The Consultative Committee for Space Data Systems

Recommendation for Space Data System Practices

SECURITY ARCHITECTURE FOR SPACE DATA SYSTEMS

RECOMMENDED PRACTICE

CCSDS 351.0-M-1

MAGENTA BOOK
November 2012

The Consultative Committee for Space Data Systems

Recommendation for Space Data System Practices

SECURITY ARCHITECTURE FOR SPACE DATA SYSTEMS

RECOMMENDED PRACTICE

CCSDS 351.0-M-1

MAGENTA BOOK
November 2012

AUTHORITY

Issue:	Recommended Practice, Issue 1
Date:	November 2012
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 represents the consensus technical agreement of the participating CCSDS Member Agencies. The procedure for review and authorization of CCSDS documents is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-3), and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the address below.

This document is published and maintained by:

CCSDS Secretariat
Space Communications and Navigation Office, 7L70
Space Operations Mission Directorate
NASA Headquarters
Washington, DC 20546-0001, USA

STATEMENT OF INTENT

The Consultative Committee for Space Data Systems (CCSDS) is an organization officially established by the management of its members. The Committee meets periodically to address data systems problems that are common to all participants, and to formulate sound technical solutions to these problems. Inasmuch as participation in the CCSDS is completely voluntary, the results of Committee actions are termed **Recommendations** and are not in themselves considered binding on any Agency.

CCSDS Recommendations take two forms: **Recommended Standards** that are prescriptive and are the formal vehicles by which CCSDS Agencies create the standards that specify how elements of their space mission support infrastructure shall operate and interoperate with others; and **Recommended Practices** that are more descriptive in nature and are intended to provide general guidance about how to approach a particular problem associated with space mission support. This **Recommended Practice** is issued by, and represents the consensus of, the CCSDS members. Endorsement of this **Recommended Practice** is entirely voluntary and does not imply a commitment by any Agency or organization to implement its recommendations in a prescriptive sense.

No later than five years from its date of issuance, this **Recommended Practice** will be reviewed by the CCSDS to determine whether it should: (1) remain in effect without change; (2) be changed to reflect the impact of new technologies, new requirements, or new directions; or (3) be retired or canceled.

In those instances when a new version of a **Recommended Practice** is issued, existing CCSDS-related member Practices and implementations are not negated or deemed to be non-CCSDS compatible. It is the responsibility of each member to determine when such Practices or implementations are to be modified. Each member is, however, strongly encouraged to direct planning for its new Practices and implementations towards the later version of the Recommended Practice.

FOREWORD

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommended Practice is therefore subject to CCSDS document management and change control procedures, which are defined in the *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-3). Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be addressed to the CCSDS Secretariat at the address indicated on page i.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 351.0-M-1	Security Architecture for Space Data Systems, Recommended Practice, Issue 1	November 2012	Original issue

CONTENTS

Section Page

CONTENTS (continued)

Section Page

Figure

CONTENTS (continued)

1 INTRODUCTION

1.1 PURPOSE AND SCOPE

1.1.1 PURPOSE

This document is intended as a high-level systems engineering reference to enable engineers to better understand the layered security concepts required to secure a space system. As such, this document is a Security Architecture for Space Data Systems (SASDS).

This architecture uses the views described in the Reference Architecture for Space Data Systems (reference [B1]) developed by the CCSDS Architecture Working Group.

The SASDS will be used:

- to establish an overall CCSDS conceptual framework for the incorporation of security into the data systems of space missions;
- to define common language and representation so that risks, requirements, and solutions in the area of security within space data systems can be readily communicated;
- to provide a source of information for the security architects on a space mission to use to develop the system security design;
- to facilitate development of standards in a consistent way so that any standard can be used with other appropriate standards in a system.

1.1.2 SCOPE

This document presents a security reference architecture for space data systems and is intended to provide a standardized approach for description of security within data system architectures and high-level designs, which individual working groups may use within CCSDS.

For further information regarding security’s role in space systems, the reader is directed to the supporting CCSDS documentation listed in annex B.

1.1.3 RELATIONSHIP WITH OTHER CCSDS DOCUMENTS

The relationship between this and other CCSDS documents is shown in figure 1-1 below:

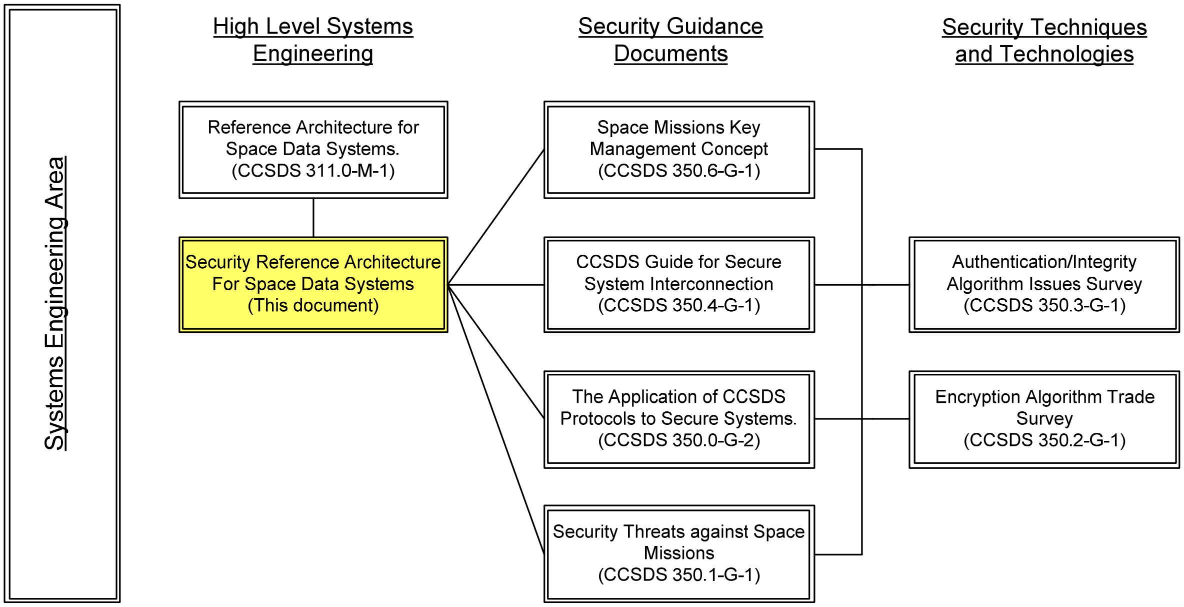

Systems Engineering Area
High Level Systems Engineering
Security Guidance Documents
Security Techniques and Technologies
Reference Architecture for Space Data Systems. (CCSDS 311.0-M-1)
Security Reference Architecture For Space Data Systems (This document)
Space Missions Key Management Concept (CCSDS 350.6-G-1)
CCSDS Guide for Secure System Interconnection (CCSDS 350.4-G-1)
The Application of CCSDS Protocols to Secure Systems. (CCSDS 350.0-G-2)
Security Threats against Space Missions (CCSDS 350.1-G-1)
Authentication/Integrity Algorithm Issues Survey (CCSDS 350.3-G-1)
Encryption Algorithm Trade Survey (CCSDS 350.2-G-1)

Figure 1-1: Relationship between This and Other CCSDS Documentation

1.2 DOCUMENT STRUCTURE

Section 2 provides an introduction into how the security architecture uses the Reference Architecture for Space Data Systems (RASDS).

Section 3 discusses the security concepts that need to be addressed by any security architecture.

Section 4 examines the security concepts and shows how the CCSDS architecture outlined in sections 2 and 3 relate to each other.

Section 5 establishes high-level principles and the scope that the security architecture addresses.

Section 6 illustrates a series of mission profiles which help identify where security is required, what the issues are, and what solutions are applicable.

Section 7 specifies the security reference architecture.

Annex **A** addresses security considerations pertaining to use of this Recommended Practice for developing real security architectures for missions.

Annex B lists informative references.

Annex C is a glossary of abbreviations and acronyms used in the document.

1.3 GLOSSARY OF TERMS

A full glossary of security terms used within this document is available in reference [B9].

1.4 NOMENCLATURE

1.4.1 NORMATIVE TEXT

The following conventions apply for the normative specifications in this Recommended Standard:

a) the words ‘shall’ and ‘must’ imply a binding and verifiable specification;

b) the word ‘should’ implies an optional, but desirable, specification;

c) the word ‘may’ implies an optional specification;

d) the words ‘is’, ‘are’, and ‘will’ imply statements of fact.

NOTE – These conventions do not imply constraints on diction in text that is clearly informative in nature.

1.4.2 INFORMATIVE TEXT

In the normative sections of this document, informative text is set off from the normative specifications either in notes or under one of the following subsection headings:

- Overview;
- Background;
- Rationale;
- Discussion.

2 THE CCSDS REFERENCE ARCHITECTURE

2.1 INTRODUCTION

RASDS (reference [B1]) describes a method for analyzing complex space system architectures. This section briefly introduces these concepts prior to exploring how they can be used to address security concerns during system design. Reference [B1] should be consulted for more information on RASDS.

2.2 BACKGROUND

Today, ubiquitous terrestrial network connectivity among principal investigators and mission operations has become standard. At the same time, computer processing power and communication resources have progressed steadily to the point that they are easily accessible to potential attackers. These two facts put mission operations more at risk than in the past when operations were carried out over closed, mission-specific networks, and computer and communication resources were not as powerful or widespread. The security risks to both spacecraft and ground systems have increased to the point where CCSDS must foster adoption of specific information security standards (as necessary) in order to protect mission-critical resources and sensitive mission information.

CCSDS promotes secure interoperability for space missions and the incorporation of security within the system. This security architecture helps to complete CCSDS's overall reference architecture by adding specific guidance for developing the security aspects of a system architecture. The security architecture for a mission should respond to threats identified via a risk assessment, which is necessary to provide mission planners with a better understanding of the risks that they should plan to counter via security technologies.

Key factors to consider for space missions are the vulnerability of sophisticated space or ground resources to potential attackers the consequences of the malicious use of public assets, including consequences of public perception. For example, hacking into the telecommand system of any Mars mission would be extremely visible, extremely embarrassing, and potentially very costly for affected CCSDS member agencies.

2.3 CCSDS REFERENCE ARCHITECTURE

RASDS employs multiple *views* to present a space data system architecture. Space data systems are complex, consist of hardware, software, and organizations, and are frequently composed of elements belonging to different organizations, some of which are on the ground, others of which are in space. Because of the complexity of these systems, it is difficult to depict all of these various aspects in a single framework. As a result, the system architecture is described with multiple views, each focusing on different concerns associated with the system.

