The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

THE APPLICATION OF CCSDS PROTOCOLS TO SECURE SYSTEMS

Informational Report

CCSDS 350.0-G-2

Green Book

January 2006

AUTHORITY

Issue:	Green Book, Issue 2
Date:	January 2006
Location:	Washington, DC, USA

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and reflects the consensus of technical panel experts from CCSDS Member Agencies. The procedure for review and authorization of CCSDS Reports is detailed in the *Procedures Manual for the Consultative Committee for Space Data Systems*.

This document is published and maintained by:

CCSDS Secretariat
Office of Space Communication (Code M-3)
National Aeronautics and Space Administration
Washington, DC 20546, USA

FOREWORD

This document is a CCSDS Report that contains background and explanatory material to supplement the CCSDS Recommended Standards for conventional telecommand and telemetry, Advanced Orbiting Systems (AOS), Space Communications Protocol Specification (SCPS), and Proximity links.

Through the process of normal evolution, it is expected that expansion, deletion or modification to this Report may occur. This Report is therefore subject to CCSDS document management and change control procedures. Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions about the contents or status of this Report should be addressed to the CCSDS Secretariat.

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- British National Space Centre (BNSC)/United Kingdom.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (Roskosmos)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- Centro Tecnico Aeroespacial (CTA)/Brazil.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish Space Research Institute (DSRI)/Denmark.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Korea Aerospace Research Institute (KARI)/Korea.
- MIKOMTEK: CSIR (CSIR)/Republic of South Africa.
- Ministry of Communications (MOC)/Israel.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic & Atmospheric Administration (NOAA)/USA.
- National Space Program Office (NSPO)/Taipei.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title and Issue	Date	Status
CCSDS 350.0-G-1	The Application of CCSDS Protocols to Secure Systems, Issue 1	March 1999	Original issue, superseded
CCSDS 350.0-G-2	The Application of CCSDS Protocols to Secure Systems, Informational Report, Issue 2	January 2006	Current issue

CONTENTS

CONTENTS (continued)

Section Page

Figure

Table

1 INTRODUCTION

1.1 PURPOSE

This Report is intended to provide guidance to missions that wish to use the CCSDS Recommended Standards for spacecraft control and data handling but also require a level of security or data protection. The report provides background information on security, details various options for security implementation in space missions, and outlines the impact of security on defined CCSDS services.

1.2 SCOPE

THE INFORMATION CONTAINED IN THIS REPORT IS NOT PART OF ANY OF THE CCSDS RECOMMENDED STANDARDS. In the event of any conflict between any CCSDS Recommended Standard and the material presented herein, the CCSDS Recommended Standard shall prevail.

This report is intended as an implementation guide to aid space missions requiring secure CCSDS space mission data systems. It primarily addresses security of the space-ground ground-space data link. Ground systems are addressed by the use of off-the-shelf security solutions such as IPSec. Detailed information on security analysis and risk assessment methodology are beyond the scope of this report; however, references [9] and [10] provide further information.

1.3 RATIONALE

To date, most civil space missions have relied on their uniqueness to deter unauthorised access to the space mission data system, whereas military missions have implemented mission specific security measures to protect the spacecraft command and telemetry data. This situation is changing with the advent of more open systems for space mission control and data distribution, increased Internet connectivity, and cross support activities. Civil space mission and ground system developers must now consider security as part of the system design process.

It is likely that most future space missions will require a level of mission-data-system security to protect the spacecraft and ground systems from unauthorised access. This likelihood is particularly evident as space mission control activities gradually make more use of public networks, such as the Internet, for ground network connectivity. Some missions will require increasingly higher levels of security for a variety of operational and commercial reasons.

The work performed by CCSDS has provided a sound basis for the spacecraft control and mission data systems for all types of space missions. The CCSDS Recommended Standards for conventional telecommand (references [1], [2], and [3]) and telemetry (reference [4]), and Advanced Orbiting Systems (AOS—reference [5]) have been developed by civil space

agencies and are primarily intended to satisfy the communications requirements of civil missions. However, the CCSDS initiative has generated significant interest within the other space communities, such as government/military and commercial, for a number of reasons, including:

a) increased complexity of spacecraft and payloads for all mission types requiring more advanced control and monitor systems, including packet-based mechanisms and on-board autonomy;

b) reduction in space mission budgets with encouragement to utilise commercial technologies and standards where appropriate;

c) availability of space- and ground-segment commercial products to reduce mission development costs;

d) initiatives to consolidate civil and military ground station networks requiring widespread data systems standardisation;

e) increased reliance on national and international co-operation to achieve space mission objectives.

Promoting the use of CCSDS Recommended Standards for a wider range of missions, including commercial and military, will make possible further reductions in mission development costs for all mission types through the wider availability of commercial products. In the same way, establishing generic security concepts to satisfy the security requirements of future commercial and military missions will further extend the CCSDS user environment. Establishing generic security concepts is one of the objectives of this implementation guide.

1.4 ORGANIZATION OF THIS REPORT

This document is organised as follows:

Section 2 provides an introduction to security, defines terms that are used in this report, and identifies generic space mission security threats.

Section 3 presents a space mission security architecture based on a CCSDS reference model and establishes the security requirements of different types of space missions.

Section 4 describes the specific security mechanisms that may be utilised to achieve required security services.

Section 5 highlights the various available options for security for missions using CCSDS Recommended Standards and describes the impact on protocol data structures.

Section 6 presents the implications of security on the space mission architecture and cross-support services. A comparison of possible security options, with guidance on option selection, is also provided.

Annex A describes some known implementation examples of CCSDS missions that have incorporated additional security features.

1.5 REFERENCES

The following documents are referenced in the text of this Report. At the time of publication, the editions indicated were valid. All documents are subject to revision, and users of this Report are encouraged to investigate the possibility of applying the most recent editions of the documents indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS documents.

[1] *TC Synchronization and Channel Coding*. Recommendation for Space Data System Standards, CCSDS 231.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, September 2003.

[2] *TC Space Data Link Protocol*. Recommendation for Space Data System Standards, CCSDS 232.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, September 2003.

[3] *Communications Operation Procedure-1*. Recommendation for Space Data System Standards, CCSDS 232.1-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, September 2003.

[4] *TM Space Data Link Protocol*. Recommendation for Space Data System Standards, CCSDS 132.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, September 2003.

[5] *AOS Space Data Link Protocol*. Recommendation for Space Data System Standards, CCSDS 732.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, September 2003.

[6] *Telecommand Summary of Concept and Rationale*. Report Concerning Space Data System Standards, CCSDS 200.0-G-6. Green Book. Issue 6. Washington, D.C.: CCSDS, January 1987.

[7] *Advanced Orbiting Systems, Networks and Data Links: Summary of Concept, Rationale and Performance*. Report Concerning Space Data Systems Standards, CCSDS 700.0-G-3. Green Book. Issue 3. Washington, D.C.: CCSDS, November 1992.

[8] *Space Communications Protocol Specification (SCPS)—Security Protocol (SCPS-SP)*. Recommendation for Space Data System Standards, CCSDS 713.5-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, May 1999.

[9] *OSI Reference Model—Security Architecture*. International Standard, ISO 7498-2-1988(E). Geneva: ISO, 1988.

[10] K. M. Jackson and J. Hruska, eds. *Computer Security Reference Book*. Oxford: Butterwoth-Heinemann, 1992.

[11] *Space Packet Protocol*. Recommendation for Space Data System Standards, CCSDS 133.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, September 2003.

[12] *Cross Support Reference Model—Part 1: Space Link Extension Services*. Recommendation for Space Data System Standards, CCSDS 910.4-B-2. Blue Book. Issue 2. Washington, D.C.: CCSDS, October 2005.

[13] *Cross Support Concept—Part 1: Space Link Extension Services*. Report Concerning Space Data Systems Standards, CCSDS 910.3-G-2. Green Book. Issue 2. Washington, D.C.: CCSDS, April 2002.

[14] *Packet Telecommand Standard*. ESA PSS-04-107, Issue 2. Paris: ESA, 1992.

[15] S. Kent and R. Atkinson. *Security Architecture for the Internet Protocol*. RFC 2401. Reston, VA: ISOC, November 1998.

[16] *Data Encryption Standard*. FIPS 46-3. Gaithersburg, Maryland, USA: NIST, October 1999. <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>

[17] *Advanced Encryption Standard*. FIPS 197. Gaithersburg, Maryland, USA: NIST, November, 2001. <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

[18] *Proximity-1 Space Link Protocol*. Recommendation for Space Data System Standards. CCSDS 211.0-B-3. Blue Book. Issue 3. Washington, D.C.: CCSDS, May 2004.

2 SECURITY CONCEPTS AND DEFINITIONS

2.1 DEFINITIONS

The following security service definitions are used within this report. Examples of the application of the security service in a space mission environment are provided as part of each definition.

2.1.1 ACCESS CONTROL

Access control is the process of granting access to the resources of a system only to authorized users, programs, processes, or other systems. Access control inhibits unauthorised use of a resource. Access controls may be applied to various types and levels of access to a resource (e.g., the actual use of a resource, the deletion of information, or the ability to read information).

An example of access control within a space mission environment is the use of the mechanisms and procedures to enable only approved operators to access the mission control system after being authenticated.

2.1.2 AUTHENTICATION

Authentication provides the ability to verify the identity of a user, device, or other entity in a system, often as a prerequisite to allowing access to resources in a system.

Authentication provides the assurance that information transmitted from a claimed source (i.e., a source entity's identity) actually came from that source. This service is also known as *data origin authentication*. It may also provide protection against duplication or modification of data.

In a space mission environment, authentication may be used to achieve assurance that the received data originated from an authorised space mission control centre. Thus, authentication can provide spacecraft protection by requiring that the on-board data handling system accept only validated telecommands. Any telecommands that do not pass the authentication process are rejected.

2.1.3 AVAILABILITY

Availability is the assurance that a system will be usable when it has to be. Availability is not entirely a security concern. It is a security concern from the perspective of an outside attacker attempting to deny access to a system by attacks such as denial-of-service or crashing the system. However, there are other aspects of availability that manifest themselves in terms of hot backups, high assurance computing paradigms, fail-safe computing, fail-over computing, etc.

2.1.4 CONFIDENTIALITY

Confidentiality ensures that information is not available or disclosed to unauthorised personnel, entities, or processes. It ensures that data is disclosed only to those who are authorised to see it.

In a space mission environment, data confidentiality may be used to prevent the disclosure of sensitive information contained within any part of the space mission data system. Confidentiality is particularly relevant for sensitive data transmitted over the ground-to-space (or space-to-ground) Radio Frequency (RF) link or via public (non-operational) networks within the ground segment.

Confidentiality may also be relevant for space mission protocol headers and trailers, to prevent analysis of the communications traffic within the spacecraft control system. Traffic analysis could disclose information on the operational status of the system, and such disclosure may be undesirable for certain types of missions.

2.1.5 DATA INTEGRITY

Data integrity provides assurance that data transmitted from a source is unchanged by detecting if it has not been accidentally or maliciously modified, altered, or destroyed.

In a space mission environment, an integrity service may be used to ensure that mission data has not been manipulated in any way during transmission across ground networks or over the RF link.

2.1.6 ACCOUNTABILITY

Accountability ensures that all system actions are logged along with the identity of the entity initiating the action, and the date and time the action occurred. This is also known as auditing.

In a space mission environment, an accountability service can be used to record all system actions in a log for later use in forensics analysis.

2.2 OVERVIEW

2.2.1 DEFINITION OF SECURITY

Security can be described as the effect or process of minimising the vulnerabilities of assets or resources. The key elements of information security for a data communications system are access control, authentication, availability, confidentiality, integrity, and accountability. Access Control results in the limiting of access to the system to specified individual or groups (or processes acting on their behalf). Authentication is the assurance that the claimed identity of the source of information is not forged. *Availability* is the assurance that a system

will be available for use. *Confidentiality* is protection against unauthorised disclosure of information, and *integrity* is protection against unauthorised modification of data.

