EUROCONTROL

ATNP/WG_____

WP/___

8 March 1995

AERONAUTICAL TELECOMMUNICATION NETWORK PANEL

WORKING GROUPS 1, 2, & 3

Toulouse, 13-23 March 1995

Security Issues for CNS/ATM-1 Package and Beyond

Prepared by: Ian Valentine, Nick Pope

Presented by: Eike Meyenberg, Martin Adnams, Henk Hof, Danny Van Roosbroek

SUMMARY

The specifications of ADS, AIDC and CPDLC, as described in the ADS Manual of May 1994, identify the need for security measures to be taken with respect to information flowing between end systems, whether these be air-ground or ground-ground flows. This paper is a collection of pre-existing technical security material, together with new material particularly aimed at WG1, relating to institutional, policy and planning matters of security.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Background

The specifications of ADS, AIDC and CPDLC, as described in the ADS Manual of May 1994, identify the need for security measures to be taken with respect to information flowing between end systems, whether these be air-ground or ground-ground flows. Papers have been presented at the San Diego meeting of ATNP WGs, and at subsequent sub-group meetings, exploring the threats and countermeasures that may be applicable to the ATN applications. This paper is a collection of that material, together with new material particularly aimed at WG1, relating to institutional, policy and planning matters of security.

1.2 Approach

The approach taken in this document is first to determine the security threats to aeronautical communications over the ATN, and to consider the relative seriousness and likelihood of each form of attack. The areas where there is a serious risk are then considered for the application of appropriate counter-measures. These are divided between the urgent (CNS/ATM-1 package) and less urgent (later) counter-measures Based on the threat analysis and countermeasures, a security policy is developed in section 5. As security is not just a matter of communications protocols, but entails active participation by user organisations, the “institutional Issues” are described in section 7. These also have to be developed to support the counter-measures proposed for CNS/ATM-1 package. Section 8 considers a more detailed technical analysis for background use in WGs and SGs involved with the development of security protocols.

2. THREATS

2.1 Initial Threat Analysis

This section presents an hierarchical breakdown of threats. Each bold phrase is a single threat; each plain text phrase is a short explanation of the threat above it. Each level of indentation represents a breakdown of the preceding threat into greater detail. After each of the lowest level threats is a list in italics of the major attack types that can realise this threat. A question mark refers to a threat not covered by one of the attack types.

Such a breakdown is useful in ensuring that all threats are covered, even though many areas turn out to be inappropriate or unimportant.

- **Read by wrong party**
  - **as a message**
    The actual content of the message is read.
    - **tapping the transmission medium** *(monitoring)*
    - **gaining access to a message in a router** *(monitoring)*
    - **gaining access to a message in a message store** *(monitoring***)**
    - **arranging that the message is routed to an incorrect destination**
      - **altering the routing information** *(modification)*
      - **altering the message address** *(modification)*
      - **making the message multicast/broadcast** *(modification***)**
    - **gaining access falsely as the expected recipient** *(?)*
  - **as statistics** *(?)*
    Traffic analysis revealing the sort of information passing, even if not the exact content. Or looking at just the headers and seeing to whom it is going and from whom, and deducing something useful from this.
- **Never reaches right party**

transmission medium is jammed *(jamming)*
altering the routing information *(modification)*
contents of message is altered *(modification)*
whole connection is set up falsely with wrong party *(?)*
message is not expected and does not require acknowledgement *(modification, jamming, flooding or other DoS)*
message is not expected and acknowledgement is given falsely *(modification, jamming, flooding or other DoS; and masquerade)*

received from wrong party

replay *(replay)*
A genuine message is recorded and played back at a different time.

masquerade
An intruder adds messages to the system purporting to come from genuine users.
message inserted in transmission medium *(masquerade)*
message inserted in storage en route *(masquerade)*
message insertion via management system *(masquerade)*

modification
Part of a genuine message is altered en route
altered while on the transmission medium (unlikely) *(modification)*
altered while in storage, e.g. router *(modification)*

wrong messages are sent
Even before the message hits the communications system, its wrong.

invalid user
An intruder gains access to a valid system as a valid user, and hence sends "valid" messages.
valid user masquerades as another valid user *(masquerade)*
intruder gains access to host *(masquerade, replay, or modification)*
This may be to the host supporting the correct message interchange, or another router, management terminal or other controller centre.
rogue software *(masquerade, replay, or modification)*
Software in the sender constructs messages it should not

valid user sends incorrect information
accidentally *(?)*
Poor user interfaces, poor documentation, poor training, inability to cancel a message once started
maliciously *(?)*
if users are not accountable for their actions they can be cavalier in the information they send

wrong messages is understood *(?)*
The system receives the correct message, but before it is used by the correct recipient it is altered to something different.

2.2 Threats by Communication Type

It is suggested that the following threats against the ATN, including ATN management and application services, pose a significant threat and hence require specific counter-measures:

a) Air Traffic Control Messages (both air-ground and ground to ground) These apply to CNS/ATM-1 package:

- Modification
- Replay
- Masquerade

b) X.400 Message Handling System (MHS). These could be considered for CNS/ATM-1 package, but are more likely to be considered subsequently.

- Modification
- Masquerade

c) Inter Domain Routing Protocol. These are certainly beyond CNS/ATM-1 package timescale:

- Modification
- Replay
- Masquerade
- Unauthorised modification of routing information base

d) OSI Systems Management. These are certainly beyond CNS/ATM-1 package timescale:

- Modification
- Replay
- Masquerade
- Unauthorised modification of management information base

e) Denial of service attacks on the ATN which impact Air Traffic Control Messages including: These are to be addressed by network design and topology, and physical access security, and should be considered by regional planning bodies:

- Jamming air-ground links
- Flooding the ATN with data packets
- Causing switches and data links to fail.

