Class S0

Presented by Jean-Marc Vacher (France)

Prepared by ATNP WG3/SG1

Summary

The goal of this paper is to provide WG3 with the status of the work on AMHS Security, as performed in WG3/SG1 and endorsed by WG1/SG2.

Based on the existing threats analysis for the AMHS, endorsed by WG3 in Rio de Janeiro, in its 16th meeting (Bordeaux, October 1998) WG3/SG1 has selected a security profile, which is defined in the MHS ISO/IEC ISPs 10611 and 12062. This profile corresponds to the (security) SEC Optional Functional Group, implementing Security-Class S0.

The choice of S0 has been made based on the attached WG3/SG1 paper, which has been endorsed by the subgroup. This paper has then been presented in WG1/SG2 in its 9th meeting (Bordeaux, October 1998), as WP9/10. In its 10th meeting (Phoenix, December 1998), WG1/SG2 has endorsed the proposed approach and confirmed that it is in line and compatible with the general guidelines adopted by the Security subgroup. An additional conclusion was that any party willing that more functionalities be included in the AMHS Security should provide a written description of its requirements.

WG3 is invited to comment, if needed, the approach retained by WG3/SG1 and WG1/SG2, and to endorse the principles proposed for AMHS Security in the context of the Extended ATS Message Service ("Package-2" enhancements to the AMHS).

ATNP/WG3/SG1

WP/225 Rev. 1

06/10/98

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL(ATNP)

WORKING GROUP 3 - APPLICATIONS AND UPPER LAYERS

SUBGROUP 1 - GROUND APPLICATIONS SUBGROUP

Bordeaux, 5-8 October 1998 (sixteenth meeting)

Agenda Item 3 : ATS Message Handling Services

WP/225 Rev. 1: AMHS Security operation using Security Class S0

Presented by Jean-Marc Vacher (France)

Commented by WG3/SG1 (and updated accordingly)

Summary

The goal of this paper is to study the implications of selecting the MHS ISP Security Class S0 for the Extended ATS Message Service, as far as AMHS security is concerned.

The subgroup is invited to adopt security class S0 for the AMHS security in the Extended ATS Message Service.

Table of contents

References

[1] ATNP/WG3/SG1 WP/208, Refined Security Approach for the ATS Message Service - Jean-Marc Vacher, 15th SG1 meeting, Toulouse, 2-4 September 1998

[2] ISO/IEC 10021-2:1990. Information Technology - Text Communication - Message-Oriented Text Interchange System (MOTIS) - Part 2: Overall Architecture.

[3] ISO/IEC ISP 10611-1:1994. Information Technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging - Part 1: MHS Service Support.

[4] ISO/IEC ISP 10611-3:1994. Information Technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging - Part 3: AMH11-Message Transfer (P1).

[5] ISO/IEC ISP 10611-4:1994. Information Technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging - Part 4: AMH12-MTS Access (P3).

[6] ATNP/WG3/SG1 WP/221, Technical implications of selecting Security Class S1 for the Extended ATS Message Service - Jean-Marc Vacher, 16th SG1 meeting, Bordeaux, 5-8 October 1998

[7] X.509

1. INTRODUCTION

A refined security approach for the ATS Message Service has been proposed in WG3/SG1 WP/208 [1], presented at the 15th SG1 meeting in Toulouse (2-4 September 1998).

WP/208 proposed for the security approach, in terms of security functions to be implemented, the combination of a profile aligned on the ISO/IEC MHS ISPs, mandating the Optional Functional Group SEC with security class S0 or S1, and of bespoke countermeasures against message flooding and Denial of Service.

WP/221 recommends, based on interoperability constraints with CNS/ATM-1 Package, that the Optional Functional Group SEC with security class S0 be mandated for the Extended ATS Message service.

This paper aims at providing the subgroup with a view on what the technical, practical and operational implications of security class S0 would be.