To incorporate security in a space mission data system, the following entities may require protection:

a) information and data contained within the system (i.e., *information*);

b) communications and data processing (i.e., *services*);

c) space mission ground equipment and spacecraft (i.e., *resources*).

Security can be achieved by the implementation of a number of different 'security services' at specific locations in the space mission data system. To incorporate the appropriate level of security for a particular mission, at least one security service or a combination of security services is required.

2.2.2 THE SYSTEM SECURITY POLICY

In selecting the appropriate security services for a particular mission, the first task is to assess the security threats to the system. This task is normally part of the development of a System Security Policy (SSP). The SSP is usually a formal document providing a description of the system, the top-level security objectives, and identification of the specific information-security and system-availability threats against the system. Other information may be included in the SSP such as the security standards and evaluation requirements to be applied to the system, rules for access and operation of security critical systems (e.g., certificate authority), and if encryption is used, the means by which keys are distributed and managed.

As part of the SSP development process, a *threat assessment* should be performed. The threat assessment should assess the vulnerabilities of the system and then establish the likelihood, consequences, and cost of realisation of each threat to the system. A threat is a problem only if a system is found to be vulnerable. Once the threat assessment process is complete, specific security services can be identified to counter each threat/vulnerability. The selection of countermeasures is likely to require a cost-benefit analysis to justify the implementation cost of security services within the system. Any remaining vulnerabilities are deemed "residual risk" and must be acceptable by system management before putting the system into production. Detailed information on threat assessment is beyond the scope of this report. There are many information sources on this subject, including reference [10].

2.3 THREATS

2.3.1 TYPES OF THREAT

A threat is defined as any circumstance or event having the potential to cause harm to a system through destruction, disclosure, and modification of data, and/or through denial of

service. A threat can also be defined as a *potential* violation of security. However, a threat remains only a *potential* violation of security until it can be shown that there is a high likelihood that the threat can cause harm. At that time, the threat is re-categorised as a vulnerability.

Threats can be classified as accidental or intentional and may be active or passive. The threats to a space mission data system include:

a) unauthorised destruction of information and/or resources (e.g., spacecraft or ground systems);

b) unauthorised corruption or modification of information within the system;

c) theft or loss of information and/or resources;

d) disclosure of information to unauthorised entities;

e) interruption of services.

Accidental threats have no premeditated intent and include system malfunctions and operational errors. Intentional threats range from casual examination of system information to sophisticated attacks using specific knowledge about the system.

Passive threats, if realised, would not result in modification to any information in the space data system and the system itself would remain unaffected. Security violations falling into this category are generally associated with loss of data confidentiality, since this is the only security property that can be compromised without trace.

Realisation of active threats would involve modification of information contained within the system or malicious changes to the operation or state of the system (space and/or ground segment). Active threats can compromise the information passing across a space mission data communication system by violating the integrity of the data or by degrading the availability of the system.

2.3.2 THREATS TO SPACE SYSTEMS

The threats to a space mission data system can be categorised into three areas:

a) threats to radio frequency (RF) transmissions;

b) threats to the space system resources (e.g., spacecraft and onboard instruments);

c) threats to the ground element of the mission data system.

Threats to spacecraft telecommands and telemetry links originate from the fact that they are transmitted through the physical RF medium. These transmissions are potentially subject to detection and interception by entities unauthorised to receive the information. As a result, there is a possibility that the information contained within the transmissions could be exploited.

A particularly dangerous active threat might allow an unauthorised entity to transmit to a spacecraft telecommands that might cause accidental or malicious damage, cause theft of the spacecraft, or ultimately destroy the spacecraft. With the large investment needed to deploy space missions, any processes that may counter the threats to the spacecraft are desirable and will be essential for some types of space mission.

A similarly dangerous active threat would be the jamming of the RF medium by an unauthorised entity to entirely block transmission to or from the space link. In this way, access is denied which could result in loss of science data, telemetry, or telecommand—possibly causing un-repairable damage to a spacecraft.

Threats to the space mission ground data system can be considered the same as the information security threats to any open or private computer network. Specific types of information security attacks are described in reference [9], and a brief overview is provided in the following sections.

2.3.3 PASSIVE ATTACKS

A passive attack is typically accomplished by eavesdropping (e.g., listening in on an RF transmission, wiretapping, packet sniffing). A space system can be subjected to two principle types of passive attack:

a) *Compromise of data confidentiality* - unauthorised disclosure of information flowing between ground and space systems or across the ground mission data network.

b) *Compromise of traffic flow confidentiality (traffic analysis)* - unauthorised disclosure of aspects such as the volume, source, and destination of the information in the system, without explicitly disclosing the content of the data.

2.3.4 ACTIVE ATTACKS

Some of the possible types of active attacks to be considered for space systems are described below.

a) *Modification of messages* occurs when some or all of the content of a data transmission is altered or destroyed without detection, resulting in an undesirable or malicious effect on the system.

b) *Masquerade* occurs when an unauthorised entity pretends to be an authorised entity. It is usually used with some other form of active attack, such as replay or data modification. For example, if an attacker can divert network connections to another computing host, which is masquerading as the genuine host, system passwords or other useful information may be captured. A related attack is known as *connection hijacking*. Connection hijacking occurs when an entity is able to observe network traffic and is able to take over a connection by blocking the true source of data and injects traffic as if it came from the true source. *Social engineering* is another related

attack that occurs when an outsider is able to obtain confidential system information (e.g., system architecture details, user names, passwords) by masquerading as a member of the support staff to elicit information from authorized system users under the pretence of needing to repair system problems.

c) A *replay attack* is carried out when a message or part of a message is recorded and is repeated at a later time to produce an undesirable effect. For example, a previously sent, authorised telecommand may be retransmitted to a spacecraft at a later time resulting in an undesirable affect on the spacecraft payload.

d) A *denial of service attack* occurs when the system, or parts of the system, is prevented from performing their proper functions. This type of attack includes jamming the communications links and overloading of space and/or ground system resources.

e) *Insider attacks* occur when authorised users of the system behave in an illicit manner.

f) *Software threats* include *viruses*, which can infect and disrupt computers within the space mission network, *worms* which infect a system and then seek ways to propagate on their own to other systems, *trapdoors*, which are intentionally created loopholes within the system software to allow access to the system bypassing usual security controls, *Trojan Horses*, which are software processes that have unauthorised functions, some of which may be damaging, in addition to their authorised functions, and *spyware* which may cause systems to slow down or cause unauthorized leakage of information.

3 CCSDS SECURITY REQUIREMENTS

3.1 SPACE DATA SYSTEM REFERENCE MODEL

To provide the overall security architecture for space mission data systems, a space link reference model is used as shown in figure 3-1. The model highlights the various CCSDS protocols that are available and four security implementation points that have been selected for a variety of reasons explained in this report. The four security implementation points considered are:

– Physical layer;

– Data link layer (conventional and AOS);

– Network (or packet) layer;

– Application layer.

Security may be applied at other layers (e.g., the transport layer) if required by the mission requirements. However, this report considers only the four security implementation points, shown in figure 3-1, that are likely to satisfy the requirements of most missions. Figure 3-1 does not show all possible CCSDS protocol combinations.

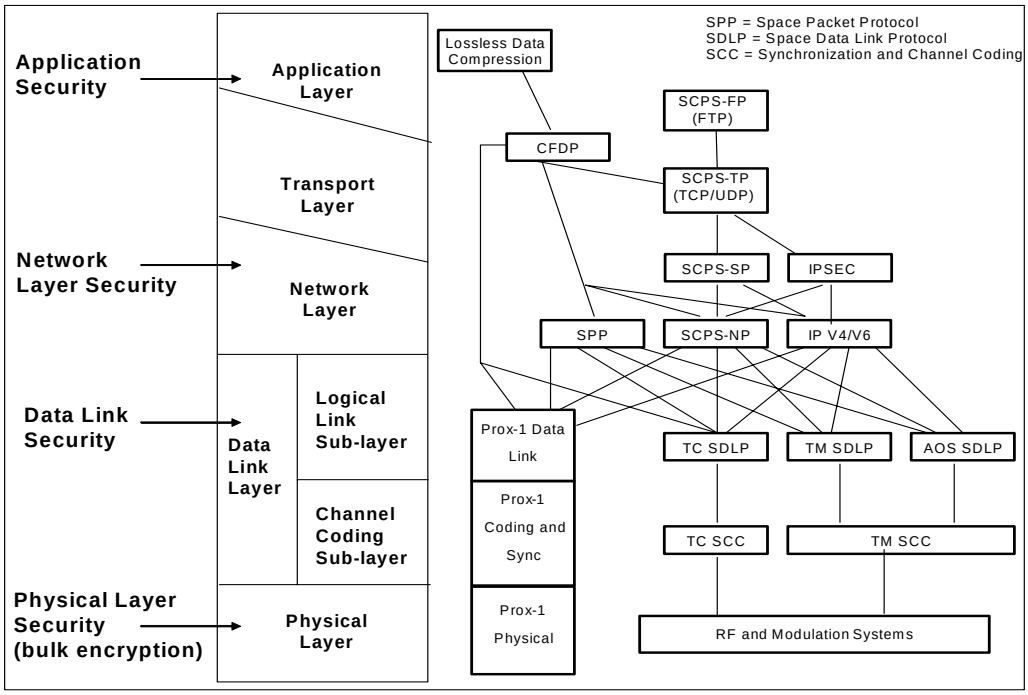

Figure 3-1: CCSDS Space Mission Protocols and Security Options

The security implementation approach selected for any particular space mission is dependent on the following factors:

a) the mission Agency's security policy;

b) the mission security requirements;

c) the mission operational requirements (to include cross support and interoperability);

d) the CCSDS Recommended Standard in use (e.g., conventional telecommand and telemetry, AOS, SCPS, Proximity-1);

e) the capability of the on-board systems.

Different security services may be applied at different layers of the spacecraft communications system as indicated in figure 3-1, although not all layers may be implemented within the data system of any particular mission.

3.2 CLASSES OF MISSIONS

To define sets of generic security requirements for different space mission types, missions have been classified as requiring either *high*, *moderate*, or *minimal* levels of security. This grouping is intended only to act as a guide for the purposes of this report and is not restrictive. Some missions may have security requirements that cannot be contained within one of these groups.

Different mission types will require the implementation of different security services to satisfy specific mission requirements. In addition, different mission types may require different *assurance of correctness of operation* for each security service. For example, high security missions will require many security services and the highest assurance that these services are operating as intended (e.g., use of high grade, government approved cryptographic algorithms). Moderate security missions may require the same security services as high security missions, but with lower levels of assurance. Minimal security missions will require the fewest security services and the lowest level of assurance.

3.2.1 HIGH SECURITY

Missions requiring high security are generally associated with the government or military sector. They may be life-critical manned missions which would require high security in order to ensure life. Commercial telecommunications missions may also fall into this class due to the mission's high cost and the operational nature of the system once on orbit. Secure access to the spacecraft control system is required at all times during the mission and under all possible operational or environmental conditions. The mission data system must be protected from unauthorised access and measures must be implemented to prevent detection, interception, and exploitation of the data links.

The following security requirements are <u>likely</u> for high security missions:

a) protection of all telecommand data:

   – confidentiality,

  - authentication,
  - access controls,
  - data integrity (including anti-replay measures),
  - availability;

b) protection of all telemetry data:
  - confidentiality,
  - data integrity,
  - possibly other security services such as authentication and access controls,
  - availability;

c) protection of all data in the ground data system:
  - confidentiality,
  - authentication,
  - data integrity,
  - availability,
  - access controls.

