WG1/SG2 WP___
WG2/**WP 488**

International Civil Aviation Organization
Aeronautical Telecommunication Network Panel (ATNP)
WG2 and WG1/SG2 Meetings
Honolulu, Hawaii, USA
January 1999

Symmetric Mechanisms for Authentication in IDRP

Presented by Tom McParland

Summary

The draft SARPS materials require that digital signatures based on public-key cryptography be used as the authentication mechanism for IDRP authentication. Although, the use of digital signatures follows naturally from the adoption of the X.509 authentication framework, their use may not be optimal in all cases where authentication is to be performed. This paper outlines a hybrid approach which uses an asymmetric algorithm for key distribution and connection establishment and a symmetric authentication mechanism for routing information exchange.

1. Introduction

The draft SARPS materials require that digital signatures based on public-key cryptography be used as the authentication mechanism for IDRP authentication. Although, the use of digital signatures follows naturally from the adoption of the X.509 authentication framework, their use may not be optimal in all cases where authentication is to be performed. This paper distinguishes key distribution from connection establishment messaging and routing information exchange messaging, thereby, identifying three environments for IDRP authentication. Within this context, asymmetric and symmetric mechanisms are examined in terms of their operating characteristics. It is proposed that while asymmetric authentication may be appropriate for key distribution, it may not be optimal for authentication of connection establishment messaging in select situations and it is generally not optimal for authentication of routing information exchange messaging. Rather, in these cases, given that non-repudiation is not necessarily required and given the general characteristics of asymmetric cryptography especially with respect to bandwidth limitations of the ATN, symmetric authentication techniques may be more appropriate.

2. Discussion

2.1 Current Requirement for Digital Signature

ATNP WG1/WP14-08, which presents draft text for Sub-Volume VIII of Doc 9705, contains the following:

> 8.3.1.5.1.1 ATN Boundary Intermediate Systems (BISs) supporting ATN security services shall support the use of ATN security provisions for authentication, using digital signatures, of routing exchanges between air-ground and ground BISs and from airborne BISs to air-ground BISs, but not vice versa, as defined in Sub-Volume V.

This requirement specifies the explicit use of digital signatures to provide IDRP authentication.

2.2 Digital signatures

Annex B (clause B.3.d) in X.509, describes digital signature as follows:

> "This mechanism involves the encipherment, by the originator's private key, of a compressed string of the relevant data to be transferred. The digital signature together with the plain data is sent to the recipient. Similar to the case of the data integrity mechanism, this message can be processed to prove integrity. The digital signature mechanism also proves the authenticity of the originator, and the unambiguous relationship between the originator and the data that was transferred.

The authentication framework supports the digital signature mechanism using an asymmetric scheme.

The digital signature mechanism supports the data integrity service but also supports the non-repudiation service."

2.3 Non-repudiation service

From a security service perspective, it is the non-repudiation aspect of (asymmetric) digital signature mechanisms which distinguishes them from symmetric origin authentication mechanisms. It is proposed that although non-repudiation is generally desirable for key distribution, it is not required for authentication of IDRP connections and routing exchanges.

2.4 Characteristics of Asymmetric Mechanisms

The clear advantage of public-key cryptography is in the area of key distribution. In particular, on an ATN-wide basis, only private keys need be kept secret while public keys may be readily distributed provided they are authenticated. The disadvantage of public-key encryption methods (at least those in general use) is their computational overhead and relatively large key sizes.

Within the ATN IDRP environment, the computational performance of public-key encryption is a particular concern for ground-ground routers. In ground-ground operation, it is expected that there will be a significant number of Update BISPDUs to advertise or withdraw routes to aircraft. Thus, the requirement to perform public-key transformations could adversely affect performance, expecially of backbone routers. This is probably less of a concern in air-ground operation since it must be performed at any rate for initial key distribution and the there will be a minimal number of BISPDUs exchanged after the connection is established. In addition, the current requirements only call for single-entity authentication.

