AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL

WORKING GROUP 3 (APPLICATIONS AND UPPER LAYERS)
Gran Canaria, Spain
September 27 - October 1, 1999

CM Security Approach

Prepared by: G. Saccone

SUMMARY

This paper gives an overview of how CM will work with the package 2 security modifications and an indication of the CM SARPs changes necessary.

1. Introduction

The security subgroup has outlined an approach for adding security to the ATN. In order to minimize impacts on air-ground applications, CM will be responsible for providing the initial exchange of necessary security information. In particular, the CM-logon service will be modified to function as an authenticated key establishment protocol in addition to the function of passing application information between aircraft and ground systems. This paper gives an overview of the process as it relates to CM, the impacts on CM, and a high level description of the changes that will be required to the CM SARPs. Details of the entire security architecture and process can be found in the corresponding security subgroup papers.

2. Discussion

The security for the ATN is designed to have minimal impact on the ATN applications. The Security Requirements parameter of the existing dialogue service D-START primitives will be used to indicate that security is to be provided. At present, it is envisioned that a package 2 CM will always attempt to use security. This means that if a package 2 aircraft wishes non-secure ATN operation, it must perform a package 1 logon, and no package 2 features may be used. This paper only covers the secure CM-logon and CM-contact services, as details for the CM-forward and CM-update services are being developed.

3. CM Secure Logon

This section gives a walk through of the secure CM logon process. Security subgroup documents will take precedence in the case of any discrepancies between this paper and those of the security subgroup.

A package 2 CM-air-user invokes a secure CM-logon request. The secure CM-logon request PDU will be identical to the package 1 CM-logon request PDU. A new parameter, the Security Requirements parameter, will be added to the secure CM-logon request primitive. This parameter indicates the desire to perform a secure CM-logon. Again, currently for package 2 this parameter must be present and indicate a desire to have security, so the CM-air-user does not have to provide this parameter; the CM-air-ASE will. Therefore the only difference between the secure CM-logon service and the package 1 CM-logon service is the addition of the Security Requirements parameter to the D-START service.

The information in the secure CM-logon request is passed to the CM-air-ASE, which invokes the D-START request with the given information and also sets the Security Requirements parameter to the abstract value "Exchange supporting key management". The D-START request is passed by the control function (CF) to the security ASO. The ASO then performs its security functions (e.g. signature) and passes the dialogue primitive to the peer ground CM application.

Upon receipt of the D-START request, the ground CM security ASO sees that a secure connection is being requested. The security ASO must have information provided by its

certificate authority in order to verify the signature of the aircraft and obtain the aircraft's key. The provision of this information to the security ASO will be a local implementation function, but will probably be done using the Directory service of Subvolume 7. These checks are done for the aircraft CM application only; the other applications will have to be checked by the CM-ground-user.

If there are any problems with the certificate checks, the security ASO will abort the connection. No specific reason will be given to the peer aircraft CM application, as the aircraft is then deemed to be an untrusted user. If all checks are completed satisfactorily, the ground CF issues a D-START indication with the Security Requirements parameter as set by the CM-air-ASE. The D-START indication is then passed to the CM-ground-ASE.

Note that if the CM-ground-ASE is package 1, the D-START parameters will get passed directly to the CM-ground-ASE by the dialogue CF. Since the Security parameter is extraneous to a package 1 CM-ground-ASE, it will simply be ignored. No protocol error will result. Since the user data of a package 2 logon will be identical to that of a package 1 logon, a package 1 CM-ground-ASE will be able to decode the package 2 user data. Accordingly, a package 1 CM-ground-ASE will reject a package 2 D-START request, so the aircraft user will receive a CM-logon response with an indication of the ground's CM-ASE version number. Therefore, the aircraft will know that only unsecured ATN is available, and the package 2 enhancement which allows CM to operate in a degraded package 1 mode will apply. This means that the proposed CM package 2 security modifications will be backwards compatible with CM package 1.

If the CM-ground-ASE is a package 2 or higher CM ASE, then the CM-ground-ASE will create a CM-logon indication with the provided D-START parameters, including the Security Requirements parameter. Upon receipt of the D-START indication, the CM-ground-ASE first ensures that the value of the Security Requirements parameter is correct. If it is not correct, but the primitive has passed the security ASO (which is must have done since the ASE now sees it), the CM-ground-ASE must abort the connection. The package 2 CM-ground-ASE does not have the option to proceed with a lower level security CM exchange; if this is required the aircraft will to have perform a package 1 CM-logon service and operate in a degraded mode.