3.2.2 MODERATE SECURITY

Missions requiring moderate security may include commercial communications, meteorological, and remote sensing missions. Satellite navigation systems may also be included in this class (but may just as well fall into the high security class depending on the nature of the system).

These missions will require spacecraft and ground system protection from unauthorised access and may need to protect payload data that is commercially or operationally sensitive, or safety-critical. Protection from unauthorised access is especially important if the mission utilises open ground networks such as the Internet to provide ground station connectivity.

At a minimum, moderate security missions are likely to have the following security requirements:

a) protection of telecommand data:
  - authentication,
  - data integrity,
  - possible requirement for confidentiality;

b) protection of some or all telemetry data:
   - confidentiality,
   - data integrity;

c) protection of some or all data in the ground data system:
   - authentication,
   - data integrity,
   - possible requirement for access control,
   - possible requirement for confidentiality.

3.2.3 MINIMAL SECURITY

Missions requiring minimal security include all other space missions. These missions are likely to require security of the telecommand system to prevent unauthorised access or tampering with the data, either intentionally or unintentionally. There may also be confidentiality requirements for specific telemetry information (e.g., medical data within manned missions).

Minimal security missions are likely to have the following security requirements:

a) protection of all telecommand data:
   - authentication,
   - data integrity,
   - possible requirements for confidentiality;

b) protection of some telemetry data: confidentiality, data integrity;

c) protection of some data in the ground data system: confidentiality, data integrity, access control.

4 SECURITY MECHANISMS

4.1 CONFIDENTIALITY

The security mechanism that provides a confidentiality service for communications is *encryption*. Encryption may also contribute to the achievement of other security services such as data integrity and authentication. Encryption, when used for confidentiality, transforms sensitive data to a less sensitive form. When used for integrity or authentication, cryptographic techniques are used to generate unforgeable functions such as a digital signature as described in 4.2.

Encryption is performed on *plaintext* to produce *ciphertext*. The reverse process is known as decryption. A key is used during both encryption and decryption to direct specific transformations as part of the cryptographic process as shown in figure 4-1. When a key is changed, different ciphertext is obtained for the same plaintext input. The security of the encryption process is dependant on the strength of the cryptographic algorithm being used, the length of the cryptographic keys, and maintaining the secrecy of the keys. Sometimes, details of the cryptographic algorithm being used are publicly known as is the case with the Data Encryption Standard (DES) [16] algorithm, originally published in 1977, or the recently adopted Advanced Encryption Standard (AES) [17]. In this case, because the details of the algorithms are known, security of the system is designed to be dependent on the secure handling of the cryptographic keys—their management, distribution, use, and destruction.

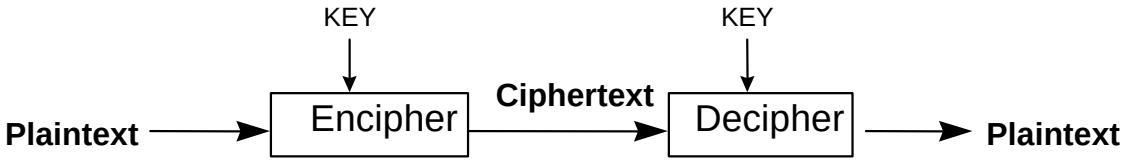

Figure 4-1: The Concept of Encryption and Decryption

Encryption may be carried out on a *point-to-point*, *hop-by-hop*, or *end-to-end* basis. In the case of a point-to-point system, encryption is provided only between the two communicating end-points (see figure 4-2). In the case of a hop-by-hop system (see figure 4-2), the data is encrypted for transmission and then decrypted by an intermediary before being re-encrypted for further transmission on towards its final destination. In an end-to-end system (see figure 4-2), encryption is applied at the source and decryption is only applied at the final destination. The data may pass through intermediary systems; however they do not decrypt nor examine the data.

Encryption algorithms may be *symmetric* or *asymmetric* (which also known as public-key). In a symmetric system both the encryption and decryption keys are the same and are kept secret. Thus, a secure key distribution system must be implemented to generate, distribute, and account for all the keys that are required in the system. DES and AES are examples of symmetric cryptographic algorithms.

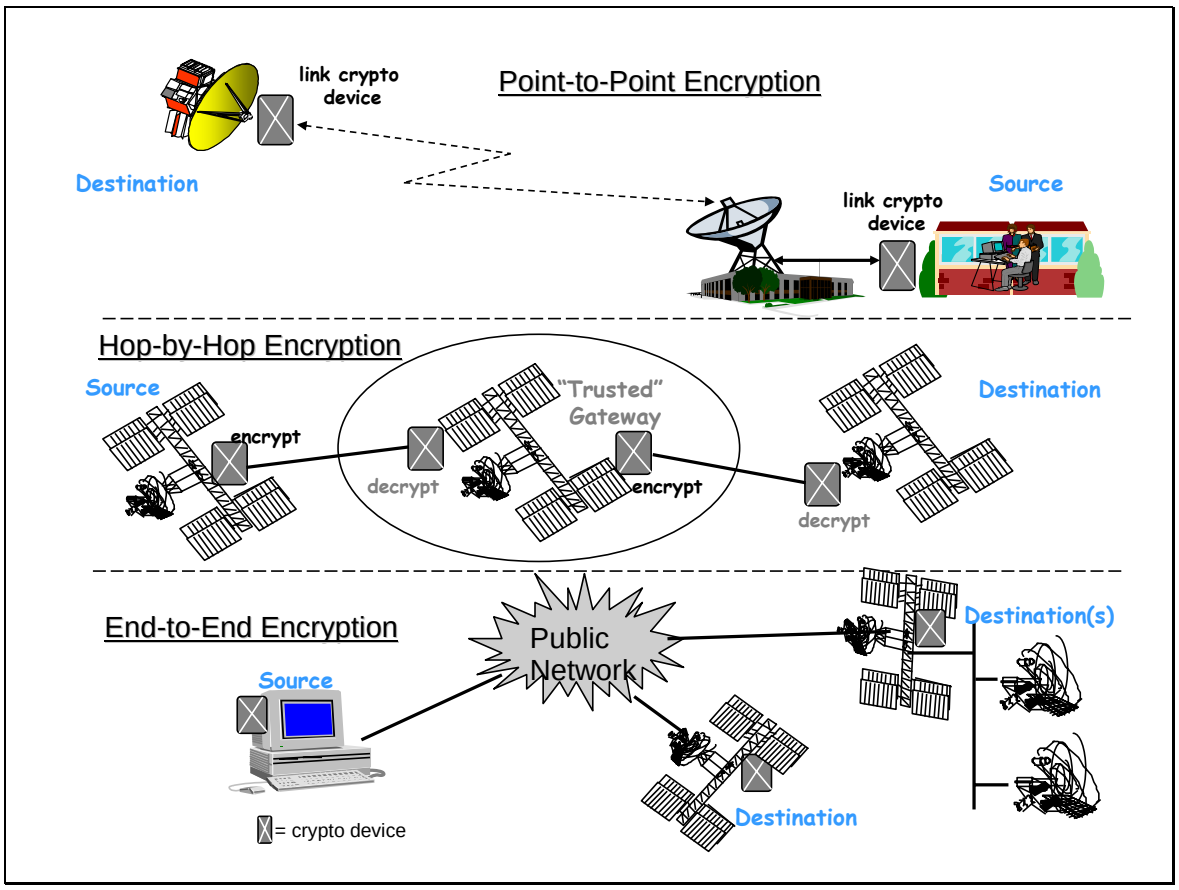

Figure 4-2: Illustration of Point-to-Point, Hop-by-Hop, and End-to-End Encryption

In an asymmetric (or public-key) system, each communicating end-system has a key-pair—a public key and a private key. The private key is kept secret, but the public key is made available to anyone who wants it. An asymmetric system relies on the fact that it is practically impossible to obtain knowledge of the decryption key from knowledge of the encryption (public) key. For example, the Rivest-Shamir-Adleman (RSA) public key system, the best known and most commercialized public key system in use, is based on the difficulty of finding factors of large prime numbers. The public key does not need to remain secure, which implies that no prior secret key exchange is required, and which in-turn leads to reduced security development and operations costs. However, in practice RSA uses a combination of public and symmetric key systems (hybrid encryption) to improve efficiency. A public key exchange is used between the communicating assets in order to arrive at a shared key (the traffic or session encryption key) which is then used with a symmetric algorithm to provide data confidentiality.

However, since public keys are openly shared, there must be a secure, high assurance *binding* between the owner of the public key and the key itself to ensure that a false or substituted public key is not used. The binding occurs by digitally signing the public key by a trusted third party (e.g., a certificate authority) whose identity is well-known and who vouches for the true identity of the public key owner.

Before they are used, cryptographic systems must be subjected to analysis in order to discover if there are any weaknesses that could be exploited by a potential attacker. During this analysis, the following worst case assumptions are usually made:

a) an attacker has complete knowledge of the algorithm;

b) an attacker has obtained a considerable amount of ciphertext;

c) an attacker knows the plaintext equivalent of a certain amount of ciphertext.

As a result, symmetric keys must be distributed and maintained securely, as it is the primary means by which information is protected.

There are different types of symmetric cryptographic algorithms that operate in different cryptographic modes. For example, a symmetric *stream cipher* encrypts one bit of plaintext at a time (e.g., RC-4), whereas a *block cipher* encrypts data in blocks which can be more convenient for octet-oriented systems. For example, the (old, weak, and no longer recommended for use) DES algorithm is a block cipher that has a 64-bit input and produces a 64-bit output under the control of a 56-bit key (56 bits + 8 parity bits). The Advanced Encryption Standard (AES), a modern block cipher algorithm, uses a larger block size (128-bits) and uses larger keys such as 128, 192 or 256 bits. Detailed information on cryptographic algorithms can be found elsewhere (see reference [10]).

4.2 AUTHENTICATION

Data authentication is usually achieved by appending an extra unit of information to the original message. This extra unit of information is called the *digital signature* as shown in figure 4-3. The digital signature definitively identifies the origin of the data, and the receiver of the data is thus assured that the data is from the claimed source. The essential characteristic of the digital signature mechanism is that the signed data unit cannot be created by an unauthorised entity.

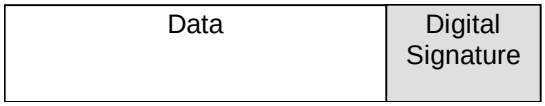

Figure 4-3: Digital Signature Concept

Many digital signature generation mechanisms require the use of an asymmetric cryptographic algorithm where sender and receiver do not hold the same cryptographic keys (as described in 4.1). Rather, a pair of public and private keys that are mathematically related to one another are used. At the origin of the data, the cryptographic algorithm generates a digital signature using the sender's private key. The signature may be generated from the data itself and is of a specific length depending on the algorithm used. Data origin authentication is achieved when the digital signature is successfully verified by the receiver using the sender's public key.

Encryption of the data itself can also provide implicit authentication when using a symmetric cryptographic algorithm. Authentication is achieved because the recipient must have and use the correct key to decipher the digital signature appended to the data. This assumes there is an assured key distribution mechanism. Also, encryption provides implicit authentication when using an asymmetric (public key) system if there is assurance that the public key is bound to the originator (e.g., signed by a certificate authority). However, caution must be used because authentication may be compromised if the encrypted data is captured and later replayed without replay protection.

4.3 DATA INTEGRITY

Data integrity can be considered as having two different functions: the integrity of the individual data units, and the integrity of a stream of data units. Different mechanisms are generally used to provide these different integrity functions.

