The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

SECURITY THREATS AGAINST SPACE MISSIONS

INFORMATIONAL REPORT

CCSDS 350.1-G-1

GREEN BOOK

October 2006

AUTHORITY

Issue:	Green Book, Issue 1
Date:	October 2006
Location:	Not Applicable

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 describes the threats that could potentially be applied against space missions. It characterizes threats against various types of missions and examines their likelihood and the results of their having been carried out.

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This document is therefore subject to CCSDS document management and change control procedures which are defined in the *Procedures Manual for the Consultative Committee for Space Data Systems*. 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.

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 Organization (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	Date	Status
CCSDS 350.1-G-1	Security Threats against Space Missions, Informational Report, Issue 1	October 2006	Current issue

CONTENTS

Section Page

Figure

CONTENTS (continued)

1 INTRODUCTION

1.1 PURPOSE

This document provides an overview of potential threats against various categories of civilian space missions and provides illustrative security threat data for mission planners.

1.2 SCOPE

In the past, space missions using CCSDS Recommended Standards were typically thought of as '*civil*' and '*scientific*' missions that were unlikely targets of malicious attackers, unlike military missions that would be targeted and have traditionally been highly protected. However this view is now changing. This document provides an overview of potential threats for several classes of missions; this overview may be useful for mission planners.

1.3 APPLICABILITY

This document is applicable to mission planners for all space missions. It provides background data and threat information so that mission planners can be better prepared to understand the security mechanisms and/or policies necessary to counter any perceived threats against the mission.

1.4 RATIONALE

Network connectivity is constantly increasing and is becoming ubiquitous. As a result, the desire is to take advantage of the existing infrastructure to operate mission payloads across networks. This opens up many threats against missions that would not have previously existed. As a result, civil space missions must take into account a wide variety of security threats.

1.5 DOCUMENT STRUCTURE

This document is divided into 5 sections. Section 1 provides this introduction and definitions of commonly used terms. Section 2 provides an overview of the subject area. Section 3 describes the threat analysis process. Section 4 describes illustrative threats against six classes of civil space missions. Section 5 is the summary.

1.6 DEFINITIONS

Access Control: The process of granting access to the resources of a system only to authorized users, programs, processes, or other systems.

Access Control Mechanism: Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access in an automated system.

Authentication: (1) Verification of the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. (2) Verification of the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.

Authorization: The granting of access rights to a user, program, or process.

Controlled Network: A network that enforces a security policy.

Confidentiality: Assurance that information is not disclosed to unauthorized entities or processes.

Configuration Management: Process of controlling modifications to the system's hardware, firmware, software, and documentation which provides sufficient assurance the system is protected against the introduction of improper modification before, during, and after system implementation.

Data Integrity: Condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Denial of Service: Any action or series of actions that prevents any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service.

Identification: The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.

Masquerading: Attempts to gain access to a system by posing as an authorized user or as a process. This is a form of spoofing.

Residual Risk: The portion of risk that remains after security measures have been applied.

Risk: A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting adverse impact.

NOTE – Risk is the loss potential that exists as the result of threat and vulnerability pairs. It is a combination of the likelihood of an attack (from a threat source) and the likelihood that a threat occurrence will result in an adverse impact (e.g., denial of service, loss of confidentiality or integrity), and the severity of the resulting adverse impact. Reducing either the threat or the vulnerability reduces the risk.

Risk Analysis: An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events. The purpose of a risk assessment is to determine if countermeasures are adequate to reduce the probability of loss or the impact of loss to an acceptable level.

Security Policy: The set of laws, rules, and practices that regulate how information is managed, protected, and distributed.

NOTE – A security policy may be written at many different levels of abstraction. For example, a corporate security policy is the set of laws, rules, and practices within a user organization; system security policy defines the rules and practices within a specific system; and technical security policy regulates the use of hardware, software, and firmware of a system or product.

Threat: Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

Threat Agent: A method used to exploit a vulnerability in a system, operation, or facility.

Threat Analysis: The examination of all actions and events that might adversely affect a system or operation.

Threat Assessment: Formal description and evaluation of threat to a system.

Trap Door: A hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. It is activated in some innocent-appearing manner, e.g., a special ‘random’ key sequence at a terminal. Software developers often introduce trap doors in their code to enable them to reenter the system and perform certain functions. Synonymous with back door.