Signature size is of particular concern in both the air-ground and ground-ground environment. RSA may be considered as an example where signature size is a function of the key length (See Annex D of X.509)
The RSA public and private keys are ordered pairs consisting of a public (e) or secret exponent (d) and an arithmetic modulus (n) as follows:

$$\text{Public Key} = \{e, n\}$$
$$\text{Private Key} = \{d, n\}$$

RSA encryption uses the public key parameters to convert a plaintext message M to ciphertext C as follows:

$$C = M^e \pmod{n}$$

Conversely, RSA decryption uses the private key parameters to convert ciphertext to plaintext as follows:

$$M = C^d \pmod{n}$$

The data block length, i.e., the length of *C* or *M*, will be determined by the modulus. Thus even a conservative length of *n*, such as 512 bits, could result in data expansion. This is a particular problem for IDRP Authentication Type 2 which has a fixed size of 128 bits for the validation pattern field.

Similar problems exist, for example, with the NIST Digital Signature Standard (DSS). As specified, DSS uses the Secure Hash Algorithm (SHA) with a 160-bit message digest.

Based on these considerations, it is proposed that WG1's algorithm analysis place special emphasis on signature size. In the event that a suitable, non-expanding public key algorithm can not be identified, the remaining section of this paper proposes an alternative hybrid approach to IDRP authentication

3. IDRP authentication using symmetric techniques

3.1 General operation

The general approach for air-ground operation is to transfer a symmetric "session" key during the IDRP Open exchange and (if required by local security policy) to apply a symmetric authentication algorithm to accomplish Type 2 Authentication for all subsequent BISPDUs. This approach requires a public key cryptosystem which is reversible and therefore would eliminate signature systems such as DSS which only provide a signature service do not provide for encryption of a session key
The general operation is in an air-ground environment consists of the following steps:

1. During the ISH exchange, the Air-ground and Airborne Routers signal their support for strong authentication.

2. The Air-ground router retrieves the aircraft's public-key certificate from a supporting directory service. The Air-ground router authenticates the aircraft's certificate using the certificate authority's public key.

3. The Air-ground router generates a symmetric session key[1] and encrypts the session key using the aircraft's public key.[2]

4. The Air-ground router sends an Open PDU with Code 2 in the Authentication Code[3] field and with the encrypted session key in the Authentication Data field. [4]

5. The Airborne router sends an Open PDU with Code 2 in the Authentication Code field and its digital signature in the Authentication Data field.

6. Upon receipt of the Open PDU, the Air-ground router authenticates the aircraft's signature using the aircraft's public key. If authentication fails, the connection is terminated.

7. The Airborne and Air-Ground routers include an authenticator as the Validation Pattern field in the header of all subsequent BISPDUs. The authenticator is generated using the symmetric session key.

Note 1: Procedures for dynamic session key generation must be developed.

Note 2: As noted above not all public-key algorithms have the property of permutability.

Note 3: Type 2 Authentication is not applied to the Open PDU itself.

Note 4: In this scenario only single entity authentication of connection establishment is performed. If mutual authentication were performed, the Air-ground router's certificate and digital signature would be sent.

For ground-ground operation, a symmetric key could be installed through system management with application of appropriate access controls. Type 2 authentication using a symmetric algorithm is then performed on all BISPDUs ,

3.2 Candidate cryptographic systems

The selection of cryptographic algorithm(s) is the subject of a separate ongoing ATNP WG1/SG2 activity. The IDRP standard (ISO 10747) provided a fixed length field of 128 bits to carry the authentication pattern thus placing a constraint on the cryptographic algorithm selected.

3. Recommendations

1) WG1 should attempt to identify a single asymmetric algorithm which is computationally and bandwidth efficient, with particular attention to the signature size. Requirements for the associated authentication procedure should also be identified.

2) If a suitable asymmetric mechanism can not be identified, then WG1 should make provision for use of an asymmetric algorithm for key distribution and connection establishment and of a symmetric authentication mechanism for routing information exchange.

3) If the item 2 alternative is selected, then WG1 should define requirements for session key generation

4) WG2 is invited to note the alternatives of asymmetric vs. symmetric authentication mechanisms for routing information exchanges and provide feedback to WG1/SG2 as deemed appropriate.