Integrity of individual data units is achieved by appending an *Integrity Check Value (ICV)* to the data structure in a manner similar to the way a digital signature is appended. However, the ICV is always a function of the data itself. A Cyclic Redundancy Check (CRC) is a simple example of such a function. Stronger functions include Message Digest 5 (MD5) and the Secure Hash Algorithms (SHA-1, SHA-2). The receiver generates a corresponding check value by performing an operation (which may be cryptographic) on the data and compares the result to a received value to determine if the data has been modified in transit. In some applications, both authentication and individual data unit integrity can be provided by one mechanism. To a certain extent, CCSDS coding such as Reed-Solomon and Turbo Codes provide data integrity by virtue of their error detection and correction capabilities.

To provide integrity of a stream of data units, a form of sequence numbering is usually implemented which protects against replay attack. Alternatively, time-stamping of data may be used to provide limited replay protection.

To ensure that the integrity check value (ICV) is not modified or corrupted, often the ICV is keyed (e.g., a keyed hash) or the ICV value can be encrypted using a symmetric encryption algorithm (e.g., DES MAC).

4.4 ACCESS CONTROL

The basic function of access control is to ensure the availability of data or information technology resources only for authorised users or processes. As a result of ensuring data availability, access control mechanisms may provide limited confidentiality and integrity. It should be noted, however, that access control is not a fundamental technique for providing these other two security services; it is purely a barrier in the path of a potential intruder.

Access control requires the use of a number of techniques, including the establishment of access control information bases where the access rights of users or processes are maintained securely. Authentication information such as identification and passwords provide management and

control of access to the system. Passwords should be administered effectively by establishing details such as appropriate password length and content, implementing procedures for regularly changing passwords, and ensuring that password secrecy is maintained. It should be noted that automation of password generation increases security significantly. Also, plaintext passwords should **never be transmitted over an unprotected medium**. If passwords must be sent over a network an encryption function (e.g. SSH, SSL, IPSec or other Virtual Private Network (VPN)) should be used. Audit trails are an important mechanism in security management. They are used to monitor system usage and password changes and should contain as much information regarding the system details and previous accesses as possible.

4.5 AVAILABILITY

Availability is the assurance that a system will be usable when it has to be. Although not entirely a security concern, it is a security concern from the perspective of an outside attacker attempting to deny access to a system. This can be done by attacks such as denial-of-service or crashing systems.

In a space environment, there are also space links which are manifested as radio frequency (RF) communications. Unlike wire line communications, RF communications can be jammed by devices emitting higher power levels on the same (or near-by) frequency. When a frequency is jammed, communication over that RF link is interrupted. This impedes telemetry and telecommand to/from a spacecraft. This also impedes the collection of data from a spacecraft potentially resulting in total, unrecoverable data loss. It can also result in the loss of the spacecraft if housekeeping data is not received on the ground and there is an emergency situation that must be dealt with immediately. Likewise a spacecraft can be lost if telemetry is received but the telecommand uplink is jammed and no commands can be received. Spread spectrum and frequency hopping, to be discussed in Section 5.2, are techniques used to counter jamming.

5 CCSDS SECURITY IMPLEMENTATION OPTIONS

5.1 OVERVIEW

This implementation guide considers the incorporation of security within four specific layers of the space mission data system: the application, network, link, and physical layers, as shown in figure 5-1. The various security options considered are described in this section, and the implications on the defined services of each layer are presented in section 6.

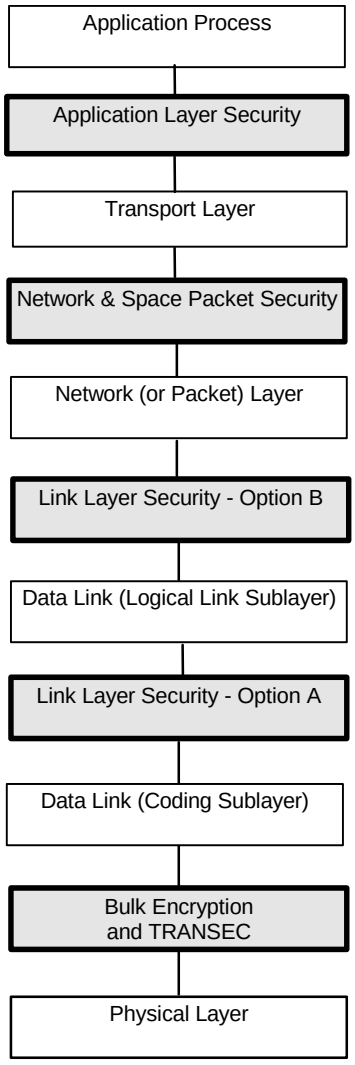

Figure 5-1: Security Implementation Options Considered in This Report

5.2 BULK ENCRYPTION

Bulk encryption provides *confidentiality* to all of the communication system data structure. It is implemented at the physical layer and provides the highest possible level of data confidentiality available on a point-to-point basis—often this is termed "link encryption." However, this is not to imply encryption at the link layer but rather over the physical link. No separate integrity, authentication or access control services are implied other than those implicitly provided by encryption. For example, if symmetric key encryption is used, authentication is implicitly achieved, because the receiving end must have the correct key, which has been distributed by an assured key distribution system, in order to decipher the data.

If applied to missions using the CCSDS Recommended Standards, bulk encryption would result in encryption of the full physical layer data structure. For telecommand (see reference [1]), use of bulk encryption implies that the Command Link Transmission Unit (CLTU) as well as the acquisition and idle sequences would be encrypted. For telemetry (see reference [4]), the Channel Access Service Data Unit (CA_SDU) would be encrypted. A similar result would be obtained if bulk encryption were applied to AOS (see reference [5]), where the full Physical Channel Access Protocol Data Unit (PCA_PDU) would be encrypted.

Similarly, to prevent jamming of the physical layer, techniques such as *spread spectrum* using *direct sequence* and *frequency hopping* can be employed. This technology is known as transmission security (TRANSEC). When data is transmitted using spread spectrum techniques, the information is transmitted over a wide range of frequencies and then are collected by a receiver onto a single frequency. In direct sequence spread spectrum, the stream of information to be transmitted is divided into small pieces, each of which is allocated across to a frequency channel across the spectrum. This technique spreads the signal so that it appears to be noise rather than data and therefore is hard to intercept and jam.

Using frequency hopping techniques, data is transmitted over a single frequency, but the frequency changes over time during the transmission. The receiver must be synchronized in order to change frequencies as is being done by the transmitter.

The implications of bulk encryption on the various physical-layer protocol data structures are shown in figure 5-2 and discussed in section 6.

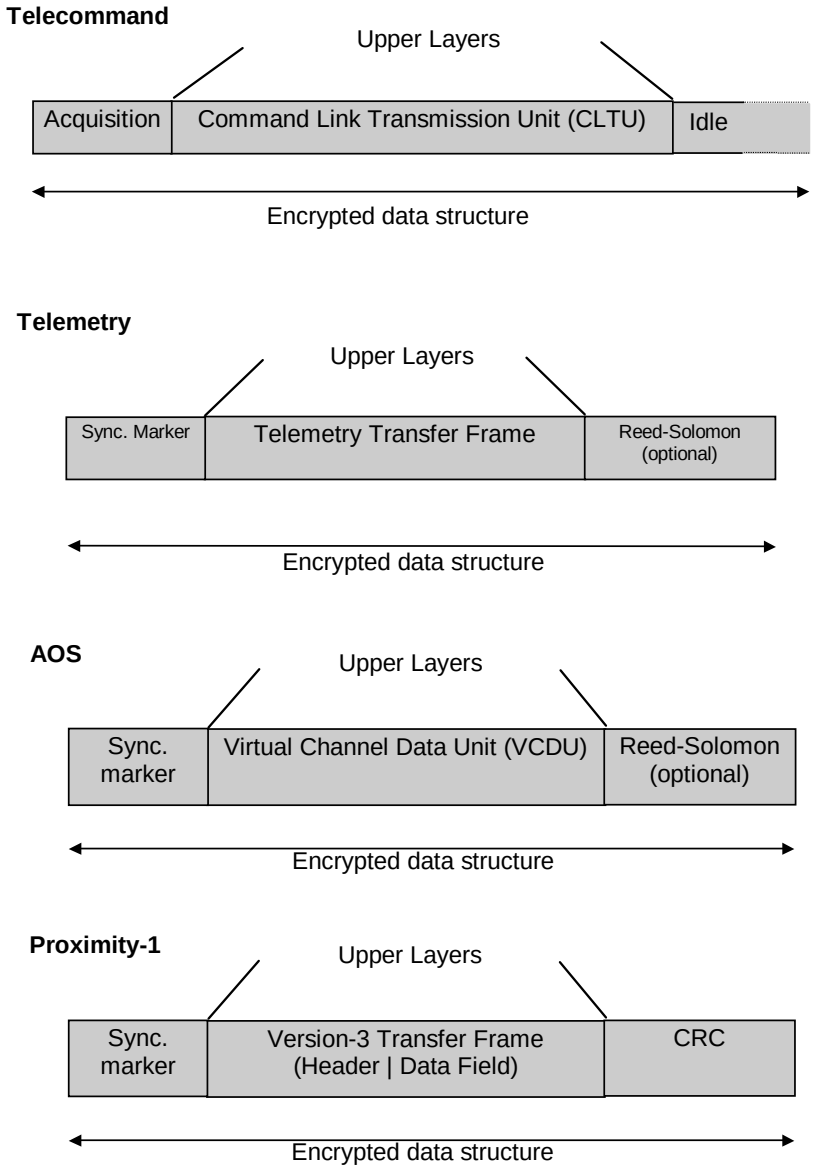

Figure 5-2: Bulk Encryption of CCSDS Protocols

5.3 DATA LINK SECURITY

Within this report, the conventional CCSDS data link layers are defined to include all the protocol layers defined within the CCSDS Space Data Link and Coding Recommended Standards (references [1]–[4]). The packet layer (including the packet header and data fields) is assumed to be located at the network layer.

The AOS data link layer includes all the AOS point-to-point Space Link Subnet (SLS) services defined in the AOS Recommended Standard (see reference [5]). These are:

– VCDU service;

- VCA service;
- Bitstream service;
- Insert service;
- Encapsulation service;
- Multiplexing service.

The AOS Path and Internet services are assumed to be part of the network layer.

The Proximity-1 data link layers are defined to include all the protocol layers defined within the CCSDS Proximity-1 (reference [18]).

The CCSDS data link layer provides protocol synchronisation, increases the space data link performance by implementing channel coding mechanisms, and provides low-level data routing functions. Also, a reliable data channel is provided through the ARQ process within the telecommand and AOS data link protocols (not available within the conventional telemetry data link). The link layer operates on the space link of the data transmission path only (i.e., not end-to-end). Proximity-1 provides a bi-directional link.

A range of security services may be applied at the Telecommand (TC), Telemetry (TM), Proximity-1, and AOS data link layers to provide confidentiality, integrity and authentication services. Implementation of access control at the data link layer is not considered; if needed, it is assumed to be provided at the application layer (layer 7).

It should be noted that security services do not have to be applied to all data units in the space link. Security services can be selectively applied to different Virtual Channels (TC, TM, and AOS) and Master Channels (TM) provided that frame headers are not encrypted. This selective application corresponds to Option B data link security as defined in the following sections. However, selective Virtual or Master Channel security may increase the difficulty of implementation, because of the incorporation of different encryption/authentication algorithms within the system, and implies an increased level of key management complexity.

5.3.1 TELECOMMAND DATA LINK SECURITY

For TC data link security, two options are considered in this report:

Option A: Implementation of security services below the transfer sublayer.

Option B: Implementation of security services below the segmentation sublayers.

Figure 5-3 outlines these two options with new *security layers* at the appropriate point in the data system. Each option has particular benefits, which are discussed, in section 6.