Trojan Horse: A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security or integrity.

Virus: A program that can ‘infect’ other programs by modifying them to include a, possibly evolved, copy of itself.

Vulnerability: Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited to violate system security policy.

Vulnerability Analysis: The systematic examination of systems in order to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.

Vulnerability Assessment: A measurement of vulnerability which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack.

1.7 REFERENCES

[1] *Glossary of INFOSEC and INFOSEC Related Terms*. Compiled by Corey D. Schou. Pocatello, Idaho: Idaho State U Simplot Decision Support Center, 1996.

[2] *Capability Maturity Model® Integration (CMMI^{SM})*. Version 1.1. CMU-SEI-2002-TR-011. ESC-TR-2002-011. Pittsburgh, Pennsylvania: Carnegie Mellon University, 2002. <http://www.sei.cmu.edu/publications/documents/02.reports/02tr011.html>

[3] Willis H. Ware, ed. *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security*. 1970. Rand Report R-609-1. Reissued, Santa Monica, California: The Rand Corp., 1979. <http://www.rand.org/publications/R/R609.1/R609.1.html>

[4] *An Introduction to Computer Security—The NIST Handbook*. Federal Information Processing Standards Special Publication 800-12. Gaithersburg, Maryland: NIST, October 1995. <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>

2 OVERVIEW

Security of data communications systems is a very important issue often not given enough attention. To date, most civil space missions have relied on their uniqueness and obscurity to deter unauthorized access. Some have ignored the issue entirely. However, this is changing because of increased international missions with cross-agency support and the potential use of public ground data networks to transfer mission control and monitoring data. Unprotected civil space mission communications systems are highly vulnerable because of increased reliance on ubiquitous networks. Furthermore they are a high profile target for malicious attackers to compromise a spacecraft just for fun. Also, spacecraft data may be sensitive from a commercial or operational perspective (e.g., commercial, space-based imagery; dual-use technologies) and therefore confidentiality, authentication, integrity, and access controls will be important considerations.

CCSDS missions must now address security. Military space systems have traditionally included a high level of built-in security whereas civil space missions have little, if any security.

With the general increasing level of security awareness in the Information Technology (IT) community, civil and scientific missions should not wait to act until *after* a security incident occurs. The continued expansion of network interconnectivity for data dissemination and science-mission scheduling creates new and additional threats against civil space missions. All threats should be analyzed and protected against to provide protection of assets and critical services.

While this document presents an overview of threats against space missions, including illustrative examples of threats against various classes of missions, detailed threat analyses should be carried out by mission planners in order to understand and state their mission's security requirements.

3 THREAT ANALYSIS PROCESS

3.1 COMMON THREATS

3.1.1 GENERAL

Mission systems, both space and ground, may be subject to a number of threats that can potentially inflict damage that may result in the loss of data or catastrophic loss of the entire mission. While this document and the threats listed are not exhaustive, the following sections will attempt to provide an overview of the most common threats to which these systems might be vulnerable.

3.1.2 DATA CORRUPTION

Data corruption could result in the loss of valuable science information or could potentially result in the loss of a mission.

Data could be corrupted in the ground systems. It could also be corrupted in transmission to or from a spacecraft. It could also be corrupted onboard the spacecraft. Corruption might be a result of, for example, software failures or bugs, hardware failures, use of unauthorized software, or active attempts to change/modify data to deny its use.

Data corruption could result in catastrophic loss if a command were modified and either no action occurred or the wrong action was taken onboard a spacecraft. For example, if a navigation maneuver burn were corrupted, the spacecraft might end up in an unusable orbit, miss an encounter with a comet/planet/asteroid, or be destroyed.

3.1.3 GROUND FACILITY PHYSICAL ATTACK

A physical attack against the ground system could result in the total loss of data or the entire mission. The physical attack's intent might be to disable the ground facility resulting in mission loss. It might also be to overtake the facility in order to take control of the spacecraft without technically attacking the systems.

