ATNP/WG3

WP/12-__

15/03/98

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL(ATNP)

WORKING GROUP 3 - APPLICATIONS AND UPPER LAYERS

Rio de Janeiro, 16-20 March 1998 (twelfth meeting)

Agenda Item __ : Ground-Ground Applications

WP/12-___ : Analysis of Threats against the ATS Message Service

Presented by Jean-Marc Vacher (France)

Summary

The twelth WG3/SG1 meeting (Orlando, 14-16 January 1998) concluded that the existing analysis of risks concerning the AMHS was too general to allow the definition of an appropriate AMHS security approach.

This risk analysis was extracted from the ATN Security concept, elaborated by Eurocontrol, presented at ATNP/2 and distributed again to ATNP/WG3/SG1 as WP/164 in the eleventh WG3/SG1 meeting to serve as a working basis on the subject.

The goal of this paper is therefore to refine this risk analysis by an assessment of the impact of each type of attack, depending on the regarded message category.

This paper has been presented in the thirteenth WG3/SG1 meeting (Rio de Janeiro, 11-12 March 1998). The meeting has concluded that the paper should be presented for endorsement by WG3 and WG1, as appropriate.

This paper is a contribution to the production of sub-deliverable D111 ("Analysis of risks and threats against the ATS Message Service ") included in the SG1 Work Programme.

Table of contents

References

[1] ATN Overall Security Concept, Appendix to ATNP/2 WP/25 (previously elaborated by Eurocontrol under the aegis of ATNP/WG1)

[2] ATNP/WG3/SG1 WP/164, Analysis of threats against the ATS Message Service - Jean-Marc Vacher, 11th SG1 meeting, Toulouse, 16-19 September 1997

[3] ATNP/WG3/SG1 WP/155, SG1 Future Work Programme - Jean-Yves Piram, 11th SG1 meeting, Toulouse, 16-19 September 1997

[4] ATNP/WG3/SG1 WP/176, Security Approach for the ATS Message Service - Jean-Marc Vacher, 12th SG1 meeting, Orlando, 14-16 January 1998

[5] Draft report of the 12th ATNP/WG3/SG1 meeting (Orlando, 14-16 January 1998)

[6] ICAO Annex 10, Vol. II

1. INTRODUCTION

A first analysis of threats against the ATS Message Service has been provided to the ATNP/WG3/SG1 in the course of its 11th meeting, by means of WP/164 [2]. This was based on an earlier paper developed by Eurocontrol and named "ATN overall security framework" [1]. The 11th SG1 meeting noted the information provided in the paper and agreed to use it as a starting point for further work on AMHS security.

However, during the presentation of a WP proposing an AMHS security approach, in the 12th SG1 meeting, it became apparent that the risk analysis was not detailed enough to allow the definition of a security approach offering an appropriate protection against the identified risks. The meeting finally agreed that a more in-depth study should be undertaken to refine the threat analysis in relation with the nature of the exchanged messages.

The goal of this paper is to provide ATNP/WG3 with such a detailed threat analysis, after review of the work by WG3/SG1.

With respect to the agreed SG1 Work Programme [3], this paper is a contribution to the production of sub-deliverable D111 ("Analysis of risks and threats against the ATS Message Service") included in the Work Programme.

2. EVALUATION OF IDENTIFIED THREATS

2.1 Types of attacks

As stated in [1], Appendix D, section 1, the identified types of attack are listed in Table 1.

Table 1: Types of potential attacks against the AMHS

Type of attack	Definition
Modifications	Modification to a message in transit.
Replay	Recording a valid message and playing it back at a later time.
Jamming	Insertion of noise or such disturbance on the transmission line to prevent the passage of messages.
Masquerade	Creating false messages (while impersonating an actual user).
Flooding	Sending so many messages that the correct messages are unable to get through.
Other DoS	Any other Denial of Service attack (such as physical damage to equipment).

These "attacks" may be intentional or may in some cases result from technical malfunctions. However, the baseline is mostly that of an intentional attack.

2.2 Risk

In the AMHS as it is currently specified, the threat associated with each type of attack may be classified with:

- a level of risk, which is defined here as the probability of occurrence of such an attack, and which is related to the "ease of attack";
- an impact, which is defined as the level of consequence of such an attack.

The level of risk does not depend at present upon the type of message, since all categories of messages are equally handled in the AMHS. The level of risk is therefore the same as the one evaluated in [1], which is recalled in Table 2.

Table 2 - Attacks to the MHS messaging system as a whole

	Air Links	**Ground Links**	**Routers**	**Other Hosts/Users**	**Sys Man't & IDRP**	**MHS store/fwd**
Modifications		L	M			M
Replay		M	M		H	M
Jamming		M	M			
Masquerade		M	M	H	H	M
Flooding		M	M	H	H	H
Other DoS		H	H		H	H

2.3 Impact

The impact of each of these types of attacks has been analysed depending on the category of messages which may be conveyed in the AMHS. It is possible that attacks are not directed to a particular category of messages. However, whatever the intention of the attacker is, the impact obviously ranks differently whether the attacked message is a distress message or an administrative one.