A *view* is a form of abstraction achieved by using a selected set of architectural concepts and structuring rules in order to focus on particular concerns within a space data system. Further background information is available in RASDS (reference [B1]). Each view is developed in the context of a specific viewpoint specification.

Five types of viewpoints and associated *views* are described in RASDS:

1) Enterprise Viewpoint: The motivation for Enterprise Views is that there are complex organizational relationships involving spacecraft, instruments, ground systems, scientists, staff, and contractors that are distributed among multiple organizations (space agencies, science institutes, companies, etc.). The Enterprise View is used to address these organizational relationship aspects of space data systems. The Enterprise View describes the organizations involved in a space data system and the relationships and interactions among them. The relationships are described in terms of the roles, responsibilities, and policies of the organizations; and the interactions among the organizations are described in terms of agreements and contracts.

2) Connectivity Viewpoint: The motivation for Connectivity Views is that the physical deployment and behavior of both ground-based and flight-system elements need to be considered. The flight elements are in motion through space and consequently cause network topology and connectivity issues associated with pointing, scheduling, delays due to round-trip light times, and low signal-to-noise ratios. To deal with these issues, special protocols and functionality are required. The Connectivity View is used to address these aspects of space data systems. The Connectivity View describes the physical structure and physical environments of a space data system.

3) Functional Viewpoint: The motivation for Functional Views is that the behavior of functional elements and their logical interactions should be considered separately from the engineering concerns of where functions are housed, how they are connected, which protocols are used, or what language is used to implement them. The Functional View is used to address these functional aspects of space data systems. The Functional View describes the functional structure of a space data system and how functions interact with each other.

4) Information Viewpoint: The motivation for Information Views is that descriptions of data objects with different structures, relationships, and policies must be provided. These data objects are passed among the functional elements and managed (that is, stored, located, accessed, and distributed) by information infrastructure elements. The Information View is used to address these aspects of space data systems. The Information View looks at the space data systems from the perspective of the Information Objects that are exchanged among the Functional Objects.

5) Communications Viewpoint: The motivation for Communications Views is that the layered sets of protocols used to support communications among the functional elements must be described. These must meet the requirements imposed by the connectivity and operational challenges. The Communications View is used to address these aspects of space data systems. The Communications View describes the protocol stacks and mechanisms of information transfer that occur among physical entities (i.e., Nodes) in a space data system.

3 GENERAL SECURITY PRINCIPLES

3.1 GENERAL

Security aspects of a Space Data System architecture may also be addressed using the same set of viewpoints as those discussed in section 2. These views can describe the security aspects from functional, physical, or communications perspectives, and are in line with the standard approaches used in literature:

– physical security (Enterprise, Connectivity Viewpoints);

– information security (INFOSEC, Connectivity, Communications, Enterprise, Functional and Information Viewpoints);

– transmission security (TRANSEC, Connectivity, Communications Viewpoints).

3.2 PHYSICAL SECURITY

Physical security is concerned with protecting the actual equipment that makes up a system. It is often noted that there is little point to having sophisticated firewalls to stop people hacking into a computer to steal the data stored in it, if they can just walk in, pick up the whole computer or hard disk(s), and walk out with it. Physical security is concerned with providing barriers such as guards, fences, locked rooms, etc. While not the primary focus of this document, physical and personnel security requirements must be considered, and these may be addressed in a Connectivity View (physical aspects) or in an Enterprise View (personnel).

3.3 INFORMATION SECURITY

INFOSEC is concerned with the protection of information whether ‘at rest’ or in transit from one place to another. The main principles associated with information security are:

a) authentication of users and computers;

b) confidentiality of data;

c) integrity of data;

d) availability of data.

Authentication is the means by which a computer (or system) verifies the identity of an agent on the system, be this a person, service, or computer. For example, authentication could occur when the identities of entities on the ends of a communication channel are verified or when a user logs on to a system.

Confidentiality is the means by which a system ensures that only authorized users, services, or systems access controlled data. Confidentiality is often achieved by the use of encryption. There are many different methods by which encryption can be employed and many different algorithms can be used. A full discussion of encryption is outside the scope of this architecture, although some aspects will be mentioned later in this document. (See reference [B2] for more information.)

Integrity is the process of ensuring that data has not undergone an unauthorized change either in transit or since it was last verified. This can be achieved either as a byproduct of an encryption process, by using a Message Authentication Code (MAC), or by using a Digital Signature.

Availability is the means by which the timely accessibility of a system by an authorized entity is assured. For example, it can be measured in uptime. This issue often manifests in mitigation against Denial-of-Service attacks, whether intended and malicious or accidental.

3.4 TRANSMISSION SECURITY

TRANSEC provides mechanisms for hiding the presence of the communications link and/or preventing the link from being jammed. Thus TRANSEC dictates Physical Layer schemes for securing a link between two points. An example is use of spread spectrum or frequency hopping on an RF link. This should be addressed in a Communications View.

3.5 PROCEDURES

The System-specific Security Requirements Statement (SSRS) defines the minimum security requirements necessary for the system to be considered sufficiently secure for the intended mission. The above schemes describe different techniques and technologies for fulfilling an SSRS.

The technical implementations must be used in conjunction with written policies, or Security Operating Procedures (SECOPS) which describe what is required both for the systems and the people that use them. Procedures, policies, requirements, and other constraints will typically be addressed in an Enterprise View.

3.6 MISSION SECURITY DOCUMENTATION

3.6.1 GENERAL

Every space mission should develop the following security documents in the order listed:

a) Security Policy;

b) Security Interconnection Policy;

c) Mission Security Risk Assessment;

d) Mission Security Architecture;

e) Security Operating Procedures.

3.6.2 SECURITY POLICY

The mission security policy should be observant of any higher-level national or agency security policies but should clearly state:

a) the confidentiality classification, and therefore level of protection, of all the information associated with the mission, both live and archive, telemetry, telecommand, and ground systems;

NOTE – This classification is relevant to all of Confidentiality, Integrity, and Availability aspects of the information.

b) the roles and responsibilities of those who have access to the system;

c) the integrity requirements of the system;

d) the availability requirements of the system.

3.6.3 SECURITY INTERCONNECTION POLICY

The mission interconnection policy should clearly state;

a) which organizations will be allowed to interconnect to fulfill the mission;

b) the type of connections that will be made, e.g., continuous or intermittent;

c) the interface of these connections, e.g., dedicated link, Internet, or dial up;

d) the classification of the information going over those links.

For further information, the CCSDS Guide for Secure System Interconnection (CCSDS 350.4-G-1, reference [B8]) should be referenced.

3.6.4 RISK ASSESSMENT

The risk assessment considers the type of the mission and the information security risks to that mission. It is important to consider all parts of the mission architecture during all phases of the mission because the risk profile will change as the mission progresses. Reference [B7] contains a more detailed discussion of mission risk assessment.

It should be noted that the threat assessment will use the outputs of the Security Policy and Security Interconnection documents to help identify attack vectors and the value of the data and assets to be protected.

3.6.5 MISSION SECURITY ARCHITECTURE

The security architecture for the mission is the logical system design with a focus on security. It should be developed in step with, and as part of, the system architecture.

The security architecture will shape how the system architecture is formed and will need to be developed and adapted as the system design matures to ensure that the mission goals can be achieved while maintaining compliance with the Security Policy.

The Security Architecture will use the system security requirements, System Security Policy, Security Interconnection Policy, and the results of the Risk Assessment as inputs.

NOTE – It is strongly advised that the security architecture be developed in parallel with the overall system design in order to avoid the possibility of costly and time-consuming system redesigns which might be necessary to accommodate required security features. Some system vulnerabilities can be determined only after the detailed design of key security-related equipment has been submitted to evaluation. Hence, it is possible that a second iteration may be required.

3.6.6 SECURITY OPERATING PROCEDURES

The SECOPS define how the users of the system are expected to operate it, and what is and is not allowed. They allow the security designer to consider the use of procedural measures to protect system security and are an integral part of the system design. The SECOPS form part of the overall system concept of operations.

Trades-offs between the use of procedures vs. technology allow for more elegant solutions without the need for resorting to overly complex and costly, purely technological solutions.

4 SECURITY AND THE CCSDS REFERENCE ARCHITECTURE

4.1 OVERVIEW

This section introduces a series of recommendations for describing the security aspects of system design for each of the viewpoints identified in the CCSDS Reference Architecture. It also provides guidance on how to analyze the system design from each of these viewpoints.

4.2 SECURITY AND THE ENTERPRISE VIEW

4.2.1 GENERAL

Security within the Enterprise View is concerned with the concept of policies and trust between organizations, particularly where cross support and interoperability are required. Many different organizations may be involved in developing and supporting a space mission. In order to ensure that a consistent approach to security is applied across these organizations, a Security Policy should be established explaining the high-level security requirements, roles, and responsibilities for the mission.

Some form of agreement must exist between participating organizations within the mission. This may take the form of, for example, a Memorandum of Understanding (MoU), a Memorandum of Agreement (MoA), a contract, or a teaming agreement. These agreements should refer to the Security Policy for the mission and state that all participants must adopt and enforce the policy. The means for doing governance and for assessing compliance must also be clearly articulated.

There may be conflicts between organizations with regard to security policy enforcement. To reduce the impact of problems associated with security conflicts, the lead agency must work with its partners to ensure that the security policy is adopted and enforced by all organizations involved.

An example of a security consideration within the Enterprise View, as illustrated in figure 4-1, is the use of an agency’s Telemetry, Tracking, and Control (TT&C) network by another agency. The owning agency is likely to have network security requirements that other organizations must adhere to when connecting to its network. Furthermore, the agency offering TT&C support services may also have access to mission data as part of a quid-pro-quo arrangement (e.g., the science team in the example below). These interfaces and technical data exchange points should be defined and documented; agreements should be established regarding their management and implementation (for example, the use of security mechanisms relating to access control, authentication, and confidentiality). All of these interfaces and security requirements must be captured within the contract or service agreement between Agencies.