3.1.4 INTERCEPTION OF DATA

Data to and from spacecraft are sent over Radio Frequency (RF) communications links which are subject to interception by listening to the allocated frequencies. RF links to spacecraft are potentially less susceptible to interception than common radio because of the large ground antennas and narrow beam widths used to communicate between the ground and space and conversely, the low power and narrow beam widths used from space to ground. But this is mission dependent since not all missions are the same. For example, GeoTransitory Orbit (GTO) and Geostationary Earth Orbit (GEO) would have a relatively large downlink beam width resulting in a much more easily intercepted signal.

3.1.5 JAMMING

Given that communications to and from spacecraft are transmitted over RF links, denial of communications could be accomplished by interfering with the RF signal. This can be done by injecting noise, by transmitting on the same frequency from another source, or by simply overpowering the original source. The interference can result in link loss and denial of communications.

3.1.6 MASQUERADE

Authentication of an entity’s true identity is crucial for applying access control policies. When access control policies are being enforced, certain entities are allowed to perform specific actions while other entities may be denied those actions. However, the access controls can be rendered useless if entities can lie about their true identity or can assume the identity of another entity. For example, an instrument operator should not be allowed to perform spacecraft bus health and status actions which might result in a loss of the mission.

3.1.7 REPLAY

Interception of command data is a potential problem. For example, if the commands were copied and later re-transmitted to their originally intended destination, those commands might be acted upon a second time. If the commands resulted in a maneuver burn or a spacecraft re-orientation, the result might be a spacecraft’s being in the wrong place at the wrong time.

3.1.8 SOFTWARE THREATS

Users, system operators, and programmers often make mistakes that can result in security problems. Users can install unauthorized or un-vetted software, which might contain bugs, viruses, spyware, or which might simply result in system instability. System operators might configure a system incorrectly resulting in security holes. And programmers may introduce logic or implementation errors which could result in system vulnerabilities or instability.

3.1.9 UNAUTHORIZED ACCESS

Strong access control policies based on strong authentication provide a means by which only those entities that are authorized to perform actions are allowed to do so while all others are prevented. Should there not be any access controls in place, or if they are weak, or authentication is weak, the result might be unauthorized access to systems. Likewise, interception of data could also result in unauthorized access because identities and/or passwords might be obtained.

3.2 THREAT ANALYSIS METHODOLOGY

In order to determine security threats against a mission, a threat analysis methodology should be followed. Such a methodology is illustrated in figure 3-1.

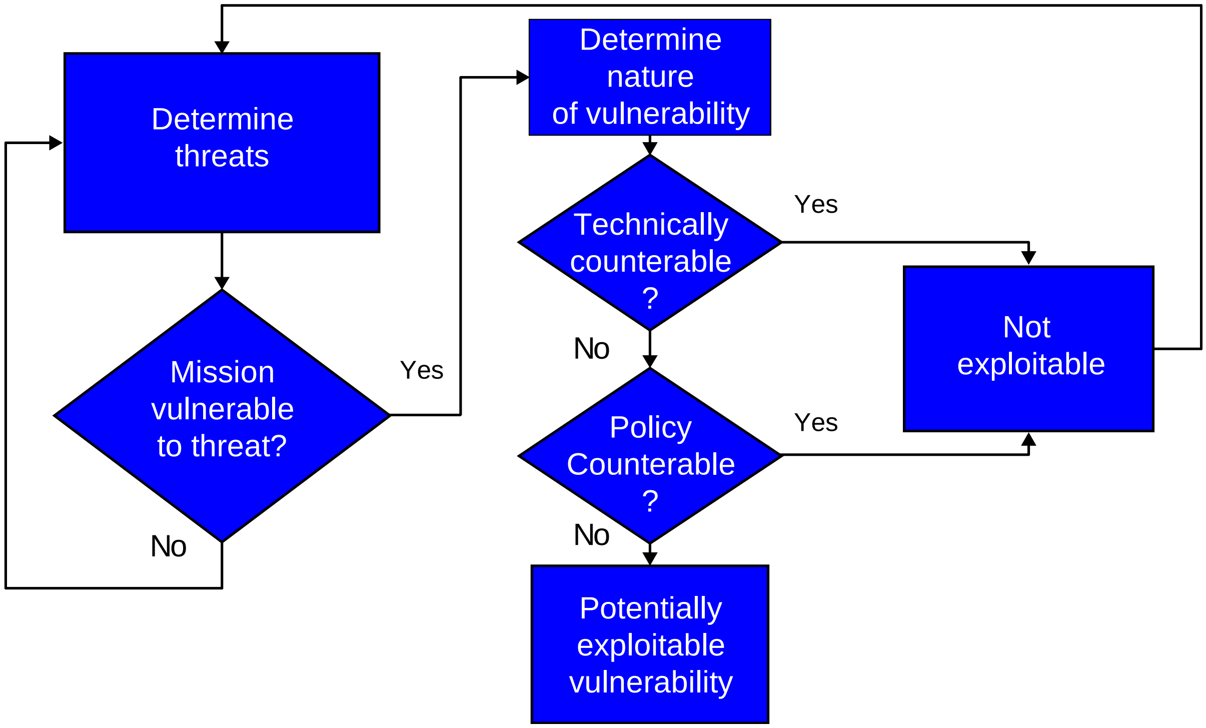
Determine threats
Mission vulnerable to threat?
Yes
No
Determine nature of vulnerability
Technically counterable ?
Yes
No
Policy Counterable ?
Yes
No
Not exploitable
Potentially exploitable vulnerability