2. TECHNICAL BACKGROUND

2.1 Definition of Security Class S0

2.1.1 Specification in terms of Elements of Service

ISO/IEC ISP 10611-1 [3] defines a Security optional functional group (FG) for the provision of secure messaging. It specifies security class S0 as a subset of the security features available in the MHS base standards:

S0 This security class only requires security functions which are applicable between MTS-users, i.e. UA to UA in the AMHS. Security mechanisms are implemented within the MTS-user. An MTA is not expected to understand the semantics of the security services, but only to support their syntax on submission and delivery.

Table 1 (extracted from [3]) summarises the requirements of security class S0 on an MTS-user and on an MTA.

Table 1 - Overview of SEC FG security class S0

Security Class	MTS-user	MTA
Basic		Supports relay of security EoS
S0	Content Integrity Proof of delivery Origin authentication (end-to-end)[1] Message Sequence Integrity[2]	Supports submission and delivery of security EoS

[1] only provided to the message recipient (using the Message Argument Integrity security element)

[2] however considered as a local matter in the ISP

2.1.2 Specification of message elements (ISPICS)

In terms of message elements, the impact of S0 on the ISP profiles is the following :

- The support and use (requirement on dynamic behaviour) of credentials is mandated for MTABind (MTA to MTA) and MTSBind (MTS-user to MTS). However strong credentials is not mandated, so simple credentials, i.e. a password, is sufficient.

- The support for origination and reception (including semantical understanding) of the P1/P3/P7 parameters associated with the EoS mentioned above (Content Integrity, Proof of Delivery, End-to-End Origin Authentication) is mandated for MTS-Users (i.e. UA or MS). This support is only a static requirement (no need to always use it). *(for more details see AMH12 ISPICS in ref. [5])* This implies :

    1. Support of content-integrity-check

    2. Support of proof-of-delivery-request

    3. Support of message-token, including the signed-data component of the message-token and within the latter, the content-integrity-check and the proof-of-delivery-request

- The support for transfer only (without the need for semantical understanding) of the P1 parameters associated with the EoS mentioned above (Content Integrity, Proof of Delivery, End-to-End Origin Authentication) is mandated for MTAs. This support is only a static requirement. *(for more details see AMH11 in ref. [4])*

2.2 Security environment

The (End-to-End) Content Integrity Check and Message Origin Authentication operates by means of digital signatures. This means that the necessary functions for signature processing are available in the Secure AMHS environment. This mostly includes:

- Selection of a hashing function;

- Selection of an assymmetrical signature algorithm, using pairs of public key/secret key. RSA is an example of such an algorithm;

- Availability of a Public Key Infrastructure.

Except where bandwidth optimisations would be required for air-ground purposes, all this environment can be common to the ATN, and not limited to the AMHS. It is therefore the intention of WG3/SG1 to use in the AMHS the signature algorithm selected by WG1/SG2 for in the overall ATN security. The same would occur with the PKI, where WG3/SG1 would be willing to use the mechanisms adopted by WG1/SG2, if suitable in the AMHS environment.

2.2.1 Hashing function

A one-way hashing function is, in broad terms, an « almost-bijective » compression function for which the converse function cannot be computed.

2.2.2 Assymmetrical encryption

Assymmetrical encryption is a transformation function, to be applied to a piece of information, using pairs of public key/secret key.

The transformation is such that :

Transformed1Info = Xp[Info] and Info = Xs[Transformed1Info] ; and

Transformed2Info = Xs[Info] and Info = Xp[Transformed2Info].

This equivalent to : Info = Xs[Xp[Info]] = Xp[Xs[Info]]

Depending on which key is used first, the mechanism provides, between a pair of users, either for signature or for encryption.

(see Annex C to X.509)

2.2.3 Public Key Infrastructure

This notion refers to the set of technical means by which public keys of users can be made available to a set of other users.

One way of doing this is to use **Certificates**. A certificate is a piece of data generated by a certification authority, containing the public key of a given user. The subject user certificate can be stored e.g. in an X.500 directory, together with the other data regarding the subject user. The subject user certificate is a sequence of data, signed by the certification authority using its private key, containing the public key of the subject user.

Every other user who has the public key of the certification authority can decode the certificate in a « reliable » manner and therefore obtain a « reliable » public key of the subject user.