3. URGENT COUNTERMEASURES (CNS/ATM-1 PACKAGE)

3.1 Initial Analysis

The initial analysis of the basic risks of the ATN in section 2.2 indicates the urgent need for security mechanisms to protect ATN Air to Ground and Ground to Ground messages against the following threats:

a) Modification

b) Replay

c) Masquerade

There are other significant threats identified by the basic risk analysis (e.g. denial of service attacks, access control, attacks on ATN management services) which are not considered as being of such high urgency, and are therefore considered in section 4.

In selecting the proposed solution some account has also been taken of the specific features of the ATN environment. In particular:

a) The limited size of many ATN messages;

b) The limited throughput of some of the communication links;

c) The 2 party and end to end nature of the message exchanges (there is no need to secure multi-cast messages, the security of messages does not need to be checked by intermediate routers or message relays).

3.2 Message Authentication Check

It is proposed that a cryptographic message authentication check (MAC) is appended to each message to provide a countermeasure to modification and masquerade attacks.

The Message Authentication Algorithm (MAA) as defined in ISO 8731-2 [3] has been identified as an algorithm which provides the required form of protection with a minimal overhead on the message length (32 bits).

However, potential weaknesses have been identified with this algorithm [4] and further analysis is required whether this is of major concern in the threat environment envisaged for the ATN. It is not recommended that this algorithm is used other than for protection of messages where message size is of major concern.

The MAA is optimised for use with 32 bit processors, operating on 32 bit units of information.

The MAA cannot be used to provide confidentiality and so is less likely to be subject to any export restrictions often associated with encryption algorithms. (Alternative MAC algorithms based on encrypted hash codes have been ruled out for this reason).

The MAC requires a shared 64 bit key be pre-established between the communicating peers (see key management below). It is proposed that the same MAC key is used for protection both directions of message flow.

Note: ISO 8731-2 leaves open the padding used in calculating the MAC. It is understood that the value chosen has no security implications. The padding is only used in calculating the MAC; no additional padding bits are sent in the message. It is initially proposed to use the value “0” for all padding bits.

3.3 Replay Protection

It is proposed that replay protection is provided using a message identifier or sequence number which is unique within the lifetime of the key. The size of this sequence number depends on the maximum number of messages that can be expected within the lifetime of the key (see key section on key management below). For example, for a maximum possible of 64,000 messages in a session the sequence number would be 16 bits.

The size of the sequence number can be further reduced if each message contains a time stamp. The sequence number can be further reduced to the maximum number of messages within a time window defined by the accuracy of the clock synchronisation, network delay.

Further investigation is required to identify the appropriate message sequence identifier.

This message identifier is added to each message before MAC is calculated.

Additional direction sensitive information is also required to avoid a message being reflected back to the originator. This could either by addressing information contained in the message or a direction flag.

Note: Timestamps were considered as an alternative replay mechanism but it is not considered that sufficient time granularity can be achieved for this to be practical mechanism for use on its own.

4. OTHER COUNTER-MEASURES (BEYOND CNS/ATM-1)

This section covers other ATN applications and mechanisms which were not addressed in the initial analysis above, and may need to be addressed in a longer timeframe than CNS/ATM-1 Package.

4.1 . X.400 MHS Security

There exists standard mechanisms for MHS security as defined in X.400 (88) and profiled in ISP10611. The S0 security functional class in the X.400 profile includes support for digital signatures and message sequence numbers applied to each message. The digital signatures are generated using public key (asymmetric) cryptography.

These mechanisms can be used as countermeasures for modification and replay attacks on X.400 messages.

Certification of public keys required for MHS security can be supported by the common public key certification mechanism (see section 7).

4.2 OSI Systems Management Security

Three possible approaches to OSI Systems Management Security may be considered to protect OSI Systems Management.

The first approach is to restrict the use of distributed systems management, disallowing any remote changes to managed objects which may significantly affect the operation of the ATN. This approach provides the required degree of protection but limits the functionality available through systems management

The second approach is to apply the following security services to systems management:

a) Access control to managed objects,

b) Peer entity authentication between the manager and agent system on application association establishment.

Access control to managed objects can either be supported using the ISO standard for “Objects and Attributes for Access Control” (ISO/IEC 10164-8) which provides a very flexible means of controlling access to managed objects but is likely to be difficult to implement. A more simple approach would be to define different managed objects which gives different “views” on the system. On view would be for system managers, who are trusted with write access to sensitive managed objects, and the other view is for general read only access. Authentication should be mandated to obtain system manager status.

Whilst there is no internationally agreed profile for applying peer entity authentication to OSI systems management, “implementation agreements” produced by the American OSI Implementors Workshop (December 1994) define a profile which supports peer entity authentication. This uses of public key (asymmetric) cryptography techniques mechanisms for “strong” authentication as defined in X.509.

This approach provides protection against masquerade but does not stop modification or replay attacks within the network.

The third approach is to apply digital signatures (as used for X.400 security) or message authentication checks (as proposed for ATC message security) to those requests which require changes to sensitive managed objects, along with timestamps and sequence numbers to avoid replay. Access control should then be applied using this authenticated identity as described earlier. This approach is not currently supported by OSI management standards. However, it can be used to protect against modification and replay threats against OSI management as well as masquerade.

The second and third approach require the certification of public keys. This can be supported by the common certification mechanism.

