ATNP WG3

W316W23

AERONAUTICAL TELECOMMUNICATIONS NETWORK

WG 3 (ATN Applications and Upper Layers) Sixteenth Meeting

Naples, 18 – 21 May April 1999

Agenda Item 3: Review Status of Appropriate Meetings

3.3 Security Subgroup

ATNP Security Considerations

(Presented by M J A Asbury)

SUMMARY

This short paper outlines points which should be considered by the ATNP Security Subgroup when refining the technical requirements relating to security of dialogue in a data link environment

1. INTRODUCTION

1.1 The ADSP has previously adopted a broad brush approach to the question of security of communications in a data link environment. However, the ATNP Working Group/Subgroup responsible for the development of security have being reviewing the topic, prior to presenting a technical solution and the appropriate SARPs to the next ATNP meeting, in February 2000.

1.2 The ATNP members have a general awareness of the operational requirements, but it should be the responsibility of the ADSP to give detailed advice where this might provide guidance to the ATNP in the development of the appropriate level of security, taking into account other factors relating to the safety of operations, including current procedures, cost effectiveness etc. The appropriate ATNP Subgroup has recognised the need for an operational input where they felt that the correct level of advice was hitherto not available, and had consulted the ADSP as required.

2. DISCUSSION

2.1 The principle reason for introducing a level of security into the operation of a data link based Air Traffic Service is to enhance safety by reducing the risk of an unauthorised person or organisation sending an instruction or information to an aircraft, generally with malicious intent, which could result in a deviation from its planned and approved trajectory, with possibly serious consequences. Thus the use of security is an exercise in risk *mitigation*, rather than in risk *elimination*.

2.2 Various levels of security can be introduced, ranging from zero to full end user authentication and message encryption. Each additional level of security above zero imposes a cost and time penalty, with additional bits on the line, possible exchange of system messages, and logistics of the distribution of security information, e.g. public and private keys.

2.3 In the voice environment, there is a strong possibility that attempted erroneous transmissions can be detected by the pilots, due to their amateur nature, although this is not always the case. But in the data link environment, when an incorrect message is sent, provided it replicates the originator in all details, the pilot has no knowledge as to whether the originator is true or false. In many cases, if an instruction or clearance was significantly at variance with those previously received, the pilot might query the message, but if the message was not too unexpected, the pilot would not unreasonable comply.

2.4 Software-based security methods are never foolproof – given enough processing power, the system will always be compromised. For example, given a cryptographic key some 128 bits long, some 2^{32} processes would have to be carried out to break the code. This could take an hour on a personal computer this week - or it could take 6 minutes next year, if processing speeds increase by only one order of magnitude. ATNP should be concerned with developing a cost beneficial deterrent – it will not be possible to develop 100% total protection.

2.5 There is a need to look realistically at the operational needs and the general safety budget, and keep things in proportion. For example, if a key is compromised, and an aircraft is given a potentially harmful clearance, what are the chances that this will not be queried by the pilot, but will be accepted regardless? What are the chances that ADS will/will not be in use? What are the chances that conflict probe/conflict detection will not be in use? What are the chances that there will be another aircraft on a conflicting path? What are the 'see and be seen' considerations? If the aircraft is also in a radar environment, what are the chances of the movement being unobserved? Technically, what are the chances that the compromise is malicious, or just a thrill seeking hacker?

2.6 Also, there needs to be a review of existing level/heading/clearance deviations which already take place, to see what effect an unauthorised deviation from trajectory has today. For example, if there is a one in 10^5 chance* that there will be an unauthorised deviation from clearance due to normal operations, then there need not be a level of message protection better
than one order of magnitude greater than that, certainly in the current and medium term environment.

(*London Area handled over 3 million movements in the last three years. Allowing that each movement received 10 instructions/clearances, there were just under 300 'level busts' in that period.)

3. RECOMMENDATION

3.1 ATNP should ask the ADSP to issue more positive guidance relating to implementation of security on air/ground and ground/ground data link networks through revised operational requirements. This guidance should take account of the present safety budgets and risk mitigation techniques currently being implemented.

3.2 A full risk assessment analysis should be carried out, based on both operational and technical expertise, in order to assess the level of security required to be implemented.

3.3 Finally, the ATNP should not act hastily to proscribe security over and above that which already exists through the use of the ATN until such a risk assessment has been carried out.

End