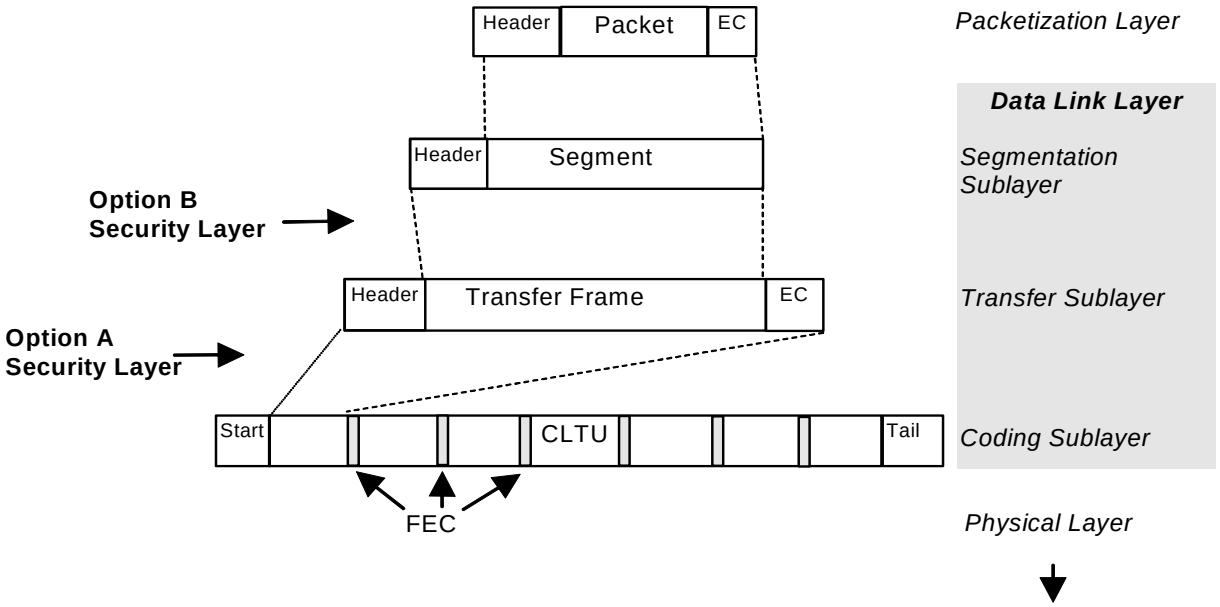

Figure 5-3: Telecommand Data Link Layer Security Options

Within both Option A and Option B, the security layer is incorporated between the relevant layers of the TC system. The necessary security services can then be contained within one layer, which will reduce the impact of security on the TC system and ensure 'clean' layering.

The basic mode of operation is encapsulation of the protocol data unit at that layer (Transfer Frame for Option A, Segment for Option B) within a new security layer protocol. The security layer protocol may implement confidentiality, authentication, and integrity services as required by the mission. The security protocol will require additional headers and trailers to be added to the data structure. An example of the headers and trailers that may be required is provided by the SCPS Security Protocol (SCPS-SP) as described in 5.4.1.

The implications of security on the TC data link protocol are discussed in section 6. Some examples of security service implementation within the TC data link protocol are presented below.

Confidentiality

Option A: The TC transfer frame is encrypted; however, the coding layer Forward Error Correction (FEC) octets and start/tail sequences are not encrypted.

Option B: The TC segment is encrypted; however, the transfer frame header and error control field are not encrypted.

Authentication

Option A: An authentication signature is appended to the transfer frame (after the error control field).

Option B: An authentication signature is appended to the segment.

Data Integrity

Option A: An Integrity Check Value (ICV) is appended to the transfer frame before the authentication signature (note that some authentication mechanisms may also provide data integrity).

Option B: An ICV is appended to the segment before the authentication signature.

5.3.2 TELEMETRY DATA LINK SECURITY

For conventional TM data link security, two options are also considered as shown in figure 5-4.

Option A: Implementation of security services below the TM Transfer Frame.

Option B: Implementation of security services above the TM Transfer Frame.

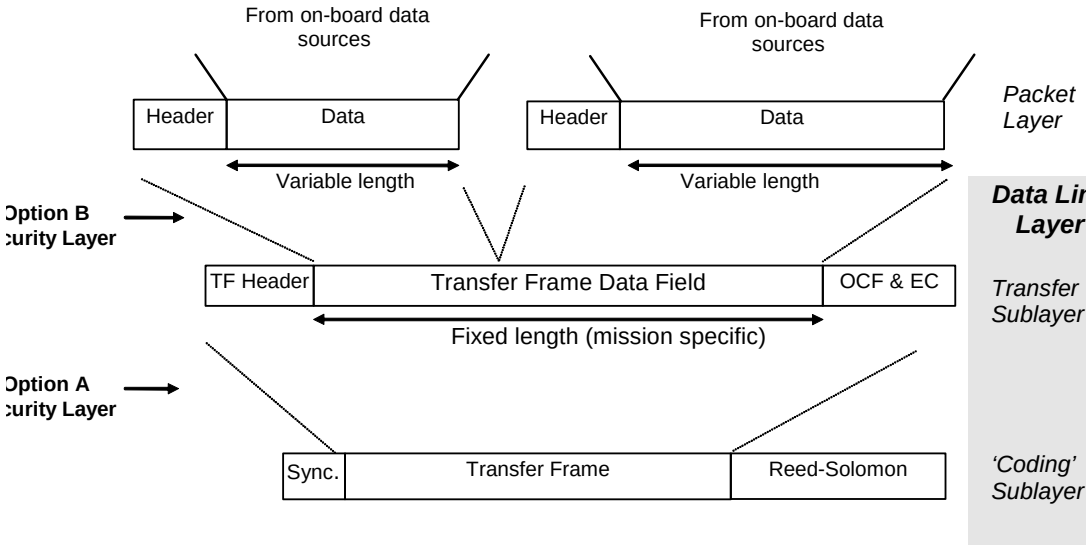

Figure 5-4: Telemetry Data Link Layer Security Options

As in the telecommand case, the security services required by the mission may be implemented within one security layer to limit the impact of security on the system. Figure 5-4 shows Telemetry Packets being multiplexed into the Transfer Frame Data Field; however, the Privately Defined Data Field (see reference [4]) may also be carried in the Transfer Frame Data Field and protected by either security Option A or B.

For Option A, the full TM Transfer Frame is encrypted after any other necessary security services (e.g., data integrity) are applied. The synchronisation word, which may be applied at the TM logical link or channel coding sublayers depending on the on-board implementation, should remain in plaintext to enable the ground systems to delimit the Channel Access Service Data Units (CA_SDU).

For Option B, the security services are applied to the Transfer Frame Data Field. For example, the application may include the addition of an ICV and encryption of the Transfer Frame Data Field. The Transfer Frame headers and trailers will remain in plaintext. In this case, the optional Frame Secondary Header (maximum 64 octets) may be used for security management functions such as key identification.

5.3.3 AOS DATA LINK SECURITY

The approach for AOS data link security is similar to the conventional case with two possible options shown in figure 5-5. Option A incorporates security services below the Virtual Channel Access (VCA) sublayer and provides a high level of protection as the complete Virtual Channel Data Unit (VCDU) is protected. Option B enables data protection and other security services to be applied to separate Virtual Channels, whilst retaining cross-support capability. Also, with Option B the security mechanisms would not interfere with the standard SLS verification techniques and would permit recovery from the effects of errors or interruptions in the communications process.

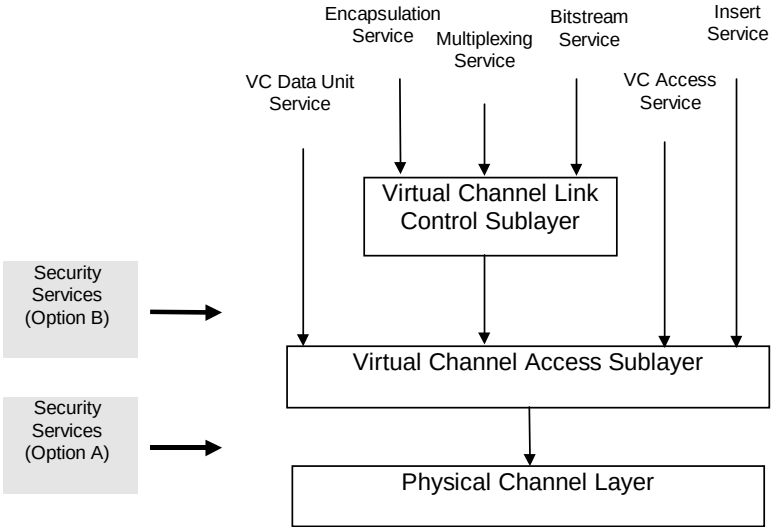

Figure 5-5: Location of AOS Security Services

If implemented within the VCA sublayer of the Space Link Subnet (Option B), the digital signature, ICV, and encrypted portion of the data should be included completely within the data field of the VCDU and should not interfere with the processing of header or trailer information. One possible location for the digital signature and/or ICV is the Insert Zone.

The Insert Zone can also be used for other security management functions such as key identification or cryptographic synchronisation.

The data structure impact of implementing security services at the VCA sublayer is shown in figure 5-6. This implementation approach for AOS security has been taken by a number of operational and planned missions (see annex A).

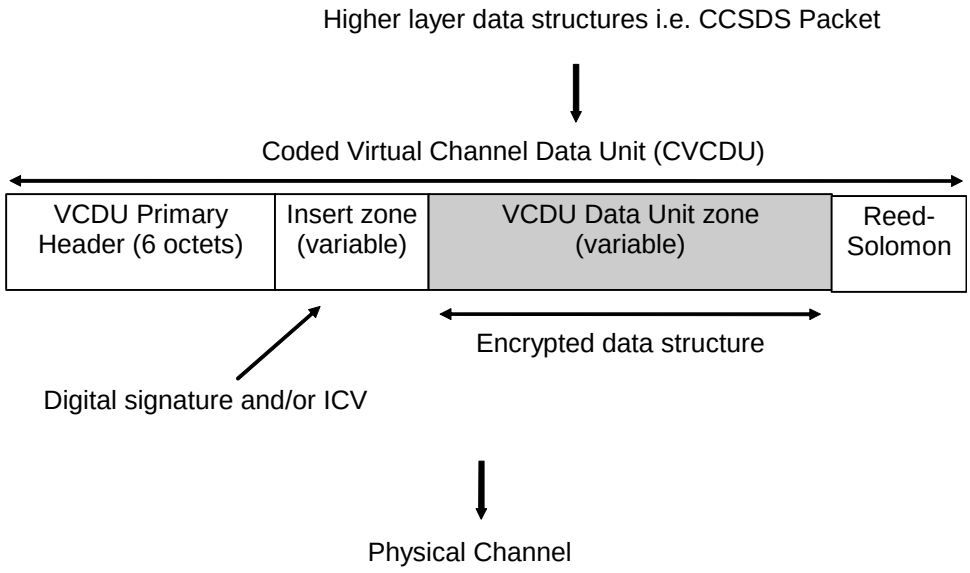

Figure 5-6: AOS VCA Sublayer Security

5.3.4 PROXIMITY-1

For Proximity-1 data link security services are best implemented above the I/O sublayer as shown in Figure 5-7.

The security services are applied to the User Data. All Proximity-1 protocol handling is carried out as it normally would be. This is analogous to the Secure Sockets Layer (SSL).