4.3 IDRP Security

The IDRP protocol supports a range of authentication mechanisms (referred to as authentication type 1, 2 and 3). Authentication type 1 provides an unencrypted checksum, and so is not secure, although it gives protection against arbitrary errors. Type 2 provides protection against masquerade and modification by use of a checksum which is encrypted using an algorithm such as DES. As this technology is subject to export controls, it is not suitable for a global network solution. Authentication type 3 also supports counter-measures to masquerade and modification attacks. This uses a "validation field" in each routing protocol exchange to carry a Message Authentication Check (MAC). The function of this MAC is similar to that proposed for ATC message security, however, the IDRP standard specifies a particular algorithm which produces a 16 octet (128 bit) MAC.

> Note: For CNS/ATM-1 Package, type 1 authentication has been selected. It may be that this would be difficult to change in the future, and that type 1 will continue as the long term solution.

The IDRP MAC requires a key (described as password in IDRP). This key could be established using a key transport mechanism along the lines described in section 7 for ATC message security. This in turn requires a public key certificate which could be supported by a general certification mechanism (see section 7).

> Note: The IDRP "Security Attribute" is not used to support authentication. This has another security related function called routing control (see denial of service countermeasures).

The IDRP standard includes a 32 bit sequence number which could be used for replay protection, except that the standard requires that this number be set 1 when a "connection" starts between two IDRP "boundary intermediate systems". Thus, for this field to be used for replay protection a new MAC key needs to be established for each new IDRP connection.

The IDRP standard itself does not define any access control mechanisms which can be used to restrict the use of IDRP for the exchange of routing information to counter unauthorised modification of the routing information base, although it does not preclude the inclusion of such facilities. The form of controls required to protect unauthorised modification of routing information requires further study.

4.4 Denial of Service Risk (DoS) Reduction

4.4.1 Introduction

It is very difficult to totally protect against denial of service attacks. However, a number of basic measures can be taken to reduce the risk of denial of service attacks having a significant effect on the operation of the ATN. It is proposed that two basic mechanisms are used together for denial of service risk reduction:

a) Alternative routing

b) Routing control

These two countermeasures are complimentary and hence should be used in conjunction. Alternative routing control helps avoid localised denial of service attacks. Routing control helps to localise the impact of denial of service attacks.

Note: Denial of service attacks frequently occur via management paths. Thus security should also be directly applied to IDRP and OSI systems management (see above) to reduce the risk of denial of service attacks.

4.4.2 Alternative Routing

Alternative routing reduces the risk of denial of service attacks by re-routing data packets along an alternative route to avoid the point of attack. For alternative routing to operate there also needs to be a form of liveness check over a route to detect that communications over a certain route operates correctly. Ideally, this liveness check should test for the round trip delay to detect if the delay is very much higher than would be expected even though the communications link is operating.

This countermeasure is effective where denial of service attacks are targeted at a single point in the network. However, where denial of service attacks are spread across the network, for example by flooding the network with packets, this countermeasure is not very effective. In addition, there will be a delay between the occurrence of a denial of service attack and alternative routing establishing an alternative route.

The Inter Domain Routing Protocol (IDRP) includes facilities which might be used to support alternative routing at the interdomain boundaries. It includes the ability to manage alternative routes and has a mechanism for checking liveness. However, the liveness mechanism does not include facilities to check the round trip delay and only operates between boundary systems.

The provision of alternative routes within a routing domain will depend on the specifics of the routing within that domain.

If there are sufficient alternative inter-domain routes then it may not be necessary to provide alternative routing within a domain. In addition, if alternative routing occurs at the inter-domain level, there is greater chance of avoiding any denial of service attacks especially if the alternative routes involve different types of networking technologies with different vulnerabilities to denial of service attack (e.g. selecting satellite links instead of radio links could avoid attacks based on use of radio equipment).

Ultimately, the ability to support alternative routing will depend on the availability of alternative communication routes. If there are no alternative communication links available then, even if the routing protocols support it, there will be no possibility to achieve alternative routing. Thus, in designing the topology of the ATN consideration should be given to the provision of alternative routes, especially to provide alternative route where a communications link is particularly vulnerable to attack.

4.4.3 Routing Control

Network layer routing control aims to minimise the potential effect of denial of service attacks through flooding by restricting the flow of packets across the network. It involves checking whether a given data packet should be passed along a given route based on knowledge of whether the source of the data should be using (i.e. has been authorised to use) a particular path. This countermeasure helps to localise any denial of service attacks, reducing its impact and making more likely that alternative routing could be used to route around the problem.

In the simplest form, routing control can be based upon an access control list, held by a network layer router (i.e. intermediate system in OSI terminology), of source addresses against given route. If a source, as identified by its address, is allowed to use a given route it would have an entry in the access control list. As the packet passes through the router the source address would be checked the access control list before passing it along a given route.

This simple approach to routing control based on access control lists would, however, be virtually impossible to manage in networks involving a potentially large community of users such as the ATN.

A more sophisticated approach to routing control, which would be more appropriate to the ATN, is routing control based on security labels. With this approach a label is assigned to each data packet (i.e. connectionless network protocol data unit) by the source. As it passes along the network each router firstly (i.e. intermediate system) checks incoming packets to check that previous system (as identified by its subnetwork point of attachment (SNPA) address) is authorised for the given label. Secondly, before forwarding a packet along a given route the route checks that that the labelled packet is allowed down an outgoing route. The check that the source SNPA is authorised for an incoming packets needs to be applied to packets arriving at an intermediate system from within a routing domain as well as packets arriving from an external domain.

The ATN already includes some support for routing control based on security labels. It supports the carrying of labels in data packets and IDRP supports the distribution of information relating security attributes (as would be used in a security label) to a particular route. However, further investigation is required whether the current use of security labels and attributes in the ATN exactly meets the requirements. In particular, specific checks may be necessary to ensure that labels are not assigned without the originator being authorised to source such types of message. Also, additional types of security attributes may be necessary to further restrict the flow of messages (for example a closed user group community identifier).

