ATNP/WG 2/WP 445

March 11, 1998

AERONAUTICAL TELECOMMUNICATION NETWORK PANEL

WORKING GROUP 2 (Internet Communication)

Rio de Janeiro, Brazil, 15 – 19 March 1998

IDRP SECURITY

Agenda Item: 6.1

Prepared by: James Moulton

Presented by: James Moulton

SUMMARY

This document presents a proposed solution to the requirement for IDRP authentication exchanges. In particular, the proposal provides for complete ground-to-ground authentication and for airborne router IDRP authentication. The proposed solution does not address IDRP authentication of air-ground routers to airborne routers.

1 Introduction

WG 2 has concluded that IDRP exchanges should be authenticated to ensure that routing information is only from authorized IDRP routers. The means of authenticating routing information is by using type 2 authentication as described in the IDRP specification.

In order for this solution to be effective, certificate information about IDRP routers must be available. This paper discusses issues and potential solutions to how the certificate and key information required for authentication can be made available to the IDRP routers.

2 Problem

The general problem is one of certificate and key management. The general problem is how to the exchange of certificate information needed for authenticating data exchanges.

The general problem can be broken down into several more manageable problems in the case of IDRP routers:

- definition of X.509 certificates for use by routers,
- ground to ground router key management, and
- air to ground router key management.

2.1 Definition of X.509 certificates for use by routers,

This problem is two-fold. First, there is the issue of the style and substance of the certificate; and second to what the certificate is attached.

For use in the ATN, it has already been decided that the X.509 standard certificate definition will be used. This certificate definition defines both the format and content of the certificate.

The next problem is where should the certificate for IDRP routers be defined. The potential solutions is either: the pilot's certificate, the airframe's certificate, or the router's certificate.

2.2 Ground to ground router key management

The problem with ground to ground key management is one of the more simple problems. The issue is how to retrieve and use the X.509 certificate information.

2.3 Air to ground router key management.

The problem with air to ground key management is based on the fact that key exchanges take both time and bandwidth. In the case of ground to ground routers, this is not an issue since the router connectivity rarely changes, and the bandwidth needed to exchange certificates is not limiting. In the air to ground case, connectivity is changing relatively frequently and the changes require multiple key exchanges. Further key exchanges will also require directory searches to gain key information.

3 Proposed Solutions

3.1 Definition of X.509 certificates for use by routers

It is proposed that each IDRP router be assigned a unique X.500 directory entry. Associated with each entry will be an X.509 certificate that is used for authenticating communications from that router.

Rationale:

For the ground, this is straight forward as each router will have associated with it a unique address. For the air, contributions have been made as to whether the certificate should be either an airframe certificate or a pilot certificate. It has been shown that the pilot certificate is not optimal since information about that certificate may not be known at the time of initial IDRP exchanges. In the case of airframe certificates, this would only work

is a limitation of one IDRP router per aircraft is enforced. Otherwise confusion may result in two routers with different addresses using the same certificate.

By attaching the certificate to the router, it is possible to "hard code" the information in the router and the router can use its certificate information without having to access any other aircraft or ground resources.

3.2 Ground to ground router key management

Ground to ground routers can establish connections and exchange routing updates using the X.509 certificates found in the X.500 directory. When establishing an IDRP connection, a router sends his certificate information encrypted in the public key of the destination router. The destination router decrypts the information using his private key and retrieves the certificate. The certificate information is compared against the certificate retrieved from the X.500 directory and if it matches, returns his certificate encrypted using the other router's public key.

The ground to ground router key management system relies on the existence of the X.509 certificates in the X.500 directory and that each router can access the directory to retrieve the certificate information.

3.3 Air to ground router key management

The exchange of certificates within the air ground environment is the most difficult problem due to the bandwidth limitation between the aircraft and the ground; and due to the relatively short period for IDRP router-to-router connections. For this reason, a standard X.500 approach may not be the most appropriate.

A number of potential solutions were analyzed to determine the most appropriate solution.

3.3.1 Proposed Solution #1 – Preloaded Certificates

In this case, an aircraft would be preloaded with the certificate information for each air-ground router in existence. If one makes the assumption that for the next 20 years the maximum number of air-ground routers will be 100 or less, this should not be an insurmountable task. If one assumes that the number is too large, it would be possible using existing PC Card technology to have a card containing 20-40 certificates that could loaded at the gate.

Rationale

With preloaded certificates, the operation of the routers would be same as for the ground-to-ground case without the X.500 lookups.

3.3.2 Proposed Solution #2 – Dynamic Loading of Certificates

This solution is based on the ability of the aircraft to request each certificate from the ground either as it is needed, or in a bulk data transfer. In this case, either X.500 or some ATN specific communication would be used to request and receive certificate information based on a request from the aircraft.

If certificates are requested on each contact of an IDRP router, then some sort of directory look-up will be required before initiating the connection request. This will require the availability of air-ground communication and will require the certificate to be retrieved and sent to the aircraft.

If the certificates are request in bulk, a list of possible routers needs to be generated based on the route of flight. These certificates would need to be stored in a cache and made available as needed during the route of flight.

3.3.3 Proposed Solution #3 – Session Keys

The third solution is based on the airborne router selecting a session key for use during the route of flight. This session key would be encrypted using the certificate of the of the airborne router and passed to the air-ground router. The air-ground router would be responsible for passing the session key to other IDRP routers along the proposed route of flight.

Rationale

This solution does not require any certificate information on the aircraft except the certificate of the router itself. The solution also requires the exchange of the session keys between routers along the path of the flight. If for some reason the movement of the session keys fails, authentication is not available.

3.3.4 Solution #4 – Airborne router authentication.

This solution is based on the assumption that the most critical element that needs authentication is an airborne router to an air-ground router. In this case, the airborne router can authenticate itself with just its own certificate. The airborne router encrypts it certificate using its private key and places is it in the ISH. The air-ground router decrypts the certificate using the airborne router's certificate that it retrieves from the X.500 directory. If the certificate is valid, then the airborne router is authenticated and for each routing update, the airborne router will use its private key to digitally sign the IDRP pdu.

Rationale

This approach provides a certain amount of security without the need for any exchange of certificate information across the air-ground link. The deficiency to this approach is that there is no way to authenticate the identity of the air-ground router without any certificate information.

4 Recommendation

The WG is invited to consider solution #4 – Airborne Router Authentication as the agreed approach to IDRP authentication. This approach is considered superior in the utilization of the air-ground link and the least disruptive to the current environment while adding an additional level of security by providing a means of authentication of the airborne router.

The use of airborne router authentication provides security to the air-ground router from unauthorized attempts to connect and propagate erroneous routing information. It conserves both bandwidth and connection request timing.