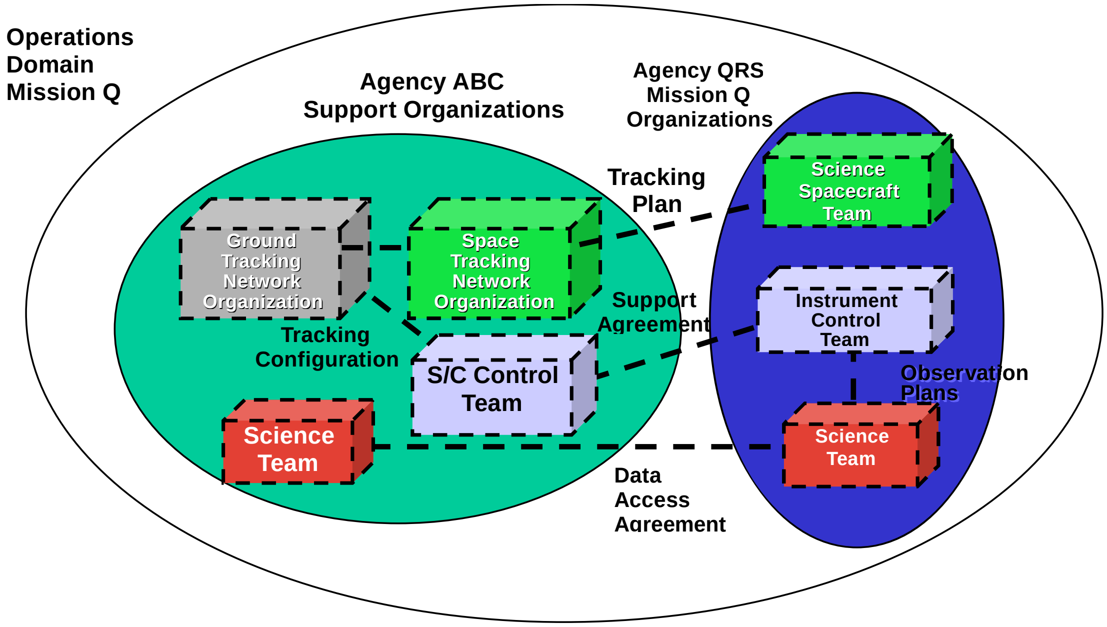


Figure 4-1: Enterprise View

4.2.2 SECURITY RISKS HIGHLIGHTED BY THE ENTERPRISE VIEW

The Enterprise View illustrates where information needs to go in order to be useful and which organizations need to communicate in order for a mission to be a success.

There are two distinct trust relationships that need to be considered by the security architecture:

a) If all of the agencies involved in a mission trust each other (at least at a system level) then the entire security of the system is as robust as the weakest agency and the risks associated with interconnected systems. In this scenario all the agencies must agree to a specific level of security and trust each other to abide by that policy.

b) If the agencies do not fully trust each other, there are two methods for interacting (assuming the agencies still need to cooperate in order to complete the mission). The first is for them to concentrate on the infrastructure and the second is for them to concentrate on the data. When an agency concentrates on infrastructure, it isolates all the systems that must deal with an untrusted entity from all its other systems. In this way it limits the damage that can be caused by a security breach such as a virus. This is expensive, as it tends to replicate existing systems and limits how information for that mission can be processed and compared or combined with other information. When an agency concentrates on the data, it places strong barriers between itself and the untrusted entity so that it can check all communications between itself and the other enterprise.

The type of relationship between the organizations will influence the nature of the interactions they will have and how they ensure security. Another factor to consider is where they interact. This can be on the ground, in space, between spacecraft, or in the case of the multi-mission spacecraft as discussed in 6.8, onboard a spacecraft.

Examining the mission structure through the Enterprise View reveals what Security Policies need to be developed, and identifies where the trust relationships will lie. For example, this approach should help identify agreements that must be reached between agencies. The technical system and security architecture should seek to enforce the Security Policies and agreements wherever possible.

4.3 SECURITY AND THE CONNECTIVITY VIEW

4.3.1 GENERAL

The Connectivity View, as illustrated in figure 4-2, reflects the physical nodes that compose the space mission operations data network, where the nodes are located, and how the nodes communicate.

In traditional terrestrial communication systems, full-period connectivity is assumed to be available between nodes at all times. This is not the typical case when dealing with spacecraft.

With the exception of geostationary missions, orbital mechanics will result in the disruption of line-of-sight communications from any given ground station. For deep-space missions, power must be conserved, and communications systems may need to be deactivated for periods of time. Spacecraft science observational schedules may result in pointing that precludes concurrent communications, or planetary bodies may obscure the radio link as the spacecraft passes behind them. In addition, space communications links are often asymmetric, with two or more orders of magnitude difference in forward data rates versus return data rates.

Any security enforcing system applied to the communications link must be able to cope with breaks in communications, both expected and unexpected, and communications asymmetries, and must be able to recover gracefully without rendering a node inactive.

Breaks in communications are not the only factor introduced by the Connectivity View. Speed and quality of communications are also issues. While not a major problem for ground-based systems and near-Earth missions, communications from deep-space missions will encounter speed-of-light communications delay and often reduced link quality. Delays due to communications paths may range from a second or less to many tens of minutes or even hours for outer planets missions. For this reason, many connection-oriented protocols used in terrestrial environments will not work in space systems without modification (for example, if a handshaking process is used during the establishment of a communication session).

What is true of all missions is the tradeoff of security overhead against the mission's ability to achieve its goal. All security mechanisms add overhead, but in bandwidth-limited space environments, overhead must be reduced to the absolute minimum required for security. A security system that uses 90% of the available communications resources or a majority of the onboard CPU cycles will be rejected by the mission planners.

Therefore a sound functional and performance analysis of the mission using the Connectivity View will allow the mission planners to consider all these factors and choose the appropriate security measures.

4.3.2 GROUND SYSTEMS

As discussed earlier, another factor which must be considered is the increased use of the Internet and other ‘open’ networks to interconnect the ground segments. In order to do this safely, all ground systems must first ensure they have sufficiently robust controls to protect themselves from the network. They may require the use of private operational circuits or of Virtual Private Networks (VPNs) to ensure secure communications between ground-based facilities, not only to protect the confidentiality and integrity of the data, but also to seek to ensure that the systems cannot be compromised by man-in-the-middle attacks.

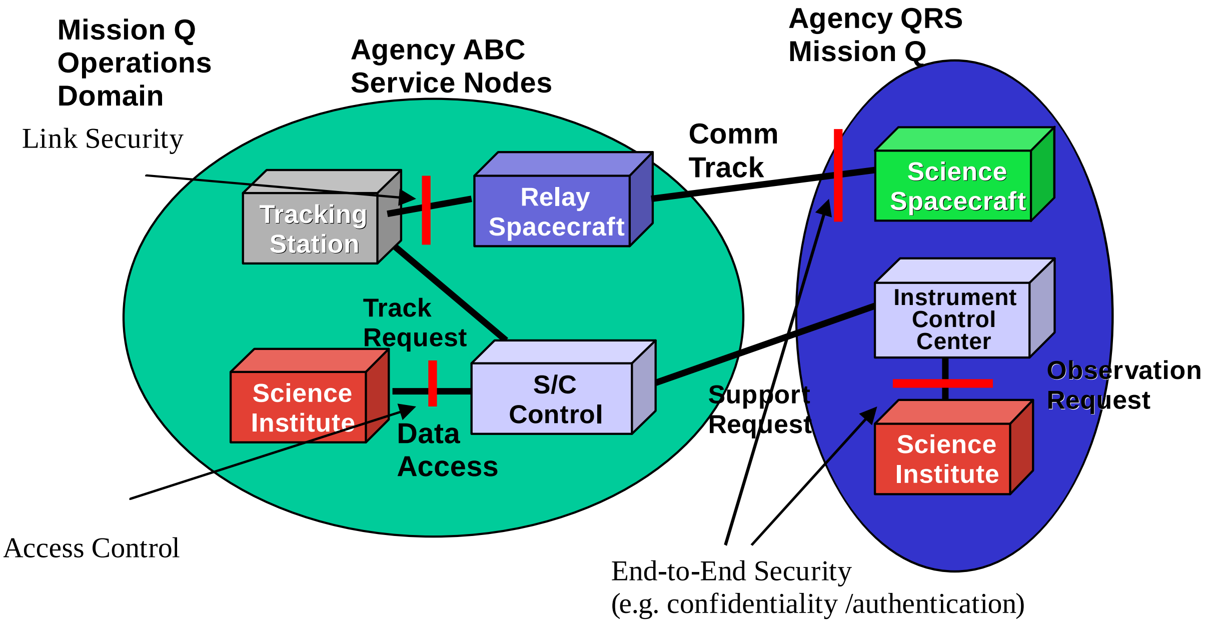


Figure 4-2: Connectivity View and Example Security Application Points

Analysis of the system from a Connectivity View allows the identification of key points within the communications network, where network tools such as gateways and border devices may be best employed.

4.3.3 PHYSICAL SECURITY

The physical security of a node is related to its environment and the protection measures needed to protect against particular threats. For example, a tracking station is likely to need guards and a fence to protect the perimeter from unauthorized personnel.

A complete treatment of physical security is outside the scope of this document. However, it is noted that some form of physical security should be applied to all ground-based systems, and this would be represented in a related Connectivity View.

4.3.4 SECURITY RISKS HIGHLIGHTED BY THE CONNECTIVITY VIEW

When considering security of the Connectivity View, all links need to be considered from the spacecraft all the way back to the mission analyst who may be based in a 3rd party research establishment. This analysis needs to consider risks relating to all intermediary nodes, and the communications links that connect them, including relay satellites, ground stations, WANs, space links, mission control, payload control, and end-user systems.

Examples of risks to consider are:

- jamming of RF signals;
- eavesdropping;
- loss of signal, both planned and unplanned; and
- use of ‘open’ networks for ground system connectivity.

4.4 SECURITY AND THE FUNCTIONAL VIEW

4.4.1 GENERAL

The Functional View, as illustrated in figure 4-3, defines the system’s capabilities. This should be the first view developed in a mission lifecycle because it is important that security is considered from the outset of a mission design. Such an approach will save money and time during the mission lifecycle.

The Functional View of the security architecture should be developed in conjunction with the mission’s overall functional architecture/design. While a functional architecture describes how different functional parts will combine to make a whole system that will meet the mission requirements, the security architecture describes how the functional parts will interact with each other and external systems so as to meet the security policy of the system. Thus as soon as the initial functional architecture takes shape, the development of the security architecture should start, as aspects of the security architecture may require the functional architecture to be changed. By doing these tradeoffs early in the design process, significant amounts of time and money could be saved.

Figure 4-3 provides an example of mission functional architecture and its allocation to physical nodes in the system. These allocations will be done to meet mission objectives and design, and may be chosen as a result of design tradeoffs. Aspects such as the use of unmanned components (e.g., ground sensor stations) or links with external entities (e.g., generating commands in a science institute in the example below) will require special consideration in the security design of the systems, including how access control is to be managed and how shared resources on the spacecraft are to be managed.