5. PROPOSED SECURITY POLICY

Based on the analysis above, the following security policy statements are proposed for the ATN security counter-measures. All counter-measures need to be analysed for their success in countering the identified threat(s).

- There is no requirement to protect any communication against monitoring or traffic analysis.
- Where a countermeasure is necessary to counter one threat, and as a side effect counters another, the success of the side effect shall be analysed and documented as though it were an explicit requirement.

  This is proposed because the presence of a security facility will lead to it being used and relied upon, even if the facility was not intended for that purpose.
- X.400 messages shall be protected against modification and against masquerade. That is:
  - it shall not be possible for anyone to modify a message once it has been produced in such a way as to alter the information content of the message or its original sender
  - it shall always be possible to reliably tell from a message who the original sender was
- DLA messages shall be protected against modification, masquerade and replay. That is:
  - it shall not be possible for anyone to modify a message once it has been produced in such a way as to alter the information content of the message or its original sender
  - it shall always be possible to reliably tell from a message who the original sender was
  - it shall be possible to recognise the correct sequence of messages, so that if a message is received out of sequence, this fact is recognisable
- Messages for the purposes of network management and the messages that carry routing information shall be protected against modification, masquerade and replay. That is:
  - it shall not be possible for anyone to modify a message once it has been produced in such a way as to alter the information content of the message or its original sender

  - it shall always be possible to reliably tell from a message who the original sender was
  - it shall be possible to recognise the correct sequence of messages, so that if a message is received out of sequence, this fact is recognisable

- The services that support messages to and from aircraft (including while these messages are on ground links) shall be protected against denial of service attacks to a chosen level of probability of compromise (to be ascertained).
- All ATN hosts and routers shall be protected against attack from unauthorised person, such that only authorised persons shall be able to send ATN messages or access ATN data.

6. KEY MANAGEMENT FOR MAC SHARED KEY

The MAC mechanism described earlier requires that a shared key be established between the communicating systems. This key can be established when a message exchange “context” is established between systems.

The relationship between the context management application and key management requires further study. In addition, consideration needs to be given whether the same key is used to protect all applications (which adds further complication to the replay detection system) or a new key is established for each application.

It is proposed that this key is generated by at ground stations and transported to the air based system using asymmetric techniques. Example of such key transport mechanisms are currently being standardised in ISO/IEC CD 11770-3 [5] and also have been defined in the recent banking standard ISO 11166-1 [1].

> Note: The specification of ISO 11166-1 is more comprehensive than ISO CD 11770-3 and has been agreed internationally. However, this banking standard has been subject to some criticism and so further study is required before recommending a specific way forward.

The RSA algorithm can be used to support this key transport mechanism. Implementations of RSA are readily available; although in the USA a licence is payable for its usage. Example implementations using an IBM PC can take a second or two to provide the required protections. Thus establishing a new session key could take a few seconds.

The key management RSA algorithm itself uses a private / public key pair which have to be managed. The private key can be permanently loaded into the avionics or ATC or system. The public key, however, need to be distributed in a protected form called a public key certificate.

Messages will need to be defined to carry the protected MAC keys and exchange certificates. A starting point for such messages are defined in ISO 11166-1.

Procedures will also need to be established for the generation and archiving of keys. A basis for such procedures may also be identified in ISO 11166-1.

7. INSTITUTIONAL ISSUES OF PUBLIC KEY CERTIFICATION

The following need to be addressed and resolved for CNS/ATM-1 package if the proposed countermeasures are going to be applied.

7.1 Introduction

The need has been identified for the provision of certified public keys in support of the interim countermeasures for Air Traffic Control message security, as has that for other countermeasures to ATN threats.

As mentioned earlier, public/private key pairs are long lived - usually for the lifetime of a piece of avionics or an ATC system. The provision and embedding of the private key into an equipment or system is a ‘once per lifetime’ process that has to be carried out in such a way that no unauthorised party gets access to the key. It is possible that secure X.400, or off-line techniques such as registered post, can be used to pass such a key to a manufacturer for this purpose.

The problem which gives rise to the need for public key certification is that new equipments and systems are coming into service at all time, and to communicate with them, the pre-existing systems need to be given access to the public key in such a way that there is no possibility that a forged (bogus) key is inadvertently acquired.

Public key certification is the process and this section discusses the institutional issues involved with the required public key certification.

7.2 Brief Explanation Of Public Key Certification

A number of the countermeasures to ATN threats involve use of public key cryptography. This is used either as the basis for key management (for example establishing a shared MAC key as required for ATC message security) or to produce digital signatures (for example in X.400 message security). Public key cryptography is based on the use of a public and private key pair. The private key is known only by one system entity. The public key should generally be available to any other system needing to communicate with the entity holding the associated private key. The system using the public key needs to be assured that the public key relates to an identified remote entity holding the private key. This assurance is achieved using a public key certificate.

A public key certificate is a data item which includes:

- a public key
- the identity or name of the entity holding the associated private key
- a digital signature produced by a trusted certification authority which certifies the validity of the relationship between the public key and the identity held in the certificate.

A public key certificate is created by a certification authority at or around the time that the public / private key pair is created. A public key certificate needs to be held on the ATN so that it can be provided to systems as needed (e.g. to check validity of digital signatures). This is normally achieved either:

- by the system owning the private key also holding its associated public key certificate which it sends to other remote systems along with any protected information.

or

- by a network based directory service holding the public key certificate for retrieval by any system requiring to check protected information.

