International Civil Aviation Organization

THE FIFTH MEETING OF AERONAUTICAL TELECOMMUNICATION NETWORK (ATN) IMPLEMENTATION CO-ORDINATION GROUP OF APANPIRG (ATNICG/5)

Kuala Lumpur, Malaysia, 31 May – 4 June 2010

Agenda Item 10: IP Sub-Network Planning

CONSIDERATIONS FOR INTRODUCING SECURITY INTO THE ASIA/PACIFIC REGIONAL GROUND ATN/IPS NETWORK

(Presented by Mark Brown – Japan)

SUMMARY

The introduction of Internet Protocol Suite (IPS) in the Asia/Pacific regional ATN network may potentially increase its vulnerability and require the introduction of security measures. This paper discusses resources that should be protected and means available to protect them. The issue of key management is also introduced. The paper recommends that the Asia/Pacific region should create a plan and policies for introducing security in the ATN IPS ground network, with policies to secure the network links and routeing information established as a matter of priority, before implementation of IPS begins.

1. Introduction

1.1 Currently, there are no technical security measures specified for the Asia/Pacific Ground ATN network. These have hitherto been considered unnecessary for a number of reasons:

- there is little knowledge of OSI protocols by potential attackers ("security by obscurity")
- connections between States use leased line circuits, which are not shared with other users and which require physical access to penetrate
- networking equipment (modems, routers) and hosts (end systems) are located in secure environments

However, the introduction of the Internet Protocol Suite (IPS) in the Asia/Pacific Ground ATN network is expected to increase its vulnerability, since the IPS protocols are well understood and a variety of tools are available to assist potential attackers.

1.2 It may therefore be necessary to review the need for security measures in the Asia/Pacific ATN. This paper presents some considerations for security in the Asia/Pacific ATN IPS ground network.

2. Cryptography-based Security Measures

2.1 In this working paper, the main security measures considered use cryptographic techniques to provide some or all of the following:

- **Authentication** verifies the identity of the sender
- **Integrity** prevents a message from being tampered with (altered). Protection can also be provided against *replay attacks*
- **Confidentiality** ensures that the message is only readable by those authorised to do so.

2.2 We consider the following threats:

- **Masquerade** (an attacker pretends to be another system)
- **Modification** of messages
- **Denial of service**

2.3 We consider the following resources that require protection from the above threats:

- **Network service.** Incorrect routeing information can disrupt the delivery of data across the network and can be used to mount a denial of service attack on the network.
- **Application messages (data).** Bogus messages can be generated, or messages modified. The potential seriousness of this is dependent upon the application: e.g. modification of real-time surveillance data carries an immediate flight safety risk, bogus flight plan information carries a much lower risk.

Note that confidentiality is not currently required in the ATN.

2.4 In the ATN IPS ground network, security can be implemented using Internet Protocol Security (IPsec). IPsec operates at layer 3 (the network layer), and can be used in two modes:

- **Transport Mode**, where an IP packet's payload (user data) is authenticated using a digital signature (hash) and optionally encrypted, but the IP header is left intact. Transport mode is typically used to secure communications between applications.
- **Tunnel Mode**, where an entire IP packet (header and payload) is secured by a digital signature and optionally encrypted, and is encapsulated in a new IP packet for transmission. This is typically used between routers and can be used to create Virtual Private Network (VPN) connections, but can also be used for end-to-end communication.

2.3 For end-to-end security of IPS applications, an alternative to IPsec is TLS (Transport Layer Security), which operates at layer 4 and provides authentication and confidentiality. In ICAO Doc 9896, TLS is optional for mobile nodes and correspondent nodes, but is not specified for ground-ground applications.

2.4 For ATS messaging, the AMHS Security Extended Service uses digital signatures to provide integrity (protection against modification), origin authentication (protection against masquerade) and sequence integrity (protection against duplication/loss) for messages.

2.5 To protect routeing information, ICAO Doc 9896 2.3.4.5 specifies that routers should authenticate routeing information exchanges using the TCP MD5 signature option (RFC 2385). According to RFC 4272 *BGP Security Vulnerability Analysis*, "This counters message insertion, deletion, and modification attacks, as well as man-in-the-middle attacks by outsiders". (However, RFC 2385 admits that it is a weak protection mechanism. Stronger mechanisms have been proposed, *viz.* Secure BGP (S-BGP) and secure origin BGP (soBGP), but neither has been adopted as an IETF standard so far.)

2.6 If PPP is used as the link layer (encapsulation) protocol between routers, the PPP Challenge-Handshake Authentication Protocol (RFC 1994) may be used as a simple method of authentication before a link can be used. CHAP also allows for periodic re-authentication using a different token.

3. Key Management

3.1 Cryptography-based technical security measures (*i.e.* all of the above apart from ACLs) use passwords or pieces of cryptographic information called *keys* to operate.