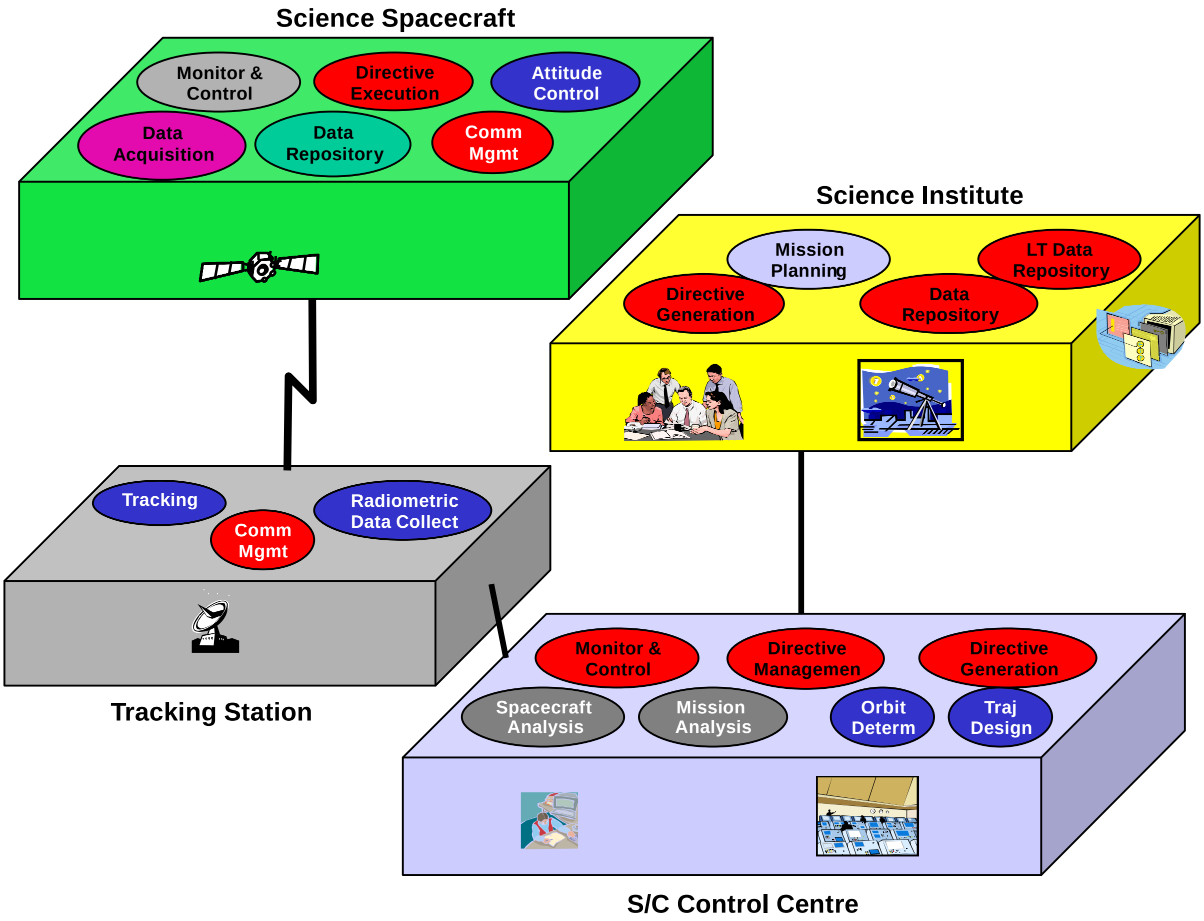


Figure 4-3: Example Analysis of the Functional View (Functions with Specific Security Requirements Shown in Red)

4.4.2 SECURITY RISKS HIGHLIGHTED BY THE FUNCTIONAL VIEW

The Functional View of any space system allows mission planners to consider how the different elements of a system and the different data flows between elements will occur. As discussed earlier, the security architecture should be developed in parallel with, and should actually shape, the Functional View of the system.

It is within the Functional View that issues such as classifying information and grouping it into domains of similar protective marking may arise.

The security Functional View will account for security controls such as connections to access control and key management functions and logical security boundaries. Some concerns, such as physical boundaries and locations of firewalls, will also be represented in a Connectivity View.

4.5 SECURITY AND THE INFORMATION VIEW

4.5.1 GENERAL

Information security controls how the data within the system is protected. This affects how data is stored and transmitted between functional elements of a system. This view, as illustrated in figure 4-4, maps onto the INFOSEC security view.

Important issues to consider are remote commanding of spacecraft and data privacy issues. The INFOSEC design must consider how a spacecraft (or a ground-based facility) can authenticate a command to ensure it comes from an approved source. It must also address how the confidentiality of personal or proprietary data is to be managed.

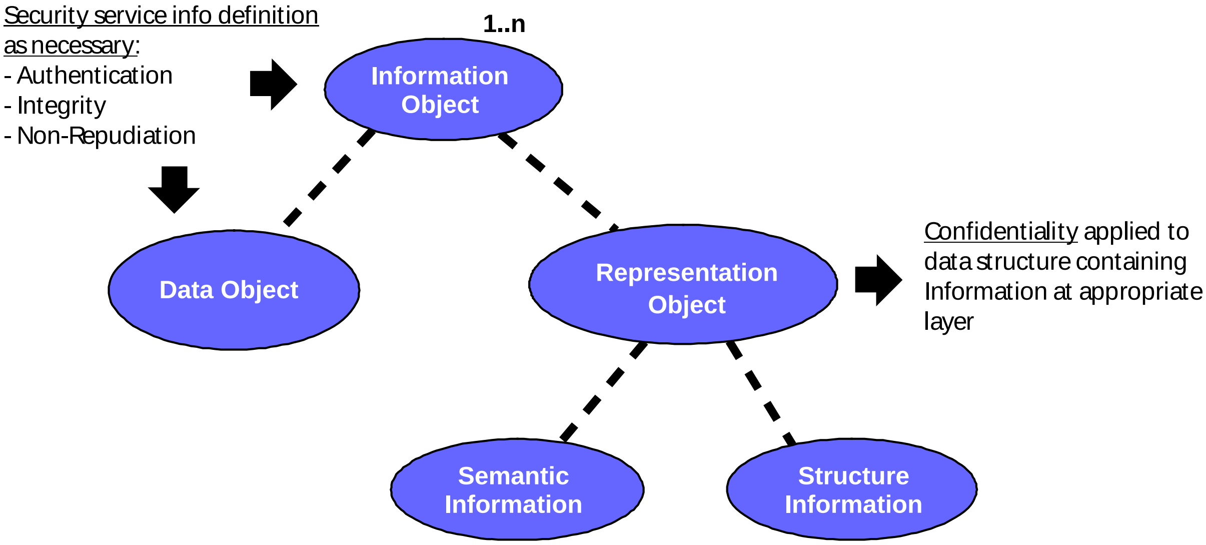


Figure 4-4: Information View and Security Implications

4.5.2 RISKS HIGHLIGHTED BY THE INFORMATION VIEW

4.5.2.1 General

The risks that become apparent from considering a system from the Information View relate to the following security services:

- authentication;
- confidentiality;
- integrity;
- availability;
- non-repudiation.

4.5.2.2 Authentication

Authentication is important to avoid spoofing of communications (including unauthorized commanding). As availability of space communications capabilities and the technology to transmit appropriate signals into space becomes more widespread, authentication becomes critical to block unauthorized users from sending commands to critical space assets. Ground-based systems must also have strong authentication systems to prevent unauthorized access or commanding which could result in mission loss.

4.5.2.3 Confidentiality

Confidentiality is required to prevent information exposure which could result in unauthorized disclosure of personal, sensitive, or proprietary information. In military, dual-use and/or highly sensitive systems, data might be classified using governmental protective markings (e.g., RESTRICTED, CONFIDENTIAL, SECRET, etc.).

4.5.2.4 Integrity

Integrity is important for telemetry and telecommands. For example, if the spacecraft receives a corrupted command, the spacecraft could be damaged and the ground station could lose control.

4.5.2.5 Availability

Ground systems need to be contactable when a space asset wishes to communicate, so availability for those systems is crucial. Any trusted third parties being used need to be contactable for communication exchanges. The systems themselves also need to ensure the availability of the data itself.

4.5.2.6 Non-Repudiation

Non-Repudiation provides accountability regarding who or what operations were performed. It is highly desirable to be able to determine, after-the-fact, who requested any specific activity during abnormal operations.

4.6 SECURITY AND THE COMMUNICATIONS VIEW

The Communications View, as shown in figure 4-5, describes the layered protocols that support communications among the network nodes in the system. From a security point of view, this View helps describe how the different communications security mechanisms fit into the overall communications-stack architecture.

A security analysis using the Communications View will consider how elements communicate with one another. This analysis will help mission planners decide which parts of the CCSDS Security Architecture, as described later in this document, to use for their mission and which layers of the security stack they wish to employ.

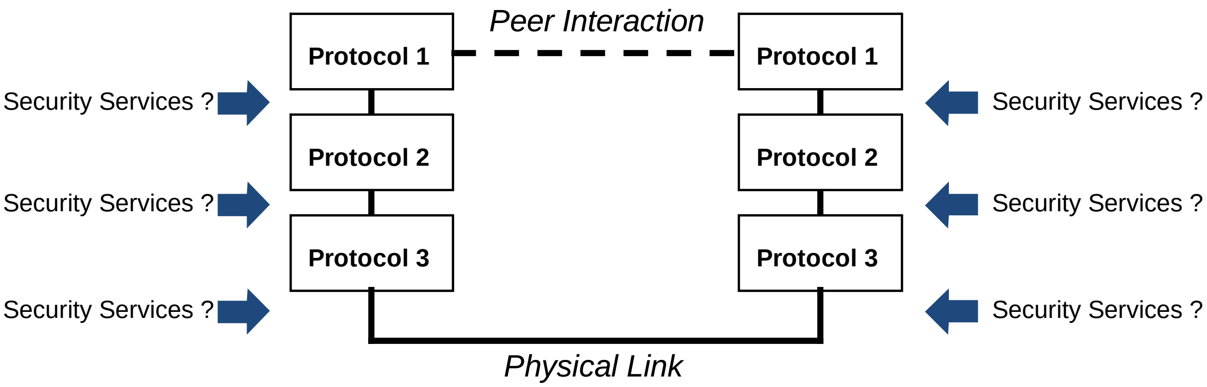


Figure 4-5: Communications View and Security Layer Choices

Depending upon the security requirements of a mission, communications link security may be applied at one or more levels. Application data may be secured via encryption, leaving all of the rest of the communications stack to operate in the clear. Alternatively, encryption may be applied at the Network Layer (see references [B1] and [B2]), where it will effectively encrypt any traffic that flows end to end between user and target application, or it may be encrypted across a single space or ground link if that is adequate for the mission requirements and physical deployment. In these cases network and link parameters are transmitted in the clear and only the contents of the transmission are protected. In some mission configurations even higher levels of security are required, including protection of all routing information to prevent traffic analysis, and in these cases Physical Layer encryption may be applied.