7.3 Nature of a certificate

It is proposed that the public keys are certified using the certificate format defined in CCITT X.509 | ISO/IEC 9594-8 [6].

These certificates are signed by a certification authority when the private and public are generated to validate the use of keys. The certificates can either be held in the same security device which holds the related security device and sent by the user when need or loaded into a directory.

A certification authority could be established for each organisation operating aircraft or air traffic control (e.g. each airline and country air traffic control agency). A further “top level” certification authority would need to be establish to certify each organisations certification authority. The institutional implications of support for generation of public keys, certification and certification authorities requires further study.

The certification authorities will also be responsible for creating lists of public keys and associated certificates that have been revoked (e.g. when a key has been compromised). Public / private keys (and associated certificates) should have a limited lifetime and would need to be replaced after a certain period.

The X.509 certification scheme has been adopted as the basis of a number of security systems including X.400 message security, X.500 directory security, internet Privacy Enhanced Mail (but ISO 11166-1 has defined an alternative certification scheme).

7.4 Certification Authorities

As mentioned above the public key certificates are created by certification authorities. A certification authority (CA) is an entity which is trusted to certify that a public key belongs to a named entity. A CA does not need to be directly on-line to the network. It can manually load the certificates into systems (or the directory) when they are being configured for use on the ATN.

It is expected that several CAs will exist for the ATN. There could be one CA for every organisation which uses the ATN. For example, there could be a CA for:

- Each airline with aircraft using the ATN
- Each country or area ATM organisation c) International ATM co-ordination organisations such as Eurocontrol

There will also need to be one top level CA for the whole of the ATN which certifies all the second level CAs on the ATN. This top level CA could be used to certify CAs for new organisations joining the ATN.

7.5 Public Key Certificate Management Functions

The use of public key certificates requires the support of a number of management functions, including but not limited to creation of public key certificates. This includes:

- Generation of new public / private key pairs for ATN systems
- Creation of public key certificates Loading of keying information and certificates into ATN systems (i.e. private key, public key certificate and CA public key)
- Loading public key certificates into the ATN directory (if the directory is used as a means of distributing public key certificates)
- Management of the revocation of compromised keys (including detection of a key compromise, reporting problem to the CA, distribution of public key certificate revocation list)

Whilst not all the above functions need to be directly carried out by a CA, it is recommended that they are all considered as being the responsibility of the organisation's CA.

A CA need not be directly available on-line to the ATN, and the operation of a CA need not be a full time activity.

The main activity of the CA will occur when a new system is configured. At this time keys and certificates will need to be generated and loaded (a to d above). After a public / private key pair has been in use for a significant period (say 1 year), it is good practice to create a new key pair and associated certificate (i.e. repeat tasks a to d above).

There is the additional activity of management of the revocation of compromised keys which requires a body to be readily available to take quick action as a CA. It would hopefully be a rare occurrence, but if a situation occurs when a key has been compromised (for example equipment has been tampered with by a terrorist organisation) rapid response is required to limit the potential impact of the compromise. The CA will need to quickly produce an updated revocation list for distribution over the ATN. It may also be necessary for the CA to regularly produce a revocation list of keys which are no longer in use, for example, due to decommissioning equipment. This may be done, say, on a monthly or weekly basis.

A CA will need to be a body with close links with technicians concerned with installing and maintaining equipment. However, it will need to be managed in a way which ensures that the operation of the CA cannot be easily compromised.

7.6 Trust Relationships between CAs, and Common Policies

For systems in one organisation to use certificates from a CA in another organisation there needs to be a trust relationship between the two. A CA has to be trusted to properly manage the keys and produce certificates correctly without compromising their security. This can be best achieved through use of an agreed security policy which organisations could commit to follow. Such agreements could either by bilateral or ATN wide.

Where an ATN wide security policy is being followed by a CA the top level CA would issue a certificate for that organisation CA’s public key. Where security policy agreements are bilateral each CA could cross certify the other CA’s public key.

8. DETAILED TECHNICAL ISSUES

This section provides more technical background for some of the issues discussed in this document, which may be of interest to the technical WGs and SGs.

8.1 Ranking Attacks

The following table categorises threats according the point of potential attack and type of attack. The identified points of attack are:

Air Links Attacks against any link between ground stations and aircraft, including VHF, satellite and Mode-S.

Ground Links Attacking the physical links between ground stations, e.g. wire tapping.

Routers Attacking the points at which messages are received and re-routed by gaining access to the routers themselves.

Other Hosts/Users Attacks via other hosts on the ATN (different from the intended sender or receiver), via other users on the ATN, or other users on the local hosts.

Sys Man’t & IDRP Use of the network management system; either access to management terminals or access to the management messages. Also attacks to the inter domain routing protocol (IDRP).

MHS system	Attacks on the Message Handling System, including in particular store and forward centres (Message Transmission Agents)

The identified types of attack are:

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.
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).
Monitoring	The contents of the message is read by an intruder, but not prevented from reaching its correct destination.

For each type of attack, we have ranked the impact of such an attack as High, Medium and Low. Clearly, this ranking depends upon the purpose of the information being attacked, in that a masquerade message requesting a different type of sandwich will have low impact wherever it is inserted, and so we have assumed the worst case, where the information is safety critical.

For each type of attack and each point of attack we have ranked the likelihood of occurrence (or ease of attack). This assumes that no protection is in place against such an attack. This is also High (very likely/easy), Medium and Low, including non-existent (∅) where such an attack is not possible.

In earlier sections we divided the analysis into four areas, only one of which routinely carries time and safety critical information. This gives us a finer grain analysis than this coarse table below.