Figure 3-1: Generic Threat Analysis Methodology

This figure illustrates a generic process in which one determines the **threats** against a mission system and then decides whether or not the mission is **vulnerable** to the threat. Based on the characteristics of the vulnerability, it then must be determined what the response will be: can the vulnerability be countered by either technical means or by policy?[1] A cost-benefit analysis must be performed to determine if it is worth countering the threat by technical means. If the technical means is very expensive, but the likelihood of exploitation of the vulnerability is low, then a policy response might be in order. For example, if it is estimated that a technical fix to counter a threat will cost 50% of what it cost to build the entire system, instead there may be a way to avoid the problem by administratively not allowing a specific mode of operation that exposes the vulnerability.

If the vulnerability can be countered, it is not exploitable and is no longer a concern. However, if there is no means to counter it either by technical means or by policy, then it remains a concern and is classified as a *residual risk*. The vulnerability may only be partially counterable and therefore some residual risk may remain.

Taking the generic methodology one step further, it can be refined into a more specific methodology for use in space mission threat analyses. This is illustrated in figure 3-2.

[1] In this discussion, '*technical means*' indicates that a security mechanism implemented in hardware or software will be employed to counter the vulnerability; '*policy*' indicates that a security mechanism will not be employed, but instead the vulnerability will be countered by a restriction (a policy) issued by the system managers responsible for ensuring the system's security.

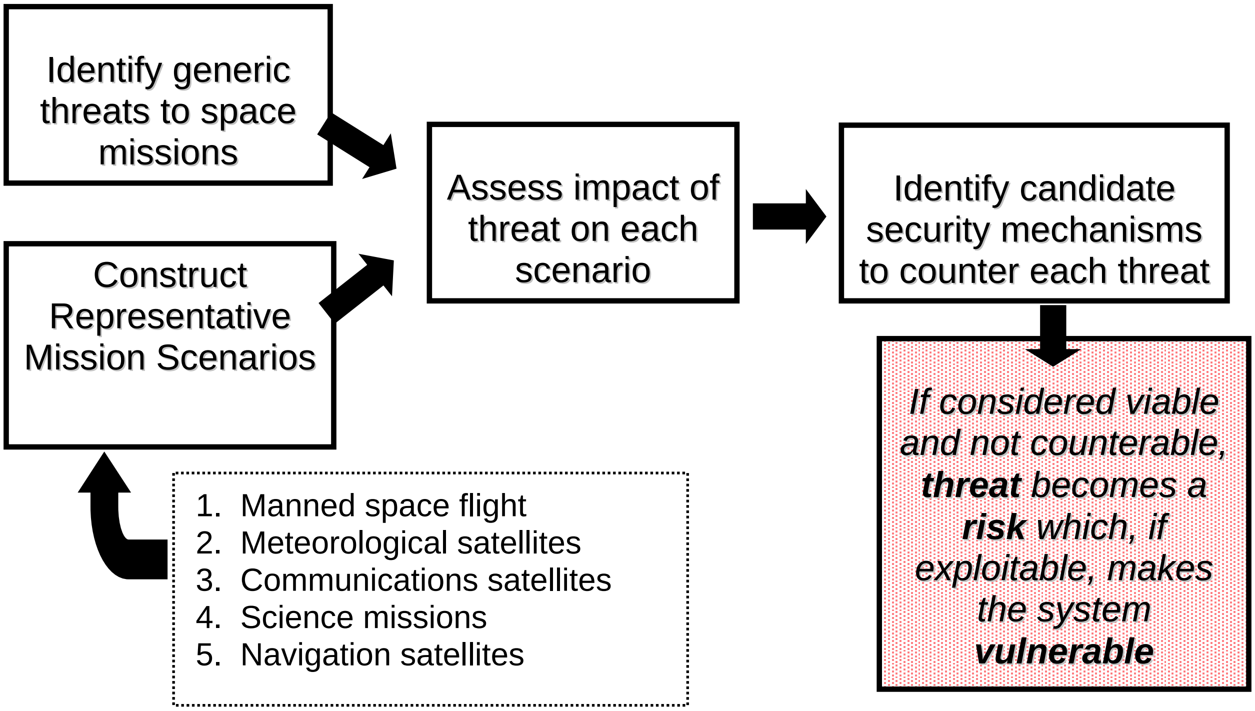
Identify generic threats to space missions
Construct Representative Mission Scenarios
Assess impact of threat on each scenario
Identify candidate security mechanisms to counter each threat
If considered viable and not counterable, threat becomes a risk which, if exploitable, makes the system vulnerable
1. Manned space flight
2. Meteorological satellites
3. Communications satellites
4. Science missions
5. Navigation satellites