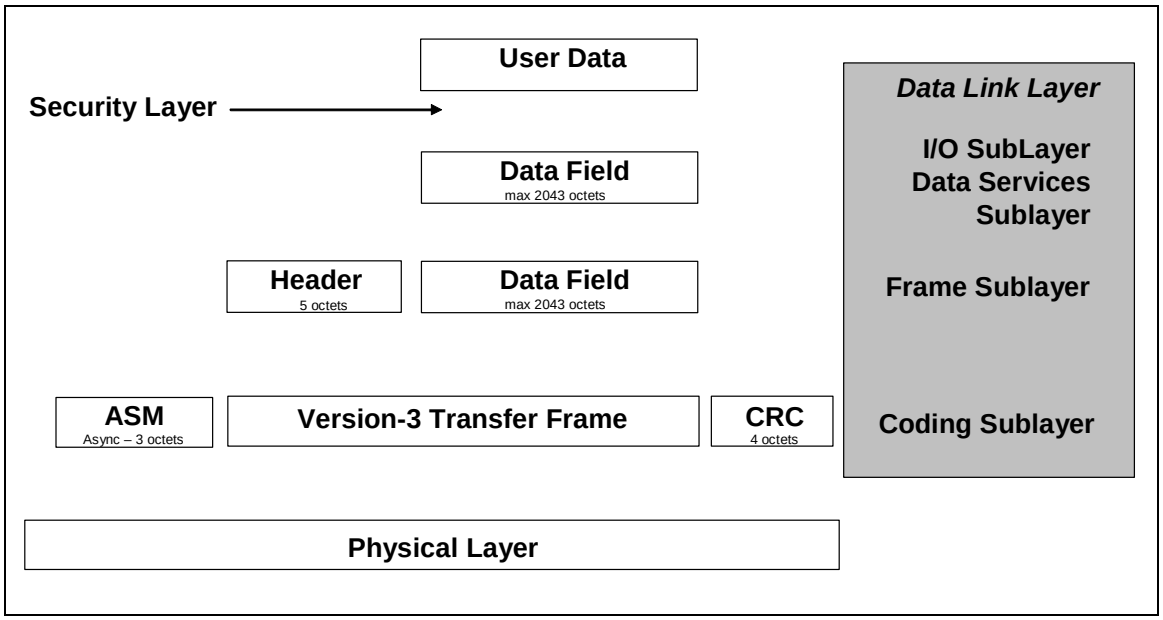

Figure 5-7: Proximity-1 Data Link Layer Security

5.4 NETWORK LAYER SECURITY

5.4.1 SCPS-SP

As part of the Space Communications Protocol Specification (SCPS), a Security Protocol (SP) has been developed to operate at the network layer in the OSI stack as indicated in figure 3-1. It is an optional protocol that may be included if the user requires *end-to-end* security services and is utilising the other protocols in the SCPS stack. SCPS-SP is based on several other layer three U.S. Department of Defence, ISO, and Internet security protocols and has been refined for space applications to ensure minimal transmitted bit overhead (see reference [8]).

The primary benefit of SCPS-SP is its ability to provide end-to-end security, i.e., from the source of the data to its final destination. Any non-security related intermediate systems and networks will not have access to the data unless explicitly authorised and therefore insecure networks may be utilised to transmit sensitive data. The communication end points are implementation specific and are defined by the implementing system. SCPS-SP does not mandate any specific security algorithm but defines the protocol framework to provide network layer data confidentiality, integrity, and authentication services for space communications systems.

The structure of SCPS-SP is shown in figure 5-8. The protocol adds a clear header of 8 bits (minimum), a protected header of 8 bits (minimum) plus options, and a variable length ICV to the protocol data unit from the layer above (e.g., SCPS Transport Protocol (TP), Internet TCP). All of the data except for the clear header is encrypted by a system-defined, implementation-specific algorithm. With there being a clear header, analysis can be performed to determine which entities are communicating with each other despite not being

able to read the data (also known as *traffic analysis*). This can be countered by the use of link layer encryption, spread spectrum/frequency hopping techniques, or both.

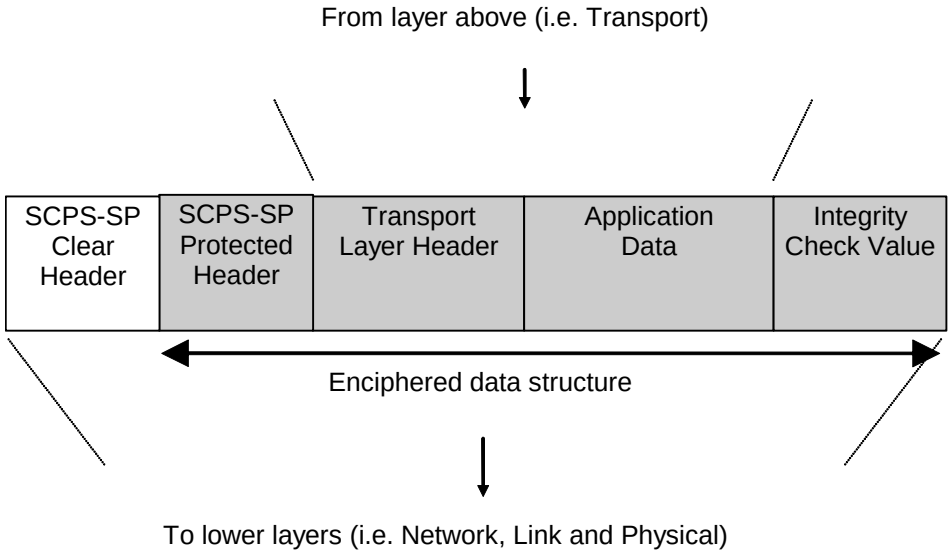

Figure 5-8: SCPS Security Protocol Structure

5.4.2 SPACE PACKET PROTOCOL SECURITY

Security may be applied at the space packet layer (see reference [11]) to protect the telecommand and telemetry data, or to achieve spacecraft command authentication. It can be achieved by encrypting the packet data field for confidentiality and including a digital signature and/or ICV within the packet data field for authentication and data integrity, respectively. The space packet protocol headers would remain unencrypted.

The concept of space packet layer security is shown in figure 5-9. Only the application data field is encrypted. The optional secondary header may also be encrypted. All other protocol fields in the lower layers of the system remain in plaintext.

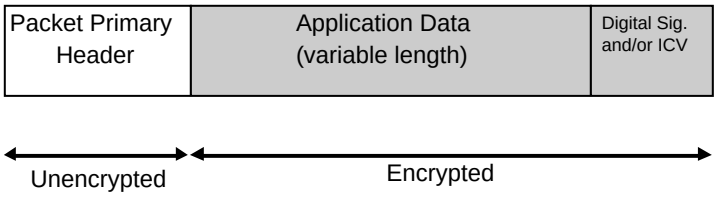

Figure 5-9: CCSDS Packet Security Concept

It should be noted that if a mission requires security of selected packets in the space link, then the Application Process Identifier (APID) in the packet header may be used to differentiate between encrypted or plaintext packets.

5.5 APPLICATION SECURITY

Security services may be applied at the application layer; however, in the case of a space mission using the space packet protocol, implementation of confidentiality, integrity, and authentication services are likely to be similar to the space packet security case as outlined in 5.4.2. However, the use of Transport Layer Security (TLS) technology (previously known as Secure Sockets Layer (SSL)) at the application layer allows individual applications the choice of implementing security services independently of the rest of the data handling system. On the positive side, the use of such services at the application layer does not require any security investment by the lower layers. Furthermore, each application requiring security services has to independently make the investment to implement security mechanisms rather than taking advantage of lower layer security services that benefit all applications. In this way, an application may make the decision to enforce security despite the fact that the underlying mission data handling system has decided against doing so. If it is decided to implement specific security services at the application layer, then it is important to ensure that consistency is maintained throughout the entire system to ensure that the security services are not compromised.

Another primary security service to be applied at the application layer is access control. Access control may be achieved by implementing secure access-rights database facilities at the mission data system access points. Access control is granted based on authenticated identity. An entity requiring access may possess a token such as an X.509 certificate containing credentials which would be authenticated before allowing access.

5.6 CCSDS SECURITY OPTION COMBINATIONS

5.6.1 GENERAL

To meet specific space mission requirements, it may be necessary to utilise a combination of the CCSDS security options defined in the previous sections. In this case security services may be implemented in multiple layers of the mission data system simultaneously.

For example, some advanced high security missions may require a combination of the network layer security to provide end-to-end data protection, particularly across ground networks, and lower layer security operating over only the space link to prevent traffic analysis between the ground and space segments. This concept, with the respective security end points, is shown in figure 5-10.

In some cases, network layer security may not be provided by the network and application layer security may be utilized instead to provide source to destination data protection. In this case, the data is protected at it source rather than in the network protocol stack potentially

affording even greater data protection. However, rather than using a network security service mechanism, each application would be responsible for implementing and calling the security service. The service may be found in a library and therefore not required to be implemented for each application but nevertheless, the application must still make an overt action to use the security mechanism rather than it automatically being applied while passing through the network layer.

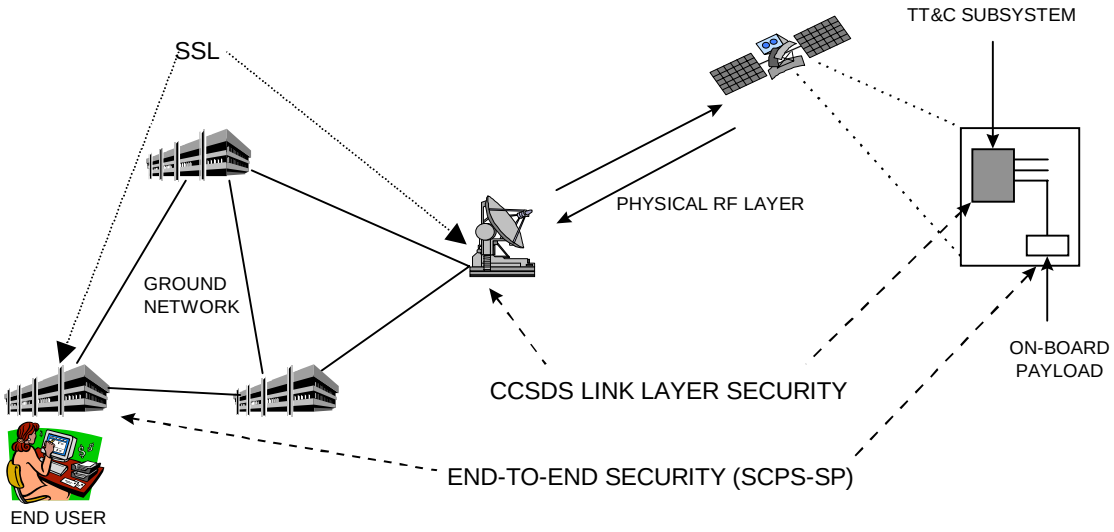

Figure 5-10: CCSDS Data Link and Network Security Combination Architecture

Space systems with a number of in-orbit resources and inter-satellite communications may also utilise the concepts proposed in the combination solution shown in figure 5-11. The combination solution may be conceived with link layer security operating on the ground-to-space links only, and network layer security operating on the communications links between different spacecraft and in the ground network.

Another alternative is the combination of terrestrial-based protocols with CCSDS protocols. For example, a principal investigator (PI) might be located at a university that is connected to the Internet. The principal investigator might make use of Internet standard desktop system protocols (e.g., IP, IPSEC, TCP, HTTP, TLS/SSL) to reach an on-board instrument via a CCSDS ground-to-space Gateway. The Gateway, in turn, runs CCSDS SCPS protocols and has the ability to bridge the terrestrial-based protocol session to a SCPS-based protocol session. This would allow the principal investigator to run a standard desktop system with little or no modification (IPSEC would require some configuration to establish a secure connection between the PI machine and the Gateway). The desktop system creates a secure connection to the gateway that in turn creates a secure connection to the spacecraft. In this way, terrestrial-based protocols are used over the Internet (where they work very well) and space-based protocols are used over the space link (where they work much better than terrestrial protocols). See Figure 5.11 for an illustration of this combination. Alternatively,

there is no reason why the space-based protocols could not be run end-to-end other than the necessity to install them on ground-based systems. Likewise, there would be no reason to not run the terrestrial-based protocols end-to-end if the environmental conditions allow (e.g., bandwidth is plentiful, continuous coverage or coverage with few, short outages).