	Impact	Air Links	Ground Links	Routers	Other Hosts/ Users	Network Man’t	MHS store/fwd
Modifications	H	L	L	M	∅	∅	M
Replay	H	H	M	M	∅	H	M
Jamming	M	H	M	M	∅	H	M
Masquerade	H	M	M	M	H	H	M
Flooding	M	H	M	M	H	H	M
Other DoS	M	M	H	H	∅	H	H
Monitoring	L	H	H	M	∅	H	M

From this we can see some areas where the most effort should be expended to counter the threats.

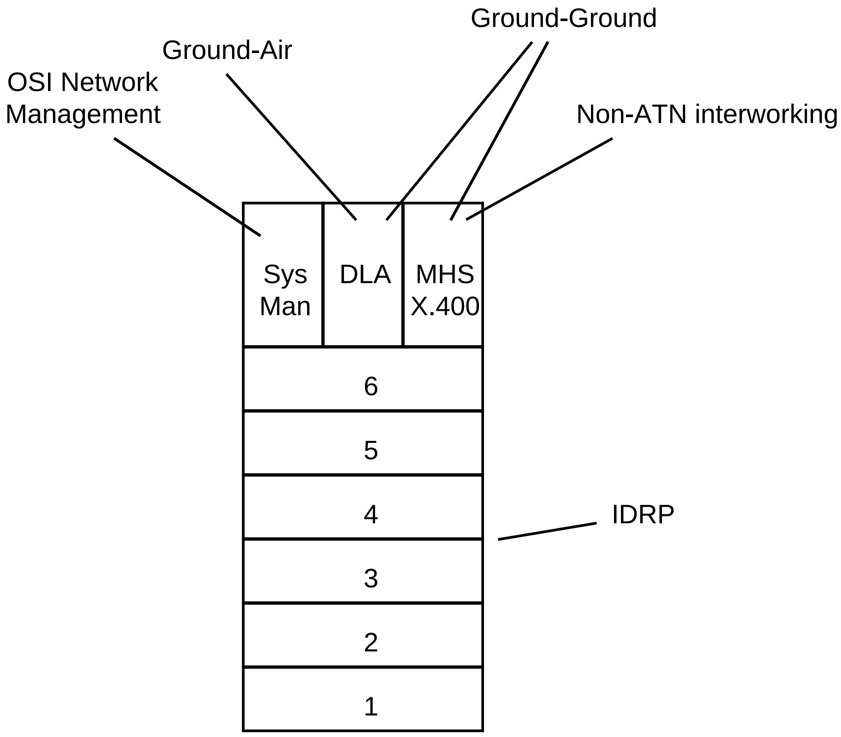
Monitoring, as the impact is very low (and possibly zero in many cases), can be ignored in future analyses.

Access to the network management system is clearly very threatening, as compromise of this area makes most types of attack very easy.

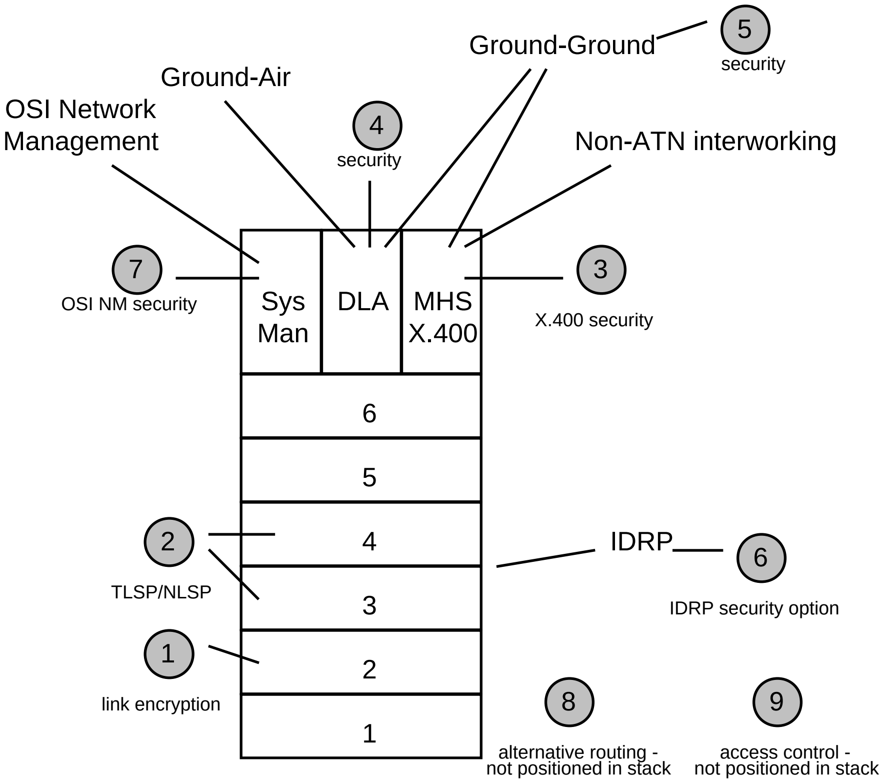
It can be seen that, apart from monitoring, all types of attacks and all points of attack play an important role, and none can be ignored.

8.2 Ranking Security Placement

We can consider the possible placement of countermeasures within the OSI communications stacks to counter the above threats. We have assumed that the basic communications structure is as follows:



We have identified nine places where security can fit into this structure:



The nine security measures are described in detail earlier, but roughly they are as follows:

1 Link encryption. The physical layer or data link layer is encrypted.

2 Network or Transport security. Either NLSP (Network Layer Security Protocol) or TLSP (Transport Layer Security Protocol) is used to protect the lower layers.