5 SECURITY ARCHITECTURE PRINCIPLES

5.1 OVERVIEW

The following paragraphs describe the key principles of the CCSDS Security Reference Architecture.

5.2 OPEN STANDARDS

As with all CCSDS Recommended Standards and Practices, all technologies required by the security architecture should be easily available and the licensing reasonable and nondiscriminatory. This does not exclude the use of proprietary technologies; however, for a system to be compatible with any other CCSDS-compatible system, the technologies used must be freely available (unencumbered) to all, or available via nonrestrictive, nondiscriminatory, reasonable-cost licenses.

5.3 PROTECTION THROUGH LAYERED SECURITY MECHANISMS

The use of multiple layers of security increases the overall security of the system since the failure of any one security layer will not put the system at risk of compromise.

5.4 EXPANDABILITY

The architecture should be expandable and evolvable to allow the use of new security technologies, in order, for example, to address new threats or mission requirements. It is desirable to allow already deployed systems to be remotely upgradeable, including, where possible, spacecraft.

5.5 FLEXIBILITY

The architecture should allow for development of different security systems to be developed that will be suitable for the majority of space missions. The use of the security architecture can allow missions to be in-situ configurable so as to be compatible with each other. This would allow the use of other missions as intermediate nodes and for links to be reconfigured as necessary without compromising security.

5.6 INTEROPERABILITY

The architecture should allow elements developed by one organization to interoperate with elements developed by another organization. Adoption of the baselined standard security services, and application of them in standardized ways at identified points in a mission architecture, will ensure that this interoperability is possible while still ensuring secure operations. Missions may choose to adopt alternate standards and deployments, but would do so at the risk of not being interoperable with elements built to the standards.

5.7 KEY MANAGEMENT

Key management, while an important part of the security architecture, is a significant area of design in its own right. Every system that uses a cryptographic function uses some form of keys so that one party may encrypt the data before transmission and have confidence that the intended recipient will be able to decrypt the data. Likewise, every system that uses an authentication function uses some form of key so that one party may authenticate the data before transmission and have confidence that the intended recipient will be able to verify the authenticity of the data.

The mission of the key management system is to ensure that cryptographic keying material is made available in such a way that only the intended recipients will receive it and be able to use it.

Reference [B5] contains detailed recommendations on Key Management.

5.8 ENCRYPTION ALGORITHM SELECTION

The CCSDS recommended algorithms and their configurations are discussed in reference [B6]. These algorithms should be preferentially selected where interoperability is a strong concern for the mission.

5.9 KERCKHOFF'S PRINCIPLE

A cryptosystem should be secure even if everything about the system except the key is public knowledge.

5.10 FAULT TOLERANCE

Security mechanisms shall be capable of recovery after a failure. Recovery mechanisms should not expose vulnerabilities in the system. However, exceptional circumstances may dictate the need to degrade the security mechanism, for example to enable the recovery of a mission by entering a predefined safe state. These scenarios should be identified and assessed as part of mission recovery design.

6 MISSION PROFILES

6.1 OVERVIEW

This section of the document describes five classes of mission profiles which are used to guide the developers of security architectures and to demonstrate how security may be applied in different situations. The five mission profiles examined are:

a) human spaceflight;

b) Earth observation;

c) communications;

d) scientific;

e) navigation.

These mission profiles are not intended to be an exhaustive list. Some of the mission profiles are further refined to illustrate different orbits, so as to explore and consider the different threat environments that may be encountered. For example, in general, lower-power equipment is needed to contact a Low Earth Orbit (LEO) satellite, but there is only a brief contact window, whereas higher-power equipment is needed to contact a Geosynchronous Earth Orbit (GEO) satellite, but there is continuous contact within its footprint.

6.2 GENERAL

Security mechanisms should take into account constraints, such as minimum bandwidth situations, and must be able to operate without compromising continuity of service. There may be overlaps between profiles.

6.3 HUMAN SPACEFLIGHT

Human spaceflight missions present a special case, as they not only have all the usual security issues, but also ‘safety-of-life’ and personal privacy issues. This means that the security architecture must be robust and reliable in order to not compromise the safety-of-life requirements. The architecture also needs to be scalable to ensure that, as the available bandwidth of links increases, the security infrastructure can scale to keep up. Human spaceflight missions require highly reliable communications, require low jitter voice communications, and often include high data rate video communications. The availability, confidentiality, and integrity of these communications and of personal data is a strong requirement.

6.4 EARTH OBSERVATION

Earth observation missions gather information about the physical, chemical, and biological systems of the planet and are used to monitor status of and changes to natural and man-made environments. Examples include weather forecasting, wildlife tracking, measurement of land use change (such as deforestation), and prediction of climate change.

Earth observation satellite systems include meteorological and other types of missions. Often the spacecraft in this mission class are critical infrastructure assets, and so may be of importance in areas such as population safety or national security.

Over the years, these missions have become a necessary and operational component of the global climate observation and prediction infrastructure. Earth observation satellites may be in LEO or GEO. These missions typically require highly secure command paths and may also include requirements for secure downlinks for certain classes of data.

6.5 COMMUNICATIONS

Communications systems are usually based on geostationary satellites that have continuous visibility of one or more ground stations, fast communications, and large amounts of bandwidth and power. The average expected lifetime is long (15-20 years) and they must be as cost-effective as possible to construct and operate.

In addition, constellations of communications satellites in LEO with satellite cross links have been deployed. The LEO constellations reduce the communications latency experienced with GEO satellites while still providing extensive Earth coverage previously only available from GEOs. However, the potentially reduced threat to LEO satellites, because of their brief visibility, no longer holds true because of the on-orbit routed network created by the satellite constellation. While a single LEO satellite is still only visible for a short amount of time, each satellite in the constellation acts as a relay to its neighbor spacecraft, which means that the threats against the entire constellation are increased.

Protections being utilized by this profile should consider the satellite telecommand and telemetry channels, as well as the payload links. There may be no mandated security for the communication payload channels; however, this document provides a recommended security suite for such channels when one is required. This leaves as much flexibility as possible for the commercial sector while supplying guidance where it is needed.

6.6 SCIENTIFIC

6.6.1 NEAR EARTH ORBIT

Near-Earth orbit systems have very little delay in their communications links because of their relatively low-altitude orbits. However, the links will be non-continuous as the satellite moves in and out of communications range of a ground station. The security systems must be inexpensive and computationally efficient. Protections being utilized by this profile should consider particularly the satellite telecommand channel, but may also need to consider protection for telemetry, depending upon the nature of the data.

6.6.2 LUNAR

Lunar missions have multiple threat characteristics depending on whether they are in Earth orbit before beginning their cruise phase or in their cruise phase. While in Earth orbit or near-Earth, these missions are just like the other LEO, Medium Earth Orbit (MEO), and GEO missions. Lunar missions in cruise or in the lunar environment have similar characteristics to deep space missions. Protections being utilized by this profile should consider particularly the satellite telecommand channel, but may also need to consider protection for telemetry, depending upon the nature of the data.

6.6.3 INTERPLANETARY/ DEEP SPACE

The following key drivers influence the security architecture development for interplanetary/deep-space missions:

– considerable communication delay;

– efficient security mechanisms;

– security mechanisms that must be able to cope gracefully with discontinuous communications;

– fault tolerance;

– ability to use intermediate relay nodes, both planned and unplanned;

– significant program lifetimes (e.g., as a result of period between launch and destination).

Deep space missions always start in near-Earth orbit and may also use Earth flybys in order to slingshot towards their target destinations. In these situations the security environment is similar to a LEO satellite, and so their security infrastructure design should take into account these periods when they are vulnerable. For the deep space portions of the mission the vulnerability to attack is lower, largely because of the size, cost, and complexity of the ground communications assets required for sending signals to these distant spacecraft. Protections being utilized by this profile should primarily consider the satellite telecommand channel, but may also need to consider protection for telemetry, depending upon the nature of the data.

6.7 NAVIGATION

Navigation satellite systems such as the US Global Positioning System (GPS) and the European Galileo system are critical infrastructure providing services for users such as airline, trucking, maritime, and military. The services provided by navigation satellite systems are used by aircraft, ships, automobile navigation systems, cellular telephones for emergency locating, and hand-held units for a wide range of leisure applications. Similar to communications satellites, the loss of navigation satellite systems could result in not only loss of financial investment, but also loss of life.

Navigation satellites are usually deployed in MEO. However, some systems are proposed with highly elliptical orbits. These missions typically require highly secure command paths and may also include requirements for secure spacecraft telemetry downlinks. These satellites usually transmit broadcast or downlink data in the clear, although some downlink data may also be encrypted.

6.8 MULTI-ORGANIZATIONAL SPACECRAFT

Multi-organizational spacecraft is not really a separate mission profile, but more a special class of one or more of the above mission profiles.

Within multi-organizational space missions, payloads (and their data) may belong to different agencies, organizations, and countries. For example, a commercial mission may have a spacecraft bus owned and operated by one company that provides payload space to other companies or to government agencies for a fee. Science missions flown by one agency will frequently carry instruments developed and operated by a second agency. Relay spacecraft may carry communication payloads developed by a second agency and provide communications services to other, separate agencies.

The main security constraint affecting these missions will be whether the security architecture must allow different security domains to exist within the satellite itself, while still allowing as much common equipment to be used as possible (communications, data storage, etc.). Command and essential telemetry streams may have to be combined into one communications channel, but still segregated so that instrument commands cannot affect critical host spacecraft operations. Within relay spacecraft it may become necessary to segregate data streams from different sources so that privacy and data integrity are maintained.

7 PROPOSED ARCHITECTURE

7.1 REQUIREMENTS

Using the mission profiles and principles discussed in previous sections, a series of requirements for the CCSDS security architecture is derived:

- The architecture should be able to support security in depth and the layering of different security mechanisms.
- Systems resulting from the application of the security architecture should be modular.
- The systems implemented employing the security architecture should be upgradeable during the mission lifetime.
- The security architecture must support non-continuous and long-delay communications links.
- The security architecture must be interoperable with other compliant missions, possibly developed by different organizations.
- The security architecture must support emergency operations.
- The security architecture must allow the use of intermediate communication nodes, both planned and unplanned.
- The security architecture must support mixed security domains onboard a spacecraft or in a ground facility.
- The security architecture must support the use of common infrastructure.
- The security architecture must be robust and scalable.
- The security architecture must be able to be extended across ground systems.

7.2 SERVICES

The security services that should be considered for any given system include:

- data confidentiality in transit;
- data integrity;
- authentication;
- authorization / access control;
- non-repudiation.

