WG2 WP 518b
WG1/SG2 WP 1309b

Aeronautical Telecommunication Network Panel (ATNP)
Working Group 2 and
Working Group 1/Sub-Group 2
Meetings
Naples, Italy
May 1999

IDRP Authentication Scenarios Using A Key Agreement Scheme And A Keyed Message Authentication Code (Revision b)

Presented by Tom McParland

Summary

IDRP Air-Ground authentication scenarios are presented which employ the Elliptic Curve Key Agreement Scheme – Diffie-Hellman Version (ECKAS-DH1) and the Hashed Message Authentication Code (HMAC).

1. Introduction

Working Paper 488, "Symmetric Mechanisms for Authentication in IDRP" was provided to ATNP WG2 and WG1/SG2 at the January meeting. This paper outlined a hybrid approach to authentication using an asymmetric algorithm for key distribution and connection establishment and a symmetric authentication mechanism for routing information exchange. The scenario presented in WP 488 used key transport to establish a symmetric session key during the OPEN PDU exchange. The symmetric key would then be used to form a Type 2 authenticator which would be included in all subsequent BISPDUs. Digital Signatures were used for peer entity authentication.

Since the January meeting, ATNP WG1/SG2 has progressed the selection of ATN cryptographic algorithms primarily through examination of Upper Layer scenarios. Based on this work, WG1/SG2 has recommended asymmetric session key establishment using a key agreement scheme (specifically the Elliptic Curve Key Agreement Scheme – Diffie-Hellman Version (ECKAS-DH1)) and symmetric authentication using a keyed message authentication code scheme (specifically HMAC).

This paper presents IDRP authentication scenarios using key agreement and keyed message authentication code schemes. Scenarios are presented for both air and ground initiated IDRP connections providing mutual and unilateral peer entity authentication. The scenarios also provide replay and intercept protection.

This version (b) contains updates resulting from WG2 discussion. This version includes provision to signal whether access to pre-stored data or a supporting directory of public key certificates is available during the ISH exchange and to signal availability of a specific certificate during the IDRP OPEN exchange. This version updates a prior version (a) which modified the original version. The previous update presented scenarios wherein the same authentication data is sent in OPEN BISPDUs independent of whether the connection is air or ground initiated. This balanced approach permits recovery of an IDRP connection by either side. This feature is required for one of the proposed solutions to PDR 99010005 (re: WG2 Working Paper 513). The consequence of this approach is that peer entity authentication occurs on the first UPDATE BISPDU for both IDRP peers.

2. Discussion

2.1 Intermediate System Authentication Requirements:

The following requirements have been proposed as draft Intermediate System security requirements in Sub-Volume VIII (Re: SG1/WG2 WP 1310).

> 8.3.1.5.1.1 If an ATN Boundary Intermediate Systems (BISs) supports ATN security services, it shall support the ATN Key Agreement Scheme (AKAS) and the ATN Keyed Message Authentication Code Scheme (AMACS).

8.3.1.5.1.2 If an ATN Air-Ground BISs supports ATN security services, it shall support peer entity authentication of Airborne BISs.

Note. — The requirement is for single entity (unilateral) authentication of airborne BISs by Air-Ground BISs. Although no requirements are defined herein for peer entity authentication of Air-Ground BISs by Airborne BISs, it is not precluded.

8.3.1.5.1.3 If an ATN Air-Ground or Ground-Ground BIS supports ATN security services, it shall support mutual entity authentication of a peer Ground-Ground or Air-Ground BIS which supports ATN security services.

8.3.1.5.1.4 If an ATN BIS supports ATN security services, it shall support data origin authentication of routing information exchanges.

8.3.1.5.1.5 If an ATN BIS supports ATN security services, it shall support protection of authentication exchanges from replay and interception attacks.

2.2 Authentication Mechanisms

2.1.1 Entity authentication

Entity authentication can be achieved in asymmetric cryptographic environment by the claimant demonstrating possession of a private key. In the following scenarios, ATN intermediate systems demonstrate possession a shared secret key by using the key in an HMAC seal. Possession of the shared secret key implies possession of a specific private key since the shared secret key could only be successfully derived (using ECKAS-DH1) if the claimant is also in possession of a private key corresponding to a verified public key. Verification of the claimant's public key is accomplished by obtaining it from a trusted third party, i.e. in a certificate signed by a certificate authority.

2.1.2 Data Origin Authentication

Data origin authentication is achieved in the following scenarios using HMAC as the Type 2 IDRP authentication mechanism. Note that data origin authentication is provided even if single entity authentication is performed, i.e., the HMAC seal is applied to BISPDUs in both directions following the Open exchange.

2.1.3 Replay and Interception Protection

Protection from replay and interception attacks is provided in the following scenarios through a challenge-response exchange. A random variable generated by the verifying intermediate system is sent in an OPEN BISPDU. The variable is returned in a sealed response by the claimant in the first UPDATE BISPDU. Subsequent BISPDUs are protected by the IDRP sequence numbers.

2.3 Scenarios for Authentication Of Boundary Intermediate System Exchanges

2.3.1 Ground Initiated IDRP Connections

1. During the ISH exchange, the Airborne and Air-Ground routers signal either single entity or mutual authentication and whether access to pre-stored data or a supporting directory of public key certificates is available.

   Note 1. – If either router does not signal support for authentication in the ISH (i.e., a Package-1 router) then the IDRP connection will be established without security (i.e., with Type 1 authentication) unless the local policy of either router prohibits an unsecured service.

   Note 2. – If the Air-Ground router signals single entity authentication but the Airborne router signals mutual authentication, then the IDRP connection will be established with single entity authentication unless the Airborne router's local policy prohibits it.