(see X.509)

2.3 Backward compatibility

All X.400 security elements are all defined as ASN.1 EXTENSIONs. This means that the behaviour of the implementation, in case a security element is not semantically understood where it would have been necessary, is governed by the CRITICALITY mechanism.

The content-integrity-check has no criticality specified. This means that a receiving UA which is not able to decode and semantically understand the content-integrity-check will just ignore it. The recipient will have no way to ensure the content integrity, but he/she will still be able to obtain the message-content. In this way compatibility is obtained.

The message-token and the proof-of-delivery-request are specified as « CRITICAL FOR DELIVERY »[3]. This means that at the moment of delivery, if the receiving UA is not able to decode and semantically understand these elements, the message will be rejected and a Non-Delivery Report generated, stating « secure messaging error » (or « unsupported critical function »). Upon reception of the NDR, the originator of the subject message still has the possibility to re-send the message without requesting for the security elements. In this way compatibility is obtained in a sort of « degraded mode ».

3. OPERATION MODE

3.1 Content Integrity and Message Origin Authentication

3.1.1 Originator

Upon generation of the message to be protected, the content-integrity-check is added to the message by the UA in the Message Submission Envelope. The content-integrity-check is a signature is which is computed on the message-content only, using the secret key of the originating user.

The content-integrity-check may additionally be protected by means of the message-token, which adds a signature (using the secret key of the originating user) on the sequence of the following elements :

- signature-algorithm-identifier,
- name (O/R name) of the recipient (tbc),
- time stamp,
- content-integrity-check.

3.1.2 MTS

The MTAs will simply transfer the message without the need to understand what is conveyed in the content-integrity-check and message-token.

3.1.3 Recipient

Upon delivery, the criticality mechanism will be applied. The detailed way of operation of the criticality mechanism is beyond the goal of this paper. The recipient's UA will receive the message and decode it. The following will be performed :

- The content-integrity-check and the message-token will be « decrypted » using the originator's public key. (This implies that this key has been obtained previously by another means) ;

---

[3] In the 1996 version of the base standards, it seems that the criticality is "recommended only". This would make it possible to specify the message token as not critical, allowing a recipient to receive a message but without security ensured. This could possibly be investigated.

- The hashing function will be applied to the message-content and to the components of the message-token ;
- The comparison for equality of the hashed message-content and of the « decrypted » content-integrity-check, if matching, ensures that the message content has not been modified during its conveyance ;
- The comparison for equality of the hashed components of the message-token and of the « decrypted » message-token, if matching, provides positive authentication of the message originator.

3.2 Message Sequence Integrity

3.2.1 Origination

The message sequence integrity is obtained by adding an end-to-end (i.e., from the originator to the recipient, and as a consequence potentially different for each recipient) message sequence number within the message-token.

3.2.2 Reception

Decoding and verification of the message-token ensures that the sequence is kept and that the token has not been altered.

3.3 Proof of delivery

This is supported only in conjunction with a delivery-report-request.

3.3.1 Subject message origination

The Proof of delivery is obtained by adding a proof-of-delivery-request flag within the message-token.

3.3.2 Subject Message Reception

Decoding and verification of the message-token provides the flag and ensures that the token has not been altered.

A proof-of-delivery is then computed, as a result of the Message Delivery operation, by adding a signature (using the secret key of the subject message recipient) on the sequence of the following elements :

- proof-of-delivery-algorithm-identifier,
- delivery time,
- name (O/R name) of the recipient,
- subject-message content.

The proof-of-delivery is then sent back to the subject message originator, as a per-recipient EXTENSION field of the Delivery Report.

3.3.3 Delivery Report Reception

Upon reception of the DR by the subject message originator, the signature is checked (using the same principle as in 3.1.3 above), and positive checking provides the proof of delivery.

4. RECOMMENDATION

The analysis above shows that Security Class S0 provides proper countermeasures against the main threats identified in WP/208, namely :

- Content Integrity against modification,
- Message Origin Authentication against masquerade,
- Message Sequence Integrity against replay.

The subgroup is invited to take the elements above into account and to adopt S0 as the mandatory security class for the SEC Functional Group composing AMHS Security features for the Extended ATS Message Service.