3 MHS. The X.400 security is added to the Message Handling Service.

4 Data Link Application: Used by both the Ground-Air links and some of the Ground-Ground links.

5 Ground-Ground links. The users of the MHS can add their own security above the OSI stack.

6 IDRP. The security option within the Inter-domain Routing Protocol is used, including the proposed use of IDRP authentication.

7 OSI network management. The management information can be specifically protected by OSI NM security facilities in the Systems Management Application in four possible ways:

a) make all management information remotely read-only

b) protect access to Managed Objects by producing multiple "view" Managed Objects, one for each type of access

c) authenticate access to Managed Objects at session start-up

d) authenticate access to Managed Objects for each management action performed on Managed Objects.

8 Alternative routing. Not strictly a security service, but the provision of multiple routes and dynamic re-routing does offer some protection against some attacks.

9 Access control: access to various resources can be controlled —

a) ensuring that only authorised users have access to hosts, and ensuring that once on such hosts, users can only do what they are supposed to do

b) layer 3 switches allow only certain routes

c) final destination controls access

d) MHS store/fwd units control routes and access.

8.2.1 MHS (X.400)

This table describes attacks to the MHS messaging system as a whole. This carries ground-to-ground data, and is generally not time-critical.

	Impact	Air Links	Ground Links	Routers	Other Hosts/ Users	Sys Man't & IDRP	MHS store/fwd
Modifications	M		L 1235	M 235			M 35
Replay	L		M 1235	M 235		H 235	M 35
Jamming	L		M 8	M 8			
Masquerade	M		M 1235	M 235	H 359a	H 235	M35
Flooding	L		M 1†8†	M 8†	H 8†9ad	H	M 9d†
Other DoS	L		H 8	H 8†		H	H

† = risk reduction, not removal

8.2.1.1 Impact

The main impact on security of MHS attack is through sending *incorrect* information. Failing to send information is less critical in general, as the information is supportive (flight plans, met data, etc.) rather than real-time control (climb to flight level x, etc.) Hence modification and masquerade are classified M, and the remainder L. Replay, although it can be used to send incorrect data, is less of a threat due to the variability of the data and the likelihood that replay will be obviously invalid.

8.2.1.2 Attacks

1 Air to ground messages don't use MHS, and so there are no attacks on MHS via the air links.

2 Modifications on ground links are hard because it involves on-the-fly altering the message on a wire. Replay and masquerade are easier because they can be done at a time that suits the attacker. The easiest DoS attack is to cut the wire.

Ground links can be protected against modification, replay and masquerade equally by security at four layers. Flooding can be protected slightly by link encryption because it stops ill-formed messages from entering. All DoS attacks can be reduced by alternative rerouting at the network layer, provided alternative routs exist and DoS can be detected.

3 Routers make modification easier than on the ground links because the message has already been stopped and held — otherwise the attack is like a ground link.

Link encryption has already been stripped off at a router, so this gives no protection. Otherwise, it is like ground links.

4 Other hosts/users cannot touch normal messages, and so can only insert spurious ones, i.e. masquerade and flooding.

As the users are genuine, only high level security protects against masquerade. In addition, preventing the unauthorised user from gaining access stops masquerade.

Store and forward units can perform some access control and can stop some unauthorised flooding.

5 Even if system management or IDRP is compromised, MHS messages cannot be modified en route. However, anything else (re-routing, replay, false insertion) can be done very easily.

Replay and masquerade can still be countered as for ground links. The DoS attacks can't now be protected by alternative rerouting because system management or IDRP can be used to circumvent the protection.

6 If the store and forward units are attacked, messages can be routed and modified at will. Given the high level of attack, only the high level protection works. Some protection against flooding is afforded by other store/fwds controlling access. As X.400 doesn't support dynamic rerouting, other DoS attacks can't be countered by rerouting.

8.2.2 DLA

This table describes attacks on the DLA system, which carries data to and from aircraft, including the ground-to-ground hops. This data is frequently time and safety critical.

	Impact	Air Links	Ground Links	Routers	Other Hosts/ Users	Sys Man’t & IDRP	MHS system
Modifications	H	L 124	L 1245	M 245			
Replay	H	H 124	M 1245	M 245		H 245	
Jamming	M	H 8†	M 8	M 8†			
Masquerade	H	M 124	M 1245	M 245	H 2459a†	H 245	
Flooding	M	H 1†8†	M 1†8†	M 8†9b†	H 8†9ab†	H	vL
Other DoS	M	M 8†	H 8†	H 8†		H	

† = risk reduction, not removal

8.2.2.1 Impact

DLA data includes time critical, safety critical communications and so the impact is higher than MHS messages. Invalid data is worse than no data, so the DoS attacks have a lower impact than those that feed invalid data.

8.2.2.2 Attacks

1 Air-ground links are only weakly susceptible to modifications (as it is hard to modify a radio transmission in flight), but can be attacked easily for replay, jamming and flooding, as the medium is open. Other DoS are hard as there is no

physical medium to attack, and masquerade just requires more sophistication than replay.

Modification, replay and masquerade can all be protected by security mechanisms at various levels, and the DoS attacks can be partially countered by alternative routing. However, alternative routing is only an option if there are alternative routes, which there may not be for many of the air-ground links.

2 Ground links are slightly less easy to tap into than the air links, and we have identified an additional placement of security above the stacks in ground-ground communications. Other than these differences, the ground leg of DLA communications is much like the air leg.

3 Routers can be attacked for DLA in a similar way to MHS, and can be protected similarly, too. Flooding can additionally be countered with level 3 access control, as the level 3 routers are under the control of the ATN authority.