Supporting security mechanisms to be considered include:

- key management;

– cryptographic mechanisms (e.g., encryption, HMAC / Hashes).

Considerations on the implementation of security mechanisms include:

– support for emergency operations;

– end-to-end security;

– maintenance of security when routing / relaying data;

– maintenance of security when converting protocols;

– defense against denial-of-service attacks (e.g., anti-jamming, defense against RF power attacks, anti-replay mechanisms).

NOTE – The term ‘denial of service’ can be applied to a wide variety of threat types. Examples include the exploitation of weaknesses in data protocol implementation, communication devices, and RF-specific attacks. For each of these groups, mitigations will also vary widely (e.g., robustness against cyber attack like repeated connection attempts, protocol design, frequency hopping, and spread spectrum).

Reference [B2] contains further discussion regarding security services and mechanisms.

7.3 PROPOSED SECURITY ARCHITECTURE

The CCSDS Security Architecture is based on a functional central core which can be tailored or expanded to meet specific mission needs. This security architecture considers the space and ground systems as two separate segments.

Ground-based systems are encouraged to use state-of-the-art terrestrial security technology to establish secure communications suitable for the missions. These might include technologies such as Internet Protocol security (IPsec), Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Secure Shell (SSH), public key encryption, and digital signatures.

The space segment defines a basic security suite in a layered fashion. This suite is known as the *CCSDS Security Core Suite*.

The use of the CCSDS Security Core Suite is recommended when developing a CCSDS-compliant security architecture. The basic suite should not limit the security mechanisms implemented on a mission. For example, additional mission or agency security mechanisms can be applied if required or desired.

7.4 CCSDS SECURITY CORE SUITE

7.4.1 AIMS OF THE SECURITY CORE SUITE

The aims of the CCSDS Security Core Suite are

– to allow security mechanisms to be applied to individual layers within a communications stack, irrespective of adjacent layer requirements, without restricting the use of other mission-specific security mechanisms that may be required on any layer;

– to define explicitly where encryption may be applied to different levels of layers of the communication stack, and state possible reasons for this from a mission perspective;

– to complement other CCSDS documentation such as *The Application of CCSDS Protocols to Secure Systems* (reference [B2]), which discusses overall security requirements for the communication stack, and *CCSDS Cryptographic Algorithms* (reference [B6]), which recommends appropriate algorithms for use with space-links.

7.4.2 SECURITY CORE SUITE DEFINITION

The key security implementation layers as described in reference [B2] and represented graphically in figure 7-1 are the Application, Network, (Data) Link, and Physical Layers.

The CCSDS Security Core Suite is primarily based on Data Link Layer, Network Layer, and Application Layer security mechanisms**;** (Physical Layer security lies outside of the Suite definition). This framework is intended to complement reference [B2] in which security mechanisms such as encryption, authentication, and access control are discussed, as well as any other mission-specific security mechanisms.

Security services can be applied to each layer in line with mission requirements irrespective of adjacent layer requirements. Choice of service type should be in line with the supporting CCSDS documentation listed in annex B, references [B1], [B2], and [B6]. A key principle is that the suite’s security services described for each layer can be applied or removed as needed. For specific missions, a solution based solely on Data Link Layer security can be envisaged.

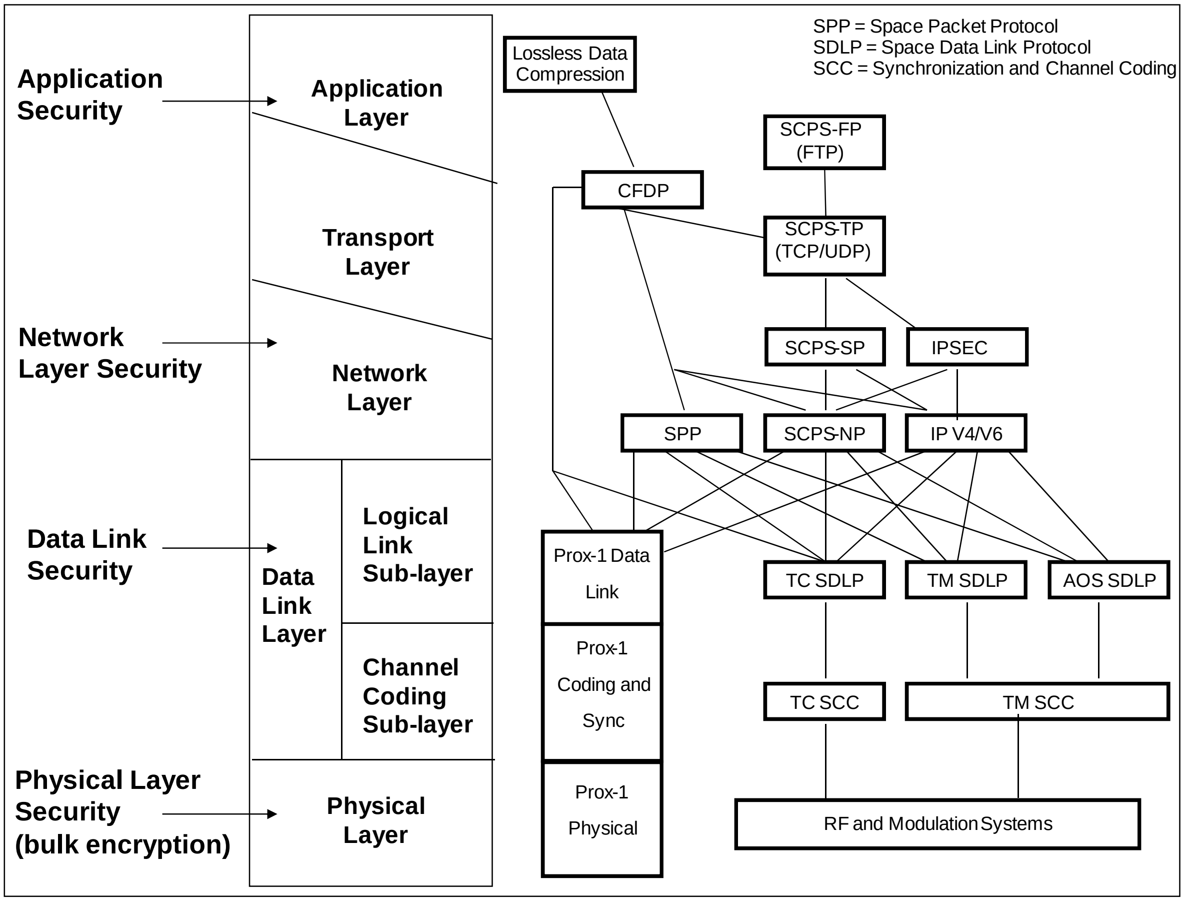


Figure 7-1: CCSDS Space Mission Protocols and Security Options[1]

[1] Source: reference [B2].

The different operational combinations of the CCSDS Security Core Suite are:

Physical	Link	Network	Application	Comment
Not defined within Core Suite	0	0	0	Core suite services not used; this is envisaged for situations where: – a mission-specific encryption suite is being used (for example at the Physical Layer); – a mission requires these services to be disabled; – there is no need for the services (e.g., some deep space missions).
	1	0	0	Link-only; very efficient for cases such as point-to-point encryption.
	0	1	0	Network-only services, suitable for routing within the same network protocol.
	0	0	1	Application-only services, suitable when end-to-end security is needed or there is a need for a change in network protocols during transmission.
	1 (Link or Network services, possibly both)		1	Both Application- and lower-layer (Data Link or Network) services are being used; in the case of encryption, this would occur when a payload control center is communicating securely to a payload, using a secure communications channel the mission control center has established using lower-layer encryption.

NOTE – This framework does not address specific protocols; this is because the choice and implementation of protocols constrains the security mechanisms and services.

7.5 SECURITY CORE SUITE CONFIGURATION

7.5.1 GENERAL

The Security Core Suite is illustrated in figure 7-2. As has already been discussed, the security profile of the spacecraft should be flexible so it can be changed during the mission if the threat profile changes.

For example, for a Mars mission during the Earth-orbit phase after launch and during shakedown tests there will be a specific threat profile. During the cruise and on-station phases the threat profile will change. Thus employing an adaptable security architecture provides communications efficiency benefits when the threat has reduced or changed.

Upper layer (e.g., Network and Application Layer) security services provide end-to-end security services. At the Application Layer, the services are provided between peer applications in the end nodes and may be implemented using encryption functions of some form. At the Network Layer, the services are provided between end-systems and might be implemented using security gateways or, potentially, by capabilities implemented within the end-system upon which operational applications are running. At the Data Link Layer, security services can be used to provide security on a hop-by-hop/link-by-link basis and implemented within the communications equipment or sub-systems.

The following paragraphs examine each of the Security Core Suite's layers.

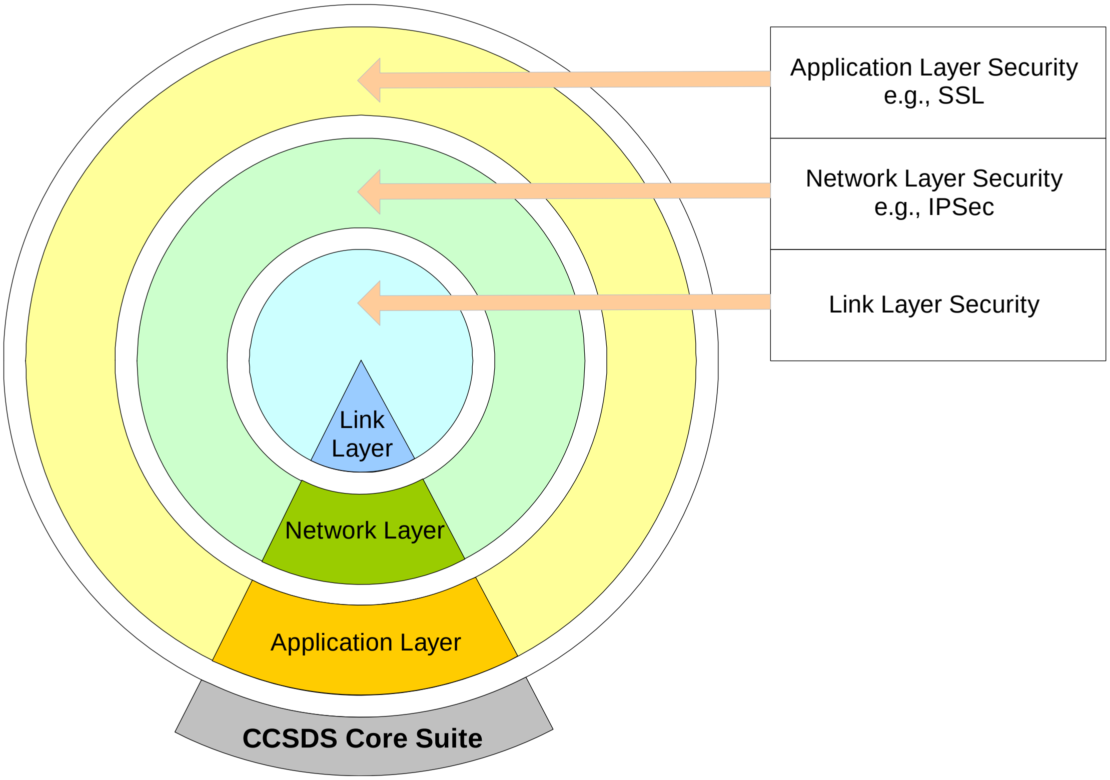


Figure 7-2: CCSDS Security Core Suite

7.5.2 DATA LINK LAYER

Data Link Layer security may be used to compliment or replace upper-layer security for certain missions. Even if a mission elects to use upper-layer, end-to-end, security mechanisms, it may choose to compliment those services with Data Link Layer security to provide additional protection.