Figure 3-2: Space Mission Threat Analysis Process

A number of generic threats to CCSDS space missions have been found. Many of the threats are applicable to non-space systems (e.g., generic computer installations) including the ground networks used to support the missions. Threats include hardware and software failures, loss of data confidentiality via data interception, replay of recorded data, loss of data integrity, and unauthorized access. However, there are some additional threats that are applicable in the space environment that would not necessarily be problems in other environments. Among these are jamming of radio frequency communications links, ‘hijacking’ of space links (another variation of unauthorized access), and space debris. And, of course, hardware failures in a space environment are much more critical than in a terrestrial environment because of the difficulty and expense involved in making repairs. These generic space mission threats are illustrated in figure 3-3.

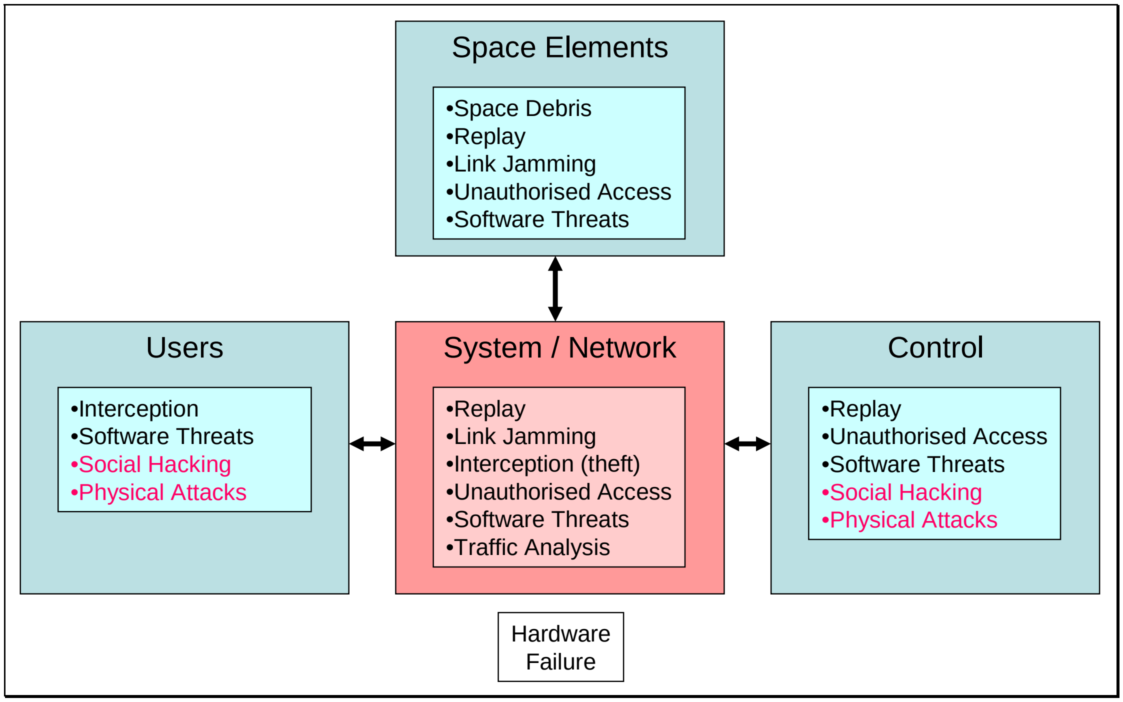

Figure 3-3: Generic Threats to CCSDS Space Missions

In addition to generic threats against space missions, there are a number of network threats, first documented in 1970 (reference [3]) that are still meaningful today, and may be even more meaningful because of the ubiquitous network connectivity that we now see and will see even more of in the future.

Among the network threats documented in 1970 that are still relevant today are:

– unauthorized access;

– theft of information (loss of confidentiality);

– software and hardware failures (denial of service, loss of integrity);

– dishonest maintenance personnel (insider threat);

– dishonest systems personnel (insider threat);

– network taps (loss of confidentiality); and