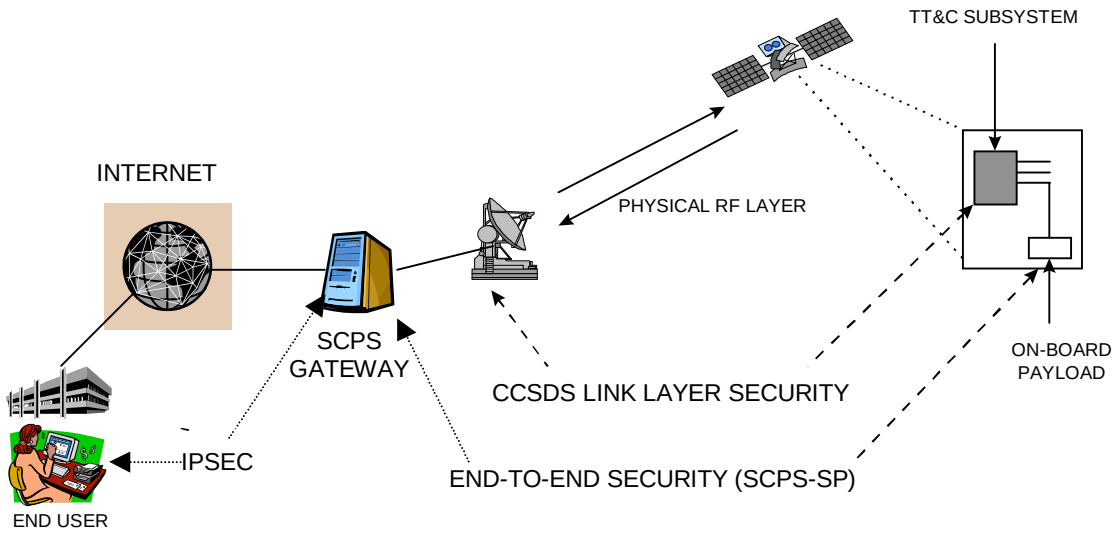

Figure 5-11: Combination of Internet and CCSDS Protocols

6 CCSDS SECURITY IMPLICATIONS

6.1 IMPACT OF ENCRYPTION

In general, confidentiality has the greatest impact on the CCSDS architecture and services, as compared with authentication and data integrity services, because specific protocol information (headers and trailers) may be hidden through encryption and may therefore be unavailable for use for other network or cross-support services. In contrast, authentication and data integrity services only require inclusion of a small number of additional fields at an appropriate point in the data structure.

The impact of confidentiality on the various CCSDS layer fields for the different security options is shown in table 6-1. The fields that are unencrypted are shown as 'Plain'.

Table 6-1: Impact of Confidentiality on CCSDS Data Fields

CCSDS Security Option	ASM + EDAC	Frame Header	Frame Data Field	Packet Header	Packet Data Field
Network Layer Security	Plain	Plain	Plain	Plain	Encrypted
Data Link (Option B)	Plain	Plain	Encrypted	Encrypted	Encrypted
Data Link (Option A)	Plain	Encrypted	Encrypted	Encrypted	Encrypted
Physical (Bulk Encryption)	Encrypted	Encrypted	Encrypted	Encrypted	Encrypted
(**ASM** - Attached Synchronisation Marker, **EDAC** - Error Detection and Correction)					

6.2 IMPACT ON EMERGENCY COMMANDING

On occasion, problems arise with spacecraft after launch or while on-orbit. Upon launch, a spacecraft may end up tumbling, unable to orient its antennas correctly and therefore not able to receive commands. Likewise, an on-orbit spacecraft may be subject to an upset due to a wide variety of occurrences (e.g., memory latching, processor upsets, etc.).

When problems arise, the operations personnel attempt to transmit emergency commands to the spacecraft. In the case of a tumbling spacecraft, this consists of a short command to allow the vehicle to reset itself and orient its antennas correctly. The emergency command is sent over and over again in the hope that it might be received during a short window in which the antennas are correctly oriented. In the case of a faulty spacecraft, this consists of a short command to cause the vehicle to go into a "safe mode" to attempt to reset the fault(s) or invoke backup equipment.

Typically, these emergency commands bypass the onboard computer and are acted upon directly by the hardware command decoder. But the question is, from a security perspective, should such emergency commands be allowed to be acted upon with or without command authentication?

If the commands are not authenticated, a security hole is opened for a potential attacker. A risk analysis must be performed to determine if this is of concern and if it should be allowed. Potentially, the sending of a reset emergency command could have no effect on a spacecraft other than the loss of availability during the subsequent restart. However, if the spacecraft has high availability requirements, then such a reset may not be welcomed. Likewise, such an unauthorized reset is highly problematic if a spacecraft is in the midst of performing navigation manoeuvres or other sensitive operations.

On the other hand, if authenticated commands are required, the size of the emergency command might increase depending on the type of command authentication employed. Whereas emergency commands are designed to be very short for the purpose of hoping that one is received and acted upon, the size increase due to authentication might negate the ability to receive emergency commands.

6.3 IMPACT ON CROSS-SUPPORT SERVICES

The CCSDS Space Link Extension (SLE) cross-support services are a set of services that provide access to the ground termination of the space link services from a remote ground-based system (see reference [12]). The SLE services can be separated into two categories:

- Return SLE services;
- Forward SLE services.

6.3.1 RETURN SLE SERVICES

The various types of cross-support services have been split into different Functional Groups (FGs) based on the CCSDS Reference Model layers. Figure 6-1 shows FGs and services included in the Return SLE architecture and the impact that each of the CCSDS security options has on the SLE services provided. The impact is defined as whether the cross-support service is available or not when using that particular security option. The CCSDS security implementation options covered include Options A and B data link security and space packet (network) layer security. Physical layer security is not considered because cross-support services are not available for this option (it is assumed that the data can be decrypted only by the end user and that no protocol information is available to enable cross-support).

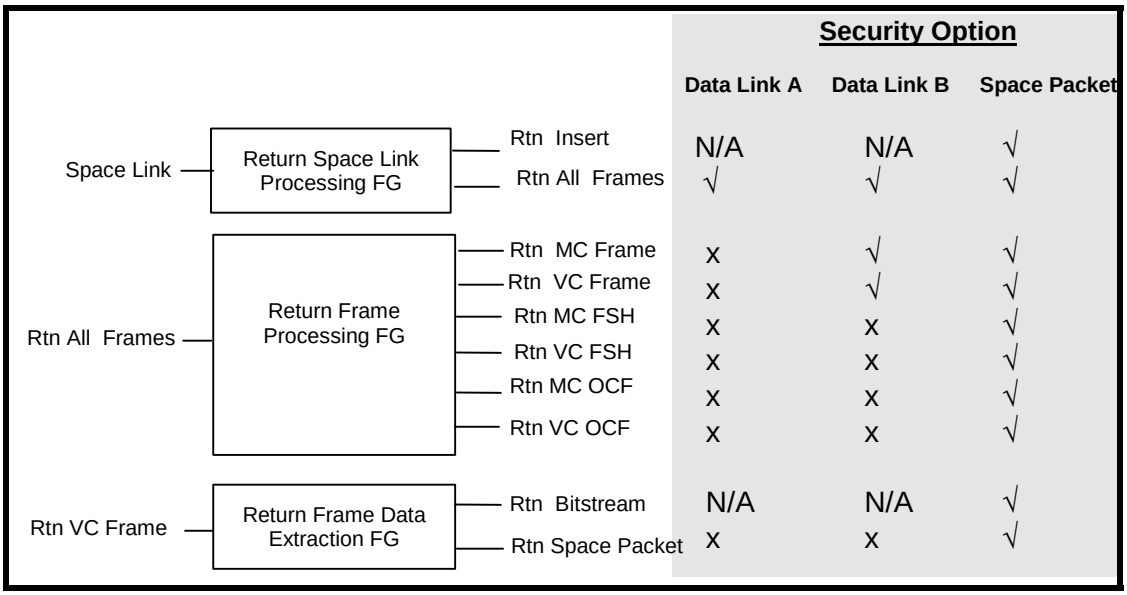

Figure 6-1: Impact of Security on Return SLE Services

6.3.2 FORWARD SLE SERVICES

Figure 6-2 shows the Forward SLE services in FGs based on the CCSDS Reference Model and the impact that each of the security options has on the services provided. The CCSDS security implementation options covered include Options A and B data link security and space packet (network) layer security. Again, physical layer security is not considered.

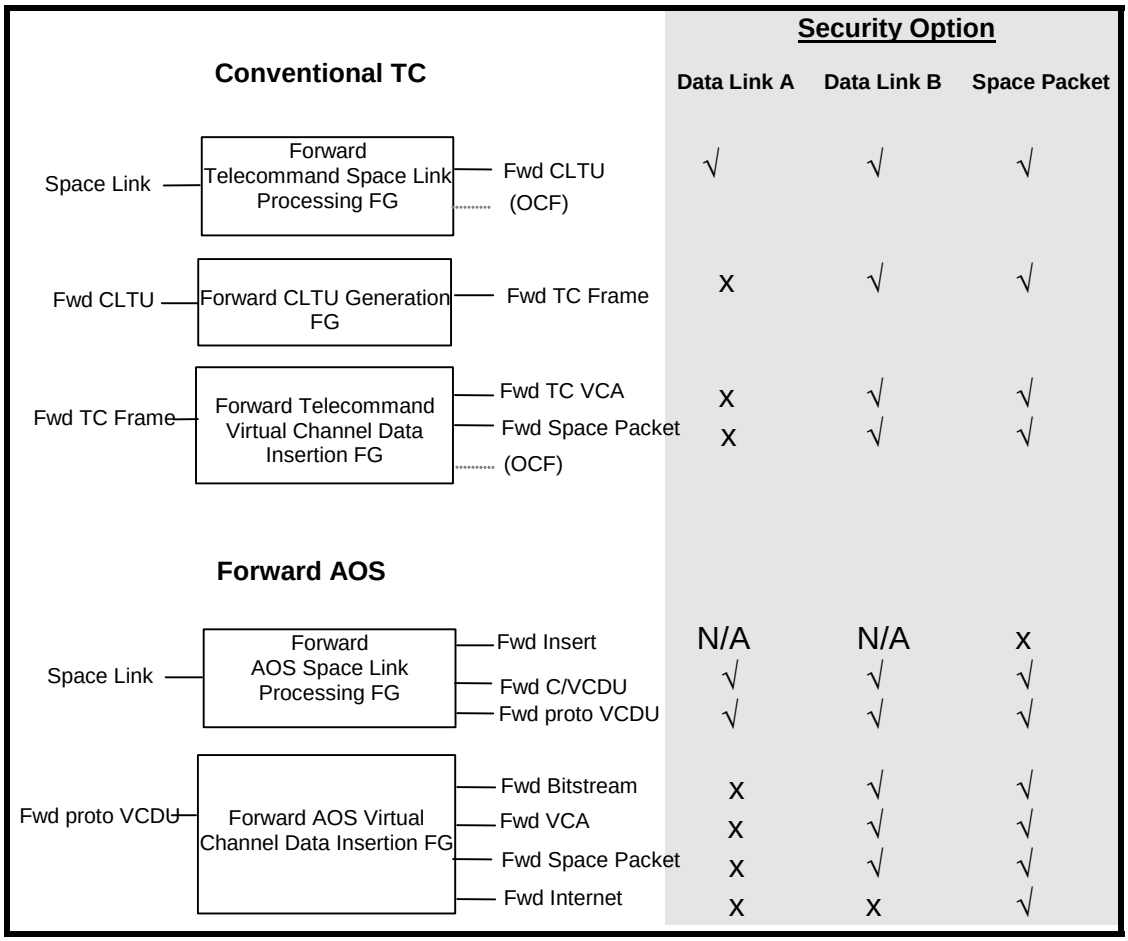

Figure 6-2: Impact of Security on Forward SLE Services

6.4 SECURITY OPTION COMPARISON

6.4.1 PHYSICAL LAYER (BULK ENCRYPTION)

Physical layer security (bulk encryption) provides the highest possible level of data confidentiality for space mission data systems but only on a point-to-point basis. No additional security services are implied other than those provided by the encryption mechanism used to provide data confidentiality.