Because Data Link Layer security services exist low in the OSI stack, less of the packet or frame is exposed to potential eavesdroppers. For example, while Network Layer encryption provides protection between the two communicating end-systems, all of the protocol machinery below the Network Layer including the Network Layer protocol (e.g., IP or BP, Data Link, Physical) is exposed. Data Link Layer services can provide additional protection, making all of the upper-layer protocols opaque. Therefore, Data Link Layer security may be useful when a threat assessment indicates a heightened risk of exposure of the underlying protocols across an RF link or when traffic analysis is a concern.

Data Link Layer services may also be used as the sole means of providing security if only a specific link, or a small number of links, require security services, such as when a mission has only one ground station and one spacecraft with point-to-point communications. Data Link Layer security services may be able to provide all of the mission's security needs, which could include authentication, integrity, and confidentiality, but only on the specific link over which the security services are provided. For an RF link, the data is afforded security only over the specific link and not any further. Therefore the data would not be protected between the ground station and mission control unless additional security services are provided.

For Data Link Layer security, there are various options for what portion of the frame is encrypted. Two common varieties are encryption of the entire frame or selective encryption of the frame data field. By encrypting the entire frame, data flowing across the link is protected, but the data cannot be routed or otherwise discriminated until it is decrypted. By encrypting the frame data field selectively, routing data is visible without decryption. (For further information, see reference [B2].)

7.5.3 NETWORK LAYER SECURITY

Network Layer security may be used in a configuration where end-to-end data security is required across a routed network. This allows routing data to be transmitted in the clear, while protecting all the data in the Transport/Application Layers. The disadvantage of this approach is that it obscures transport-level routing information that may be used in intelligent routing services. An example of Network Layer security is IPSec.

7.5.4 APPLICATION LAYER ENCRYPTION

In situations requiring end-to-end security that cannot be fulfilled by Network Layer security, Application Layer encryption can be used. As an example, a mission might not use a network stack and instead run applications directly on top of Data Link Layer services such as TC/TM.

Examples of Application Layer security mechanisms are Secure/Multi-purpose Internet Mail Extensions (S/MIME) or Transport Layer Security (TLS), both of which have available many implementation libraries which can be incorporated into an application.

7.5.5 PAYLOAD SPECIFIC SECURITY

The security architecture permits the use of security mechanisms other than those specified by the CCSDS Security Core Suite. In these situations, the use of Network and Application Layer-specific encryption for space links may be judged an unnecessary addition to payload specific-communications and not used.

For example, this flexibility may be useful in missions where communication links are sporadic and brief, have a long delay, or when the payload is used as an intermediate node in a store-and-forward mode. In these cases data encryption could be performed prior to establishment of communications; once they are available the encrypted data block can be passed to the first node. Should communications then be lost, the data can still travel to its final destination securely at a later time.

7.6 EXPANDABILITY

As has been stated, the security architecture is designed to be expandable to fit specific mission needs or to comply with Agency guidelines. So while it is intended that the CCSDS Security Core Suite should always be implemented, there is no reason other security mechanisms, either individually or as complete stacks, could not be used.

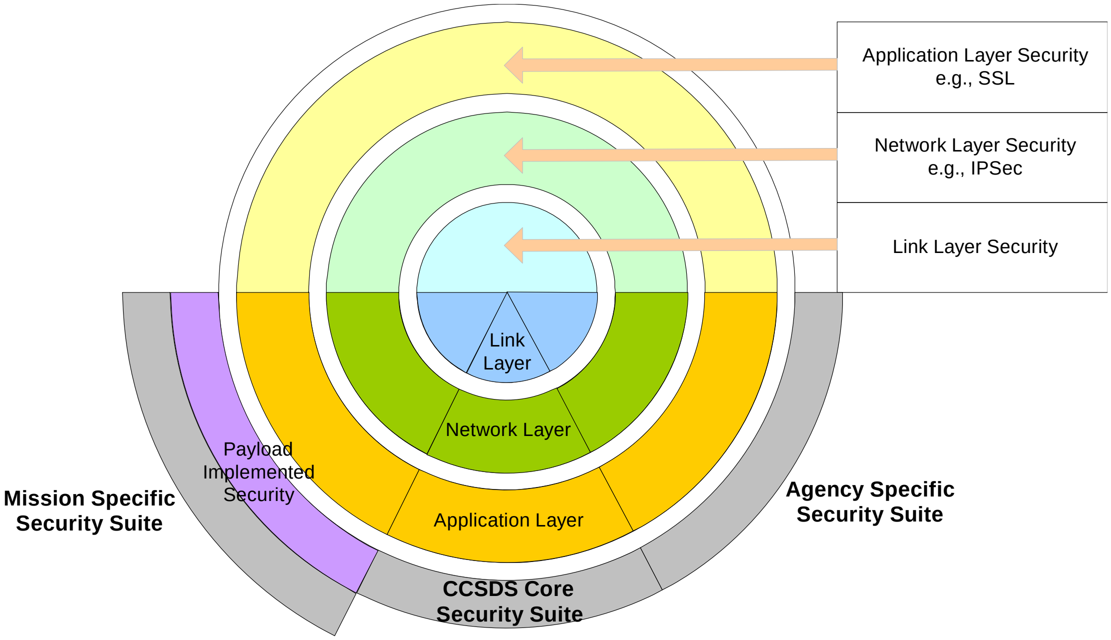

Application Layer Security
e.g., SSL
Network Layer Security
e.g., IPSec
Link Layer Security
Link Layer
Network Layer
Application Layer
Payload Implemented Security
Mission Specific Security Suite
CCSDS Core Security Suite
Agency Specific Security Suite

Figure 7-3: Example Security Architecture for 'Mission 1'

Figure 7-3 presents a fictitious ‘Mission 1’ that has a requirement to include special security needs. The CCSDS Security Core suite has been implemented, but it has also implemented two other security suites, one mandated by the mission agency and one specific to the mission.

‘Mission 1’ decided to extend its specific mission security suite with additional Data Link Layer and payload security mechanisms. Both of these are perfectly allowable and compatible within the CCSDS Security Architecture.

While it can be seen that ‘Mission 1’ is purely fictitious, it demonstrates how the CCSDS Security Architecture allows for such flexibility.

While figure 7-3 presents a complex security architecture, a mission could choose to use just one mechanism, as illustrated in figure 7-4.

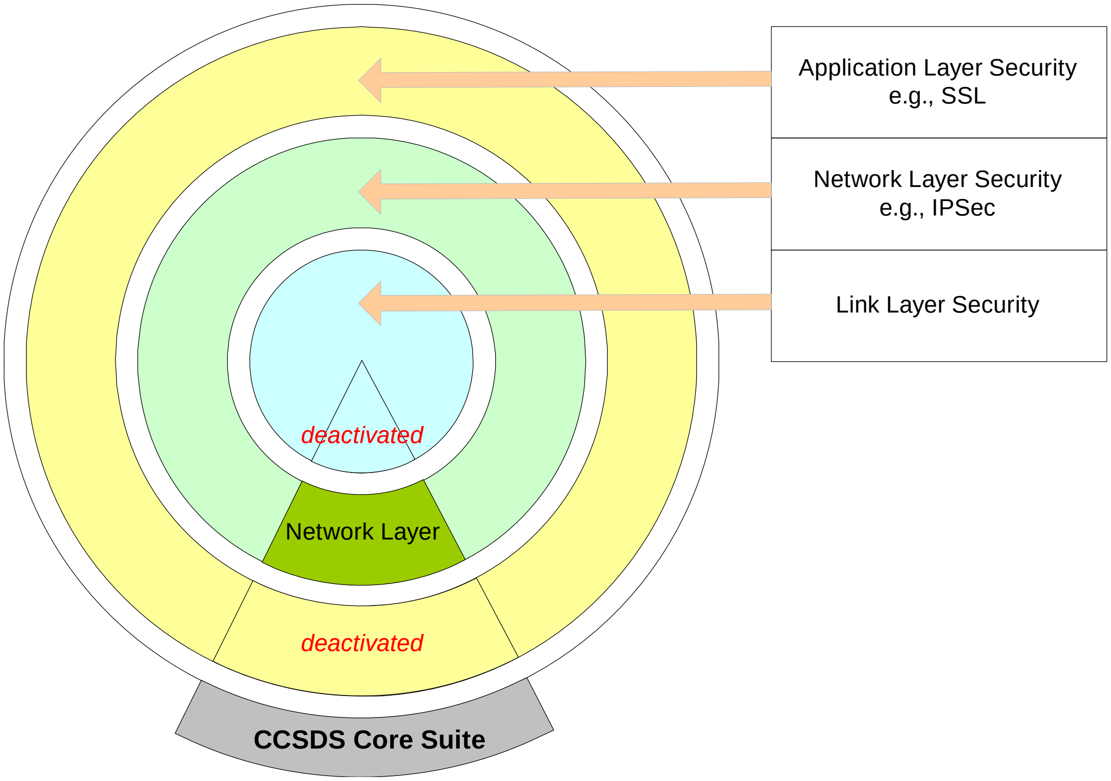
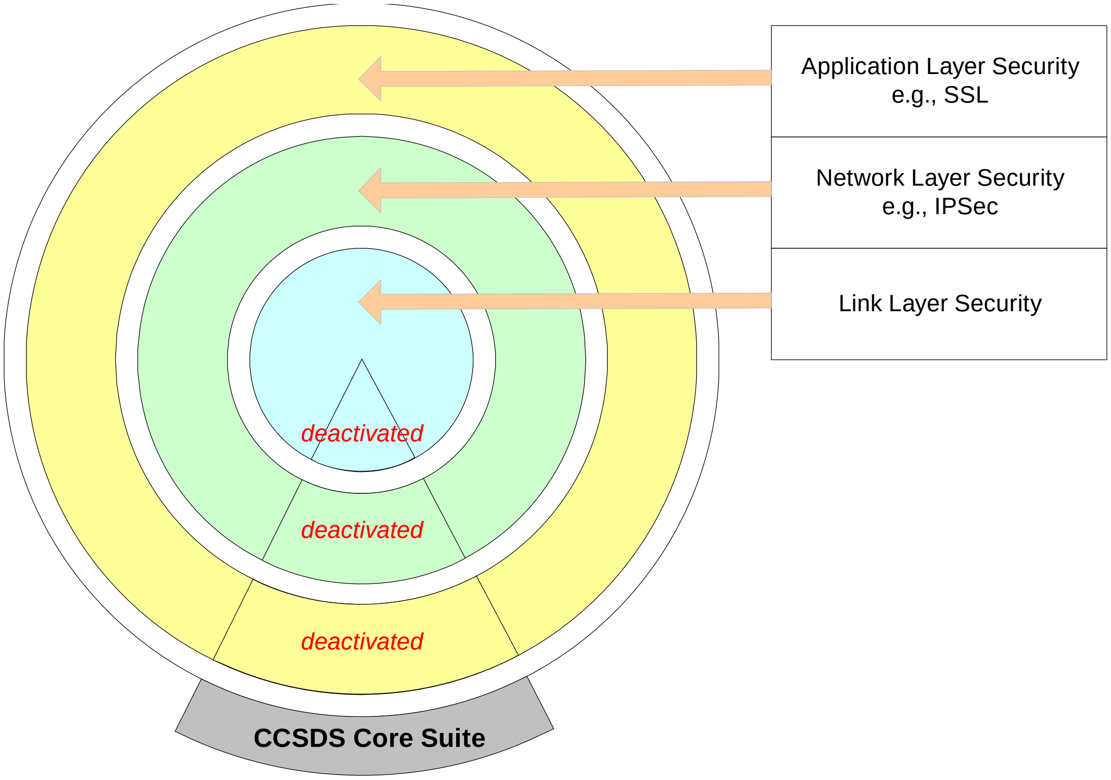