If the security choice is acceptable, then the CM-ground-user distributes the application information to the other application users. For each supported application, the CM-ground-user must then retrieve the key agreement public key certificate (KAPKC) from the Directory, verify the certificate path (the details are in Subvolume 8), and check the Certificate Revocation List (CRL) (which verifies that the KAPKC isn't revoked). The other applications can then perform their own secured services with this information.

The CM-ground-user will then initiate the secure CM-logon response. This will consist of the package 1 CM-logon response with the addition of security information in the user data (e.g. the 21 octet public key for each application, and a boolean flag for each application indicating whether or not the key is used for all instances of that application

in the CM domain) and the Security Requirements parameter (indicating acceptance of the secure CM service). The CM-ground-ASE constructs the D-START response primitive, which is then given by the CF to the security ASO. After appropriate security calculations are performed the primitive is sent to the peer aircraft CM application.

Upon receipt of the secure D-START response containing the secure CM-logon response data, the aircraft security ASO performs security calculations. If there are any calculation problems, the security ASO aborts. If there are no problems, the security ASO releases the D-START response to the CF which then releases the corresponding D-START confirmation to the CM-air-ASE.

If the secure logon has not been accepted by the peer ground system (i.e. CM-ground-ASE has initiated an abort), the CM-air-user then has the option of attempting a non-secure package 1 CM-logon service. Note that there is not a specific reason for this case (since it will be viewed as a protocol error), so the actual abort reason may not be immediately apparent to the CM-air-user.

If the secure logon has been accepted by the peer ground system (i.e. the Security Requirements parameter is set to the same value as was originally set by the CM-air-ASE), a CM-logon confirmation is given to the CM-air-user containing the ground security and application information (the Security Requirements parameter is not confirmed to the CM-air-user). The CM-air-user then distributes the information received in the user data, including the security information, to the other applications on the aircraft as well as to the dialogue service (for use by the security ASO). Each application can then perform its own secured services with this information.

4. CM Secure Contact

Since the CM-contact service only takes place after a successful logon, there is an inherent level of security already in place between the package 2 aircraft and package 2 ground system. Therefore, no additional security data needs to be carried in the secure CM-contact service user data. However, if there is not already a dialogue maintained from the CM-logon service, then the dialogue service Security Requirements parameter must be set to "Secured application dialogue". This will be set by the CM-ground-ASE.

Upon receipt of the CM-contact request, the air security ASO will check to see that everything is in order. If not, an abort will be invoked. Otherwise, the aircraft will attempt a package 2 logon with the indicated facility. The result is then indicated back to the originating CM-ground-user. Note that the CM-ground-user originating the CM-contact service does not need to know whether or not a successful secure logon was accomplished, only whether or not a successful logon was accomplished. So there are no changes required to the CMContactResponse PDU. Therefore, the CM-air-ASE will only need to set the Security Requirements parameter to "Secured application dialogue".

Upon receipt of the D-START response or D-DATA request containing the CM-contact response parameters, the ground security ASO will check that all is in order. If there are any problems, an abort will be issued. Otherwise, the CM-ground-ASE will receive the

dialogue service confirmation or indication primitive and pass the information to the CM-ground-user via the CM-contact confirmation.

5. Changes to the CM SARPs

The security additions will require changes to the CM SARPs. However, these changes can be made so that CM backwards compatibility can be preserved. The high level changes that need to made are as follows:

2.1.1 - Add new explanatory notes explaining the secure services.

2.1.2 - No change required.

2.1.3 - New secure CM-logon service additions to the existing CM-logon service (includes new CM-logon parameters for Security Requirements and new CM-logon response parameter) and the CM-contact service (Security Requirements parameter added). Also, other package 2 services need to be revisited to add the security data.

2.1.4 - New PDUs will need to be added for the secure CMLogonResponse. In addition, all requisite ASN.1 for that service will need definition.

2.1.5 - New requirements dealing specifically with the Security Requirements parameter of the dialogue service will need to be added. Also, the corresponding PDU to user data mapping will need to be specified.

2.1.6 - No change, unless the Security Requirements parameter is to be defined in this section.

2.1.7 - New user requirements for both invoking and receiving new security service primitives. This will include the distribution of the security information to the other applications as well as the obtaining of necessary information from the Directory.

2.1.8 - Need to add that for package 2, security is one of the base functions and is not an option.

6. Conclusion

This paper gives a high level functional overview of how CM will operate within the security guidelines put forth by the security subgroup, and also gives an idea of the scope of the changes required. These changes will not affect the backwards compatibility aspects of CM.

The meeting is invited to note and comment on the CM security approach.