The basis for such an assessment is the categories of messages which can be handled by the AFTN, and consequently by the AMHS in the future. These categories are listed in ICAO Annex 10, Vol. II, section 4.4.1.1.3.

Obviously, such an assessment is subjective by essence. Table 3 has been reviewed by WG3/SG1, in the light of its experience of AFTN, and the rationale for the table has been amended and complemented.

The classification used to rank the impact is as follows:

H high - immediate safety impact

M medium - potential direct or indirect safety impact, but not time-critical and as such allowing for verification, correlation, etc. and/or for which alternative communications may be implemented. In cases where safety is not impacted, there is at least an impact on regularity and efficiency of air traffic

L low - potential disturbance or loss of regularity and efficiency in air traffic, without any safety impact

- none - no impact at all.

Table 3 - Ranking impact of attacks depending on message category

	Modification	Replay	Jamming	Masquerade	Flooding	Other DoS
Distress Messages messages sent by mobile stations reporting that they are threatened by grave and imminent danger and all other messages relative to the immediate assistance required by the mobile station in distress	H	M	H	H	H	H
Urgency messages messages concerning the safety of a ship, aircraft or other vehicles, or of some person on board or within sight	H	M	H	H	H	H
Flight safety messages						
Movement and control messages as defined in PANS-RAC (Doc 4444), Part VIII	M	M	M	M	M	M
Messages originated by an aircraft operating agency of immediate concern to aircraft in flight or preparing to depart	L	L	L	L	L	L
Meteorological messages restricted to SIGMET information, special air-reports and amended forecasts	M	L	M	L	M	M
Meteorological messages						
Messages concerning forecasts, e.g. terminal aerodrome forecasts (TAFs), area and route forecasts	L	-	L	L	L	L
Messages concerning observations and reports, e.g. METAR, SPECI	L	-	L	L	L	L

	Modification	Replay	Jamming	Masquerade	Flooding	Other DoS
Flight regularity messages						
Aircraft load messages required for weight and balance computation	L	-	L	L	L	L
Messages concerning changes in aircraft operating schedules	L	-	L	L	L	L
Messages concerning aircraft servicing	L	-	L	L	L	L
Messages concerning changes in collective requirements for passengers, crew and cargo covered by deviation from normal operating schedules	L	-	L	L	L	L
Messages concerning non-routine landings	M	-	L	L	L	L
Messages concerning pre-flight arrangements for air navigation services and operational serving for non-scheduled aircraft operations, e.g.overflight clearance requests	M	-	L	L	L	L
Messages originated by aircraft operating agencies reporting an aircraft arrival or departure	M	-	L	L	L	L
Messages concerning parts and materials urgently required for the operation of aircraft	L	-	L	L	L	L
Aeronautical information services (AIS)						
Messages concerning NOTAMs	M	L	M	L	M	M
Messages concerning SNOWTAMs	M	L	M	L	M	M
Aeronautical administrative messages						
messages regarding the operation or maintenance of facilities provided for the safety or regularity of aircraft operations	L	-	L	L	L	L
Messages concerning the functioning of aeronautical telecommunication services	L	-	L	L	L	L
Messages exchanged between civil aviation authorities relating to aeronautical services	L	-	L	L	L	L

Note: The categories of messages listed in the Core SARPs are consistent with the list of Annex 10, Vol. II used for WP/186. However network or system management messages are out of the scope of Table 3, since such messages would be conveyed using the Systems Management Application based on CMIP, rather than AMHS.

The following comments can be made about the rationale for the ranking above:

- modification generally ranks highest because it affects a true message or true operational conditions, and thus information critical to the meaning/use of the message may be lost;

- masquerade ranks lower or equal to modification, because it does not affect true operational conditions;

- replay generally ranks lowest because many systems or recipients would detect the inconsistence or irrelevance associated with a replayed message;

- jamming, flooding and other DoS generally rank identical with modification for the message category, since they all may result in the loss or excessive reception delay for the considered message.

3. NEXT STAGES

The next stage in the work to be performed will be to define an appropriate set of countermeasures, able to reduce the risk identified in this paper. An approach has been started, aiming at the selection of an appropriate security class for the SEC optional functional group of MHS ISPs. This approach now needs to be refined and complemented as appropriate.

4. RECOMMENDATION

The working group is invited to comment, amend as appropriate and endorse the risk analysis detailed above. It is further invited to submit this analysis to ATNP/WG1, if considered appropriate, as the base risk analysis for the elaboration of the AMHS security approach.

I.