The application of bulk encryption to the CCSDS conventional telecommand, telemetry, and AOS Recommended Standards will deny all cross-support services without pre-placed copies of the encryption keys at system access points or the use of public key technology used to encrypt content encryption keys. Also, bulk encryption does not allow the CCSDS link layer synchronisation services to operate, and, as a result, the cryptographic devices utilised must provide data synchronisation.

Bulk encryption does not allow any Error Detection and Correction (EDAC) information to be available in plaintext. Thus, all CCSDS channel coding services would be rendered

meaningless, as the data must be acquired, synchronised, and decrypted before the coding sublayer information becomes available. The CCSDS EDAC information would therefore be unnecessary overhead in such a scheme. However, it should be noted that some high-grade cryptographic devices might include independent EDAC functionally.

Bulk encryption does not provide any concept of end-to-end security in the OSI sense. It is applied to the data on a point-to-point basis with a cryptographic device at each end of a link in the communications network. However, anti-jam techniques which provide link availability (e.g., spread spectrum, frequency hopping) can and should be employed at the physical layer to ensure non-interference over the RF link.

In summary, the security requirements of high security missions would be satisfied by bulk encryption at the physical layer; however, specific operational benefits provided by the CCSDS Recommended Standards would not be available.

6.4.2 DATA LINK SECURITY

Data link layer security can be considered as a compromise for missions requiring a relatively high level of security but required to retain a number of CCSDS benefits. The CCSDS data structure may be used throughout the mission data system; however, only the coding sublayer of the data link layer and the physical layer remain in plaintext.

Traffic flow security is provided through encryption of the data link layer headers and trailers by implementing encryption below the data link transfer layers (Option A in 5.3). Specific CCSDS data link benefits such as link synchronisation and performance enhancement through EDAC mechanisms are retained as the EDAC information remains in plaintext over the space link.

Data link layer encryption does not provide end-to-end security in the OSI sense. It is applied to the data on a hop-by-hop basis; however, some low-level cross-support services are available to extend the secure space link within the ground network.

6.4.3 NETWORK

SCPS-SP provides security on an end-to-end basis, from the source of the transmitted data to the final destination. For example, an instrument control centre could be one end point where the security services (confidentiality, integrity, and authentication) are applied to the data, and an instrument on board a spacecraft could be the other end point. All intermediate systems, such as routers, gateways, and control centres, would not have access to the user data unless explicitly authorised. All applications using the network would be able to make use of the SP-provided security services with no additional burden placed on the application itself.

In order to provide end-to-end security, the SCPS-SP approach allows the headers from the layers below (e.g., network, link, and physical) to remain in plaintext to enable the

intermediate routing of the SCPS-SP protocol data units. Thus, traffic analysis protection is not provided, and the encrypted data may be intercepted in the intermediate networks. However, because the data is encrypted, confidentiality is maintained.

6.4.4 APPLICATION LAYER SECURITY

The CCSDS packet protocol or application-layer security (e.g., SSL/TLS) approaches are suitable for implementations requiring protection of only the application data itself. However, there may be requirements for a number of different application-specific security mechanisms, which could lead to duplicated effort or more importantly to the introduction of security flaws in the system (see 6.4.1). But for those payloads that must use security mechanisms when no such mechanisms are provided by the mission bus or if the provided mechanisms are not adequate, then application layer security may be the fall-back without impacting the entire program.

6.5 SECURITY OPTION SELECTION

6.5.1 CHOICE OF POSITION OF ENCRYPTION

Most space missions that require confidentiality services will not require encryption at more than one layer in the data systems architecture. By limiting the implementation of encryption to one layer, the following benefits are obtained:

- a simplified system security approach;
- minimised security-development and operating costs;
- low overall security processing requirements on the data system.

Also, if encryption implementation is limited to the network layer or below, different applications will not need to implement their own encryption mechanisms. Multiple encryption mechanisms duplicate effort and could introduce security flaws as well as increase development and operations cost. Flaws can be introduced through multiple implementations where security services are incorrectly implemented. There is less chance of propagating problems if a single, verified encryption implementation is used within the space data system.

If full traffic analysis protection is required, then encryption will need to be implemented at the physical layer on a point-to-point basis. Physical layer encryption (or bulk encryption) may be combined with transmission security techniques such as frequency hopping or spread spectrum to enhance the level of security by reducing the probability jamming, detection, and interception of the RF link.

If a mission requires a high level of security with some traffic flow confidentiality, and requires key benefits provided by use of CCSDS Recommended Standards, then data link layer security will provide the solution. It is noted that data link layer security will operate almost exclusively

over the space link only; however, low-level SLE services (Return All Frames and Forward CLTU) may be used to extend the secure space data link within the ground network.

If a mission requires confidentiality of different virtual channels, which could correspond to confidentiality between different payloads on a shared spacecraft, then encryption should be included above the frame sublayer (conventional transfer frame or AOS VCDU) within the data link layer. This approach corresponds to the conventional CCSDS 'B options' and AOS security approach described in 5.3.

If a mission requires end-to-end protection of all data in the space mission data system, then either application-layer or network-layer encryption should be chosen. Depending on the mission data system architecture, network-layer encryption may be implemented via use of the SCPS-SP confidentiality service or via encryption of the space packet protocol as described in 5.4. Alternatively, Option B as described in section 5.3 would also provide end-to-end protection as long as no intermediate systems or SLE come into play.

If a mission requires a high granularity of data protection (for example, a separate key for encryption of different application data in the system) or selective field data protection, then encryption of the different application processes is necessary. Although more complex to implement, selective field encryption may be beneficial to protect only the sensitive fields in the application data, as most cryptographic algorithms consume large amounts of processing power.

If a mission requires high security over the RF medium, with additional end-to-end security services in the ground network or on board the spacecraft, then encryption may need to be provided at more than one layer. For example, bulk encryption or data link layer security may be applied on all space-ground and ground-space links with additional encryption at the network layer to achieve end-to-end data protection.

6.5.2 LOCATION OF OTHER SECURITY SERVICES

The choice of implementation of authentication, data integrity, and access control services has less impact on the data system architecture. For example, it may be beneficial to locate the additional fields (e.g., digital signature, ICV, sequence number) that may be required for authentication and data integrity services at the same layer as encryption to keep all security services in one 'clean' security layer.

Otherwise, it may be more appropriate to provide authentication and data integrity between different network-layer or application-layer entities. The choice is very much dependent on the data system's architecture, the protocol in use, and the mission security requirements.

Access control security services are likely to be implemented at the application layer. Many missions may wish to utilise the access control mechanisms built into network operating systems (e.g., Windows NT/2000, UNIX). Other missions may elect to use other access control systems such as Radius or certificate-based identity.

ANNEX A

SPECIFIC AGENCY SECURITY IMPLEMENTATIONS

A1 THE ESA TELECOMMAND AUTHENTICATION APPROACH [*HISTORICAL*]

ESA had standardised their approach to telecommand authentication within the ESA Packet Telecommand Standard (reference [14]). While this approach was adopted as an ESA standard and was implemented within space-qualified chip sets integrated into ESA spacecraft, it is no longer a standard. Modern, high speed processors and flaws in its foundation technology (Knapsack) have relegated this authentication standard as historical. It is presented here only as an illustration of a technology that can be adopted by a space agency.

The technique appends a digital signature (generated by an authentication algorithm with a secret key, the command data, and an additional counter) to the telecommand packet as part of the segmentation layer. The inclusion of a counter, which increments each time a telecommand segment is successfully authenticated on board the spacecraft, provides protection against replay attack (i.e., anti-spoofing). In effect, an authentication and data integrity sublayer is included between the transfer sublayer and the segmentation sublayer. Data confidentiality services are not provided by the system.

ESA have specified that a nine octet 'authentication tail' be added to the segmentation layer. The general layout of the layer is shown in figure A-1. The counter is defined as a two-bit identifier and thirty-bit count number. The authentication signature is a five-octet data field. The ESA authentication approach is similar to the space packet layer security concept described in 5.4.2 with authentication and data integrity services implemented.

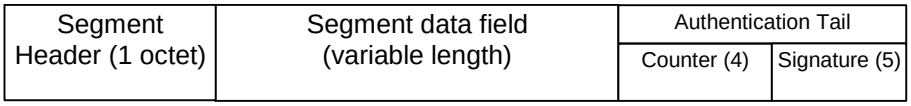

Figure A-1: ESA Telecommand Authentication Sublayer Structure

A2 INTERNATIONAL SPACE STATION

The International Space Station (ISS) mission communications system uses the AOS Recommended Standard (reference [5]) for the telecommand and telemetry links. The Multiplex Protocol Data Unit (MPDU) and Bitstream services are used to support different data types.

Encryption using the Data Encryption Standard (DES) algorithm is incorporated on the uplink at the VCA sublayer as described in 5.3 of this report. This means that the VCDU data unit zone is encrypted. The insert zone (set to 64 bits) is used to provide cryptographic synchronisation.

A3 EUMETSAT

EUMETSAT are planning to implement security on the downlink of the METOP polar orbiting spacecraft. The proposed location of security is similar to the ISS implementation, with the VCDU data zone encrypted via the triple DES (3DES) algorithm. The insert zone (set to 16 bits) is used for encryption control.

EUMETSAT have also implemented encryption on the Meteosat Second Generation (MSG) spacecraft.

A4 THE SPACE TECHNOLOGY RESEARCH VEHICLE 1C/D MISSIONS

The Space Technology Research Vehicle (STRV) 1c/d microsatellite missions designed and implemented conventional CCSDS data link layer security on the telecommand and telemetry links. This corresponds to the Option A security layers in 5.3. Confidentiality and authentication services were implemented as part of the security layer on the telecommand link, with confidentiality only on the telemetry link.

A5 THE ESA AUTOMATED TRANSFER VEHICLE

The Automated Transfer Vehicle (ATV), the European servicing vehicle for the International Space Station (ISS), protects its Telecommand link by applying encryption and time authentication to its Telecommand Packets.

The encryption sublayer concept illustrated in figure A-2 below follows the Triple Data Encryption Standard (3-DES) as per ANSI-X.9-52. The Segment Data field includes the following three fields:

– A 2-octet Key Index, pointing to the decryption key;

– A 8-octet Initialization Vector (IV), which is unique per message;

– Encrypted Packet Data.

Telecommand packets include a Time Authentication field. The spacecraft Telecommand Packet processor compares the packet value of this field with the spacecraft Onboard Time. If the value is higher than a threshold value, the Packet is rejected.

<table>
<tr><td rowspan="2">Segment Header</td><td colspan="3">Segment Data Field</td></tr>
<tr><td>Key Index</td><td>Init. Vector</td><td>Encrypted Packet Data</td></tr>
</table>

Figure A-2: ESA ATV Telecommand Encryption Sublayer Structure