– communication radiation (loss of confidentiality).

All of these threats from 1970 are *still* relevant with respect to CCSDS space missions, not only from a space perspective but also from a ground network perspective as well. Of course, there are new, more sophisticated threats as well which will be discussed in subsequent sections of this document. Figure 3-4 is a reconstruction of the diagram from the 1970 report, shown here to illustrate that network threats are not new problems.

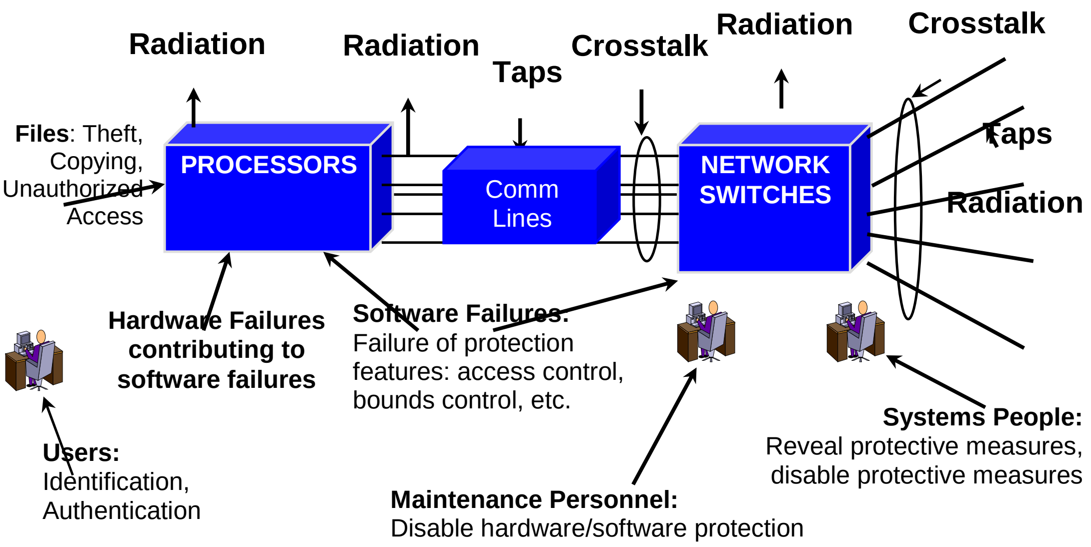
Radiation
Radiation
Taps
Crosstalk
Radiation
Crosstalk
Files: Theft, Copying, Unauthorized Access
PROCESSORS
Comm Lines
NETWORK SWITCHES
Taps
Radiation
Hardware Failures contributing to software failures
Software Failures:
Failure of protection features: access control, bounds control, etc.
Users:
Identification, Authentication
Maintenance Personnel:
Disable hardware/software protection
Systems People:
Reveal protective measures, disable protective measures

Figure 3-4: Classic Network Threats (from Reference [3])

3.3 THREAT ANALYSIS AND MISSION PLANNING

As previously stated in the introduction, this document provides mission planners with a threat overview that can be used to understand and state their mission's specific security requirements.[1]

If one looks at the way a threat analysis should be conducted, it is very similar, if not identical to, a quality assurance process with the following steps:

- Mission start (design): produce recommendations resulting from the threat assessment and the risk analysis;
- Implementation: use standards (CCSDS and others), contingency and disaster recovery planning, conduct conformance testing;
- Operations: Operating procedures, Continuous Contingency Capability, Threat monitoring.