2. The Air-Ground router retrieves the aircraft's public-key certificate, $Cert_{Air}$ from a supporting directory service. The certificate contains the aircraft's public key agreement key ($r_{Air}P$). The certificate is verified using the Certificate Authority's public key.

   Note. – If the Air-Ground router is unable to retrieve the aircraft's certificate, then the Air-Ground router will signal (step 4b) that the airborne router should send its public key certificate in the OPEN BISPDU if local policy permits it.

3. The Air-Ground router generates a random number $R_{A/G}$.

4. The Air-Ground router sends an OPEN BISPDU with:

   a. Code 2 in the Authentication Code field,
   b. the random number $R_{A/G}$ and the Air-Ground router's public key ($r_{A/G}P$) in the Authentication Data field if single entity authentication was signaled in the ISH exchange. If mutual entity authentication was signaled in the ISH exchange, the Air-Ground router's public key is sent in a certificate $Cert_{A/G}$; in the Authentication Data field. If the Air-Ground router was unable to retrieve the aircraft's certificate, it will also indicate that the certificate is required in the Authentication Data field.

   c. a Type-1 authenticator in the Validation Pattern field.

5. Upon receipt of the OPEN BISPDU, the Airborne router:

   a. generates a random number, R_{Air}
   b. computes the Diffie-Hellman shared secret value $Z=r_{Air}r_{A/G}P$

c. derives the session key $K=hash(Z||Cert_{Air}||r_{A/G}P||R_{Air}||R_{A/G})$

Note. – If a certificate was included in the OPEN BISPDU, it will be verified using the signing public key of the Certificate Authority.

6. The Airborne router sends an OPEN BISPDU with:

   a. Code 2 in the Authentication Code field,
   b. the random number R_{Air} and if required, its public key certificate in the Authentication Data field
   c. a Type-1 authenticator in the Validation Pattern field.

7. Upon receipt of the OPEN BISPDU, the Air-Ground router:

   a. computes the Diffie-Hellman shared secret value $Z= r_{A/G}r_{Air}P$
   b. derives the session key $K=hash(Z||Cert_{Air}||r_{A/G}P||R_{Air}||R_{A/G})$

   Note. – If a certificate was included in the OPEN BISPDU, it will be verified using the signing public key of the Certificate Authority.

8. The Air-Ground and Airborne routers send subsequent BISPDUs with the Airborne and Air-Ground random numbers and an HMAC seal over the BISPDU (including the random numbers) in the Validation Pattern field, i.e., $R_{Air,}R_{A/G},HMAC_K(R_{Air}||R_{A/G}||BISPDU)$.

2.3.2 Air Initiated IDRP Connections

1. During the ISH exchange, the Airborne and Air-Ground routers signal either single entity or mutual authentication and whether access to pre-stored data or a supporting directory of public key certificates is available

   Note 1 and Note 2 under 2.3.1 step 1 apply.

2. The Air-Ground router retrieves the aircraft's public-key certificate, $Cert_{Air}$ from a supporting directory service. The certificate contains the aircraft's public key agreement key ($r_{Air}P$). The certificate is verified using the Certificate Authority's public key.

3. The Airborne router generates a random number R_{Air}.

4. The Airborne router sends an OPEN BISPDU with:

   a. Code 2 in the Authentication Code field,
   b. the random number R_{Air} and if required, its public key certificate in the Authentication Data field
   c. a Type-1 authenticator in the Validation Pattern field.

5. Upon receipt of the OPEN BISPDU, the Air-ground router:

    a. generates a random number, $R_{A/G}$
    b. computes the Diffie-Hellman shared secret value $Z=r_{A/G}r_{Air}P$
    c. derives the session key $K=hash(Z||Cert_{Air}||r_{A/G}P||R_{Air}||R_{A/G})$

    Note. – If a certificate was included in the OPEN BISPDU, it will be verified using the signing public key of the Certificate Authority.

6. The Air-Ground router sends an OPEN BISPDU with:

    a. Code 2 in the Authentication Code field,
    b. the random number $R_{A/G}$ and the Air-Ground router's public key ($r_{A/G}P$) in the Authentication Data field if single entity authentication was signaled in the ISH exchange. If mutual entity authentication was signaled in the ISH exchange, the Air-Ground router's public key is sent in a certificate $Cert_{A/G}$; in the Authentication Data field.
    c. a Type-1 authenticator in the Validation Pattern field.

7. Upon receipt of the OPEN BISPDU, the Airborne router

    a. computes the Diffie-Hellman shared secret value $Z=r_{Air}r_{A/G}P$
    b. derives the session key $K=hash(Z||Cert_{Air}||r_{A/G}P||R_{Air}||R_{A/G})$

    Note. – If a certificate was included in the OPEN BISPDU, it will be verified using the signing public key of the Certificate Authority.

8. The Air-Ground and Airborne routers send subsequent BISPDUs with the Airborne and Air-Ground random numbers and an HMAC seal over the BISPDU (including the random numbers) in the Validation Pattern field, i.e., $R_{Air,}R_{A/G},HMAC_K(R_{Air}||R_{A/G}||BISPDU)$.

3. Conclusions

The above scenarios demonstrate that the IDRP authentication requirements can be met using the same key agreement and message authentication code schemes which have been recommended for Upper Layer use. As was the case with previously proposed key transport approaches, the impact will be that the aircraft needs to carry its own private key agreement key and the public key of the Air-Ground router's Certificate Authority (if mutual authentication is supported). The Air-Ground router will similarly need the public key of the aircraft's Certificate Authority and will require access to the supporting directory service.

4. Recommendations

1. It is recommended that both WG2 and WG1/SG2 consider the above scenarios and endorse or otherwise develop recommended changes to the draft Intermediate System Security requirements in Sub-Volume VIII.

2. If accepted, WG2 should develop corresponding Sub-Volume V ch9anges.