Figure 7-4: Security Architecture for a Simple Mission, Which Uses Only the Network Layer Security Subsystem from the Core Suite

However, if a mission’s needs are not served by the Core Suite and alternative security services/mechanisms are used, then the layered approach described by the Core Suite scheme should still be implemented. In this scenario, the security mechanisms described in reference [B2] would not be used, and compatibility needs are satisfied (see figure 7-5, below).



NOTE – Core Suite is still present but deactivated.

Figure 7-5: A Simple Mission Using Its Own Transport Layer Security

7.7 EMERGENCY OPERATIONS

The requirements for emergency commanding may conflict with the requirements for security. On the one hand, emergency commands need to be as short as possible in order to maximize their chance of being received by a tumbling spacecraft. On the other hand, operators do not want emergency commands to be accidentally invoked if the specified bit pattern just happens to occur within a normal data stream or if the system is under attack.

A spacecraft may be in one of two states that require emergency commanding:

– the spacecraft is in trouble and has gone into safe mode; or

– the spacecraft is in trouble but has not detected this and is not in safe mode.

Add to these two scenarios the added complication that the spacecraft's central information processing subsystem may or may not be operational.

Because of the possibility of the central information processing subsystem's being in an unknown state, emergency commands are usually implemented entirely in hardware, with no software or processor involvement. This is done in order to be able to recover even when a processor has 'crashed'.

In situations where the spacecraft has gone into a safe state and the internal command and control systems are functioning, authenticated commands can be sent. This is not truly emergency commanding, as normal operational procedures can deal with this situation.

For situations where the spacecraft may be tumbling or the main command and control system has failed, either an alternate form of authentication, which reduces the size of the authenticated commands, can be used, such as use of an emergency back-up key or keys (although there is the risk of the same keys' being used more than once), or non-authenticated commands can be sent. It should be noted that for some high-integrity systems, it might be preferable to lose the system than to have it compromised.

In situations where there is sufficient communications bandwidth even when the spacecraft is tumbling, for example, a LEO satellite with an omni-antenna, there might be a reason to use non-authenticated commands. This might be the case if the onboard system, based on a predesigned set of conditions, like a timer expiry in the absence of received commands, decides itself to turn into clear mode to favor communications acquisition and command recovery.

The preferred series of events in emergency situations would be a controlled degradation from full authentication, to reduced authentication, and finally to non-authenticated commands. At no point during normal operations should non-authenticated emergency commands be acted upon.

In order to perform this function, it is suggested that an Emergency Detection System (EDS) be used. This system would be implemented separately from the main data handling system and be as simple and robust as possible. It would encompass a state machine that would monitor events onboard the spacecraft, such as CPU keep-alive, internal temperatures, receiver status, and communications from the ground. It would use the monitored events to determine the health of the spacecraft. If it detects an abnormal situation it could activate an emergency mode. For example, should the keep-alive signal from the CPU stop, the EDS would allow non-authenticated, hard-wired, sequenced commands to be entered into the command decoder and acted upon.

The mission planners must make the final choice regarding how to deal with emergency situations. They must take into account the security threat analysis for their specific mission. However, they should consider how the threat to their mission changes over time in dealing with emergency situations.

References [B2], [B5], and [B7] contain more information regarding security threats to space missions, key management, and possible use of security mechanisms.

ANNEX A

SECURITY CONSIDERATIONS

(INFORMATIVE)

A1 INTRODUCTION

All normative CCSDS documents are required to include a security section to ensure that all security aspects are fully considered. The requirement applies to normative CCSDS security documents as well. This annex addresses that requirement.

This document describes the Security Reference Architecture for CCSDS that applies to both space and ground systems. The entire document is concerned with security issues surrounding the design, development, and operation of space missions. It discusses the steps necessary to understand what security is needed for a mission and how to design the security aspects in consonance with the functional architecture.

A2 SECURITY ASPECTS

A2.1 DATA CONFIDENTIALITY

This document describes data confidentiality, where it may be required in the mission system architecture, and how it can be accomplished by the use of encryption technology.

A2.2 DATA INTEGRITY

This document describes the need for data integrity to ensure that telecommands are correct and have not been modified without authorization while in transit. This document also describes the need for data integrity to ensure that data received on the ground from a spacecraft is exactly what the spacecraft sent, such that if housekeeping data is received, the ground controllers will not issue commands based on erroneous data.

A2.3 AUTHENTICATION OF COMMUNICATING ENTITIES

This document describes the need for only authenticated entities to have the ability to issue commands to the spacecraft. In addition, it describes the need for spacecraft to act only upon authenticated commands and to ignore all others.

A2.4 CONTROL OF ACCESS TO RESOURCES

This document describes the need for a mission architecture to only allow access to resources based on entity identity and authorizations.

A2.5 AVAILABILITY OF RESOURCES

This document describes the requirement for mission-critical systems such as ground systems to be available at all times to carry out the mission and to ensure that there is no loss of data, or, in the case of human spaceflight missions, loss of life.

A2.6 AUDITING OF RESOURCE USAGE

This document does not need to describe where auditing is necessary.

A3 POTENTIAL THREATS AND ATTACK SCENARIOS

As described throughout this document, different mission classes have varying threat and attack scenarios. Near-Earth missions require less transmission power than deep-space missions and therefore might be more easily attacked. LEO missions have less visibility on the ground than do GEO missions. But LEO missions require less power and smaller antennas than do GEO missions. The document guides the user through the risk and vulnerabilities in order to derive a Mission Security Architecture.

A4 CONSEQUENCES OF NOT APPLYING SECURITY TO THE TECHNOLOGY

This document provides the user with the ability to design a Mission Security Architecture. Agency and national policies require mission security. Missions flying without any security services or mechanisms may be lost or destroyed.

ANNEX B

INFORMATIVE REFERENCES

(INFORMATIVE)

[B1] *Reference Architecture for Space Data Systems*. Recommendation for Space Data System Practices, CCSDS 311.0-M-1. Magenta Book. Issue 1. Washington, D.C.: CCSDS, September 2008.

[B2] *The Application of CCSDS Protocols to Secure Systems*. Report Concerning Space Data System Standards, CCSDS 350.0-G-2. Green Book. Issue 2. Washington, D.C.: CCSDS, January 2006.

[B3] T. Dierks and E. Rescorla. *The Transport Layer Security (TLS) Protocol*. RFC 5246. Version 1.2. Reston, Virginia: ISOC, August 2008.

[B4] S. Blake-Wilson, et al. *Transport Layer Security (TLS) Extensions*. RFC 3546. Reston, Virginia: ISOC, June 2003.

[B5] *Space Missions Key Management Concept*. Report Concerning Space Data System Standards, CCSDS 350.6-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS.

[B6] *CCSDS Cryptographic Algorithms*. Recommendation for Space Data System Standards, CCSDS 352.0-B-0. Blue Book. Issue 0. Washington, D.C.: CCSDS, forthcoming.

[B7] *Security Threats against Space Missions*. Report Concerning Space Data System Standards, CCSDS 350.1-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, October 2006.

[B8] *CCSDS Guide for Secure System Interconnection*. Report Concerning Space Data System Standards, CCSDS 350.4-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, November 2007.

[B9] *Information Security Glossary of Terms*. Draft Report Concerning Space Data System Standards, CCSDS 350.8-G-0. Draft Green Book. Issue 0. Washington, D.C.: CCSDS, forthcoming.

ANNEX C

ABBREVIATIONS AND ACRONYMS

(INFORMATIVE)

Term	Meaning
BP	Bundle Protocol
EDS	Emergency Detection System
GEO	Geosynchronous Earth Orbit
GPS	Global Positioning System
HMAC	Hash-based Message Authentication Code
INFOSEC	Information Security
IP	Internet Protocol
IPsec	Internet Protocol Security
LEO	Low Earth Orbit
MAC	Message Authentication Code
MEO	Medium Earth Orbit
MoA	Memorandum of Agreement
MoU	Memorandum of Understanding
OSI	Open Systems Interconnection
RASDS	Reference Architecture for Space Data Systems
RF	Radio Frequency
SASDS	Security Reference Architecture for Space Data Systems
SECOPS	Security Operating Procedures
SSH	Secure Shell
SSL	Secure Sockets Layer
SSP	System Security Procedure
TLS	Transport Layer Security
TRANSEC	transmission security
TT&C	Telemetry, Tracking, and Control
VPN	Virtual Private Network