4 Other hosts can masquerade and flood (as with MHS, other hosts can't access existing messages) and can be countered in a way similar to MHS.

5 Attacks on system management and IDRP cannot modify messages, but can reroute and insert new messages. Rerouting (flooding and DoS attacks) cannot be protected against by alternative routing because this mechanism is already assumed compromised.

6 There is a very low chance of flooding if MHS store/forward centres are compromised through MHS messages clogging the level 3 switches, and hence blocking DLA messages, but it is hard to imagine this in practice.

8.2.3 System Management

This table describes attacks on the system management functions, i.e. the management of the network.

	Impact	Air Links	Ground Links	Routers	Other Hosts/ Users	IDRP	MHS system
Modifications	H	L127d	L 127d	M 27d			
Replay	M	H 127d	M 127d	M 27d			
Jamming	L	H 8†	M 8	M 8			
Masquerade	H	M 127cd	M 127cd	M 27cd	M 27cd	H 27cd	
Flooding	L	H 1†8†	M 1†8†	M 8†9ab†	H 8†9ab†	M 8†	vL
Other DoS	L	M 8†	H 8†	M 8†		H	

† = risk reduction, not removal

8.2.3.1 Impact

Altering or inserting system management messages can severely disrupt the network. Replaying past messages have less of an effect, given the wide range of management messages possible. It also depends upon the time frame for replay — sending a close-down-switch message five minutes after the correct close-down-switch message was sent probably has little effect, whereas sending it five days later is as bad as modification or masquerade. DoS is second-order, in that it may prevent correction of some other problem, but isn't a problem in itself.

8.2.3.2 Attacks

1 It is believed that system management messages will travel over the air links. It is easier to insert and replay than modify air-link messages, and it is easy to jam or flood. Other DoS attacks are harder, with no physical medium to attack. Low level encryption protects against the modification/insertion. If high level security is used, only the more powerful OSI management security on a per-action basis can protect against modification and replay of messages. Masquerade of a whole transaction can be protected by transaction based authentication, but his still leaves open inserting a false message in the middle of a genuine transaction.

Rerouting can protect against DoS attacks, where alternative routes exist.

2 Ground links are harder to attack than the air links, but in other respects the threats and protections are the same.

3 Routers are similar to ground links, except that modifications are easier (because messages are at least temporarily stored) and lower level encryption is inappropriate. Access control to the router can also protect against flooding.

4 Other hosts can attack system management only by sending their own messages (they haven't got access to existing messages) which can be countered by transaction based security.

Flooding can be countered by rerouting and some access control — either at the host itself or at routers.

5 If IDRP has been compromised, masquerade of system management messages is easy, because the routing tables can lie about addresses. This can, however, be countered using transaction based security.

Flooding can be partially protected by rerouting. IDRP compromises can deny system management access completely by not routing messages at all.

6 Compromise of the MHS system has a small likelihood of flooding and stopping system management messages.

Security protection 7a, which makes remote system management read-only, generally reduces the impact of any system management compromise, rather than alters the ease of compromise.

8.2.4 IDRP

This table describes attacks on the automatic routing, IDRP.

	Impact	Air Links	Ground Links	Routers	Other Hosts/ Users	Sys Man't	MHS system
Modifications	H	L 126	L 126	M 26			
Replay	H	H 126	M 126	M 26		H 26	
Jamming	L	H 8†	M 8	M 8†			
Masquerade	H	M 126	M 126	M 26	M 26	M 26	
Flooding	L	H 1†8†	M 1†8†	M 8†9ab†	H 8†9ab†	H	vL
Other DoS	L	M 8†	H 8†	H 8†		H	

† = risk reduction, not removal

8.2.4.1 Impact

The impact of replay on IDRP is higher than on system management because of the more limited range of IDRP messages. However, the comments on time frame given under system management are still applicable.

In other ways, IDRP is affected in a similar way to system management.

8.2.4.2 Attacks

IDRP can be attacked in the same way as system management, and can be protected on a per-message basis using the IDRP security option. The only difference is in the last-but-one column, where IDRP can be attacked through compromise to system management. In this case, replay and masquerade of IDRP messages is easy, and in each case can be countered by layer 3/4 encryption or the IDRP security option (which works on a per-messages basis). But system management compromises can deny IDRP service through routing, flooding or switching off relevant services.

Although it isn't possible to modify IDRP messages via system management, it is possible to alter the static routing tables that IDRP relies upon, thus modifying the effect of IDRP messages, but not their content. This has not been reflected in the above table as it is not strictly modification.

Router attacks (third column) on IDRP have one further form, in which the compromised router sends out valid IDRP messages (as a router it is able to do this) containing invalid routing information. This is not masquerade, because the router does not pretend to be something it is not. This can be countered partially by 9a and 9c — access control on the router and by other routers.

8.2.5 Summary

The four tables in this section can be summarised by identifying those attacks for which the impact is high or medium and the vulnerability is high or medium. Doing this we can see the following:

- MHS (X.400 messages) are most at risk from modification and masquerade. These threats can be adequately countered using mechanism 3, the X.400 security options.
- Air traffic control messages (via DLA) are at risk from all forms of attack. Modification, replay and masquerade can be countered using the mechanism described in section 3, "Urgent Countermeasures". The threat of Denial of Service can be lessened by alternative routing (provided alternative routes exist), and by specifically protecting system management and IDRP (see below). The DoS attacks may still have an impact, though.
- System management is most at risk from modification, replay and masquerade. This can be countered by mechanism 7, the OSI system management security options, using message-by-message authentication (not just authentication per session).
- IDRP is also at risk from modification, replay and masquerade. In this case the IDRP security options can work on a message-by-message basis between routers and hence achieve suitable protection.