3.2 A shared key or password known to both peers may be used to protect a resource. The quality of the key (length, randomness) has a large impact on the security of the resource it is used to protect. It is desirable to share keys as little as possible (*i.e.* each resource should ideally be protected using a different key), and to periodically change the keys. (See RFC 3562 *Key Management Considerations for the TCP MD5 Signature Option*.)

3.3 A shared key or password must be communicated between the peers in advance. This is vulnerable to interception by a third party, who could then use the information to masquerade as one of the peers and gain access to the resource. *Public key cryptography* addresses this risk by using so-called *asymmetric encryption*: the key used to encrypt a message is different to the key used to decrypt it. Each party has a pair of key values that are mathematically related: a *public key* that it makes available to those that require access to the protected resource, and a *private key*, which it keeps secret. Asymmetric encryption can be used to protect a resource directly *(e.g.* a sender computes a message digest using its own private key which is verified by the receiver using the sender's public key) but is computationally intensive. Instead a *key-exchange algorithm* may be used whereby both peers use their own private key and the public key of the peer to generate a common shared key value. In this way, a computationally efficient shared key is used but its value is never directly communicated between the peers (only the public keys are communicated, and interception of a public key does not compromise the resource).

3.4 Key management (generating and distributing keys, updating keys periodically if necessary, and withdrawing old or vulnerable keys) is a major issue. A *Public Key Infrastructure* (PKI) is a system for creating, distributing and revoking keys. PKI uses *digital certificates*, which bind a public key with information such as the identity of the party associated with the public key, the certificate's validity, and a hash that is used to protect the certificate against tampering. ITU-T X.509, part of the X.500 series of directory services standards, specifies the formats of public key certificates, certificate revocation lists etc.

3.5 Shared key values or public key certificates may be manually installed in each system. With a PKI, however, it also becomes practical to store public key certificates in a repository and retrieved when necessary using directory services. This greatly simplifies setting up devices, but relying on a directory service creates a security vulnerability in itself.

4. Router Security Measures

4.1 Routers act as the "gatekeepers" of networks and are critical to its security. The US National Security Agency publishes a Router Security Configuration Guide[1] to help network administrators improve security. Some details are Cisco-specific, but information on the threats and countermeasures is generally applicable.

4.2 Access Control Lists (ACL) and packet filters may be used to ensure that resources can only be accessed by entities authorised to do so and prevent unauthorised traffic traversing the network. Similarly, route ingress filtering and egress filtering can be used to ensure that prefixes of inappropriate length are not propagated. Minimum ACL and filtering policies should be regional for consistency.

4.3 To ensure consistent deployment, a secure BGP+ template configuration for the region could be developed, *e.g.* similar to that developed by Team Cymru for BGP[2]. On the other hand, being vendor specific should be avoided.

5. Implementation Issues and Recommendations

5.1 Technically speaking security is by and large a "solved" problem – the difficulty lies in how to apply and manage it. Institutional rather than technical issues may be the major hurdle to implementing security. (That notwithstanding, there may be interoperability issues between equipment from different vendors, and even different software versions from the same vendor, due to varying interpretations of the standards and levels of implementation support. This is especially true for more recent protocols and those for which standards are still evolving.)

5.2 To introduce security in the Asia/Pacific region in a consistent way, it will be necessary to create a plan and policies: for example to specify what should be protected, how it should be protected, when security should be introduced, how things like keys should be generated, distributed and used, how to manage and audit security, and what measures should be taken in the event of a security compromise.

> Recommendation 1: *The Asia/Pacific region should create a plan and policies for introducing security in the ATN IPS ground network.*
> As a minimum, policy to protect network links, routers and routeing information should be established as a matter of priority, *before* implementation of IPS proceeds.

> Recommendation 2: *Policy and Guidance material and should be created for password and key management and use.*
> Resources will be protected by keys and passwords. Criteria should be specified for key generation (*e.g.* minimum length) and guidance given on tools available for generating passwords, shared keys and public/private keys. Guidance is also needed for the distribution of keys, the degree of key sharing permitted (whether a single key may be used to protect multiple resources) and the frequency of key replacement. Where keys are exchanged between two sites, template agreements on key management should be developed.

Practically, it is considered that keys would initially be managed bilaterally/multilaterally, but eventually a regional key management function could be established.

---

[1] http://www.nsa.gov/ia/guidance/security_configuration_guides/cisco_router_guides.shtml

[2] http://www.team-cymru.org/ReadingRoom/Templates/secure-bgp-template.html

6. Conclusions

6.1 The meeting is invited to note the information in this report, and to recommend that the Working Group proceed to draft initial security policy, standards and guidance material.

– – – – – – – – – – – –