A threat assessment begins with gathering data about the threatened areas and analyzing the information. The assets being protected must be assigned a value. Such an asset valuation should take into account the asset's intrinsic value as well as the near and long-term impacts if it is compromised. Some assets can be assigned a monetary value. For some, assigning a monetary value might prove to be impractical or impossible. In those cases, a determination must be made to assess the value of the system and/or the data if it were to be lost. In some cases, the loss might be assessed as a 'national disgrace'. In some cases, it might be assessed

[1] More specifics will be found in the planned-to-be-written CCSDS Mission Planners Guide for Security.

as damaging to a national space program. In yet other cases, it might be assessed as a 'too bad—we'll get more data from another mission' occurrence.

Threats against the assets must be identified and analyzed to determine their likelihood of occurrence and their potential to inflict harm. If there is no (or very low) likelihood of the occurrence of a threat, then it is not of high concern. If there is a likelihood of occurrence, it should be rated either numerically (e.g., on a scale from 1 to 5) or as high, medium, or low.

A vulnerability analysis compares the outcome of the threat analysis against the mission systems. A valid threat is not of concern if there are no system vulnerabilities that it can exploit. For example, if there is a damaging Windows virus threat in the wild but all systems involved in the mission are UNIX, Linux, or VxWorks based, then there is no concern and no action needs to be taken.

If there are threats that are likely to occur, and there are system vulnerabilities that could be exploited by the threat, it must be determined if there is a way to counter the threat, either by technical means or policy. If neither is available, or if it is determined that the costs are too high to implement a counter, then the residual risk must be documented and accepted by the mission authorities.

3.4 ACTIVITIES AND EXPECTED RESULTS

The reasons for integrating security into space activities have already been stated, and if anything, the threats against missions are only increasing with the sophistication of the *threat agent*.

It is suggested that a Common Assessment Methodology be agreed upon and adopted by all Agency Space Mission Security Officers. Furthermore, a common analysis process will help agreement on common conformance testing and facilitate the agreement on interoperation procedures for multi-agency missions.

Since the threats are constantly evolving and changing, special emphasis has to be put on constant risk awareness and management. Operational contingency management is a key issue, based on a common (i.e., inter-Agency) organization that would provide all missions with continuous threat monitoring.

3.5 THREAT SOURCES

The possible sources of threats may be:

- terrorists and criminals;
- foreign intelligence services;
- subversives or political activists;
- computer hackers;

- software failures;
- hardware failures;
- commercial competitors;
- dishonest maintenance personnel;
- dishonest systems personnel;
- inadvertent actions of staff members; or
- disgruntled staff members.

4 THREATS AGAINST ILLUSTRATIVE MISSION TYPES

4.1 GENERAL

CCSDS space missions threats have been categorized to into two classes: *active* threats and *passive* threats.

4.2 ACTIVE THREATS

An active threat requires an adversary to initiate a sequence of events to attempt to exploit a vulnerability. During an active attack, the adversary attempts to probe the system, or cause mischief or upsets in order to compromise the system(s).

Active threats include but are not limited to exploits such as the following:

- communications system jamming (resulting in denial of service);
- attempting access to an otherwise access-controlled system resulting in unauthorized access;
- replay of recorded authentic communications traffic at a later time with the hope that the authorized communications will provide data;
- masquerading as an authorized entity in order to gain access;
- the exploitation of software vulnerabilities (bugs);
- unauthorized modification or corruption of data; and
- malicious software such as a virus, worm, Distributed Denial-Of-Service (DDOS) agent, or Trojan horse.

Active threats may be carried out against both spacecraft and ground systems. In the case of ground systems, it is imperative that they are operated as *controlled networks*. That is, in general they should not be connected to open, external networks such as the Internet without any safeguard. If a connection across an open network is required, it should be accomplished through the use of formal risk assessment and technical security controls (e.g., secure Virtual Private Network (VPN), firewalls, anti-virus, anti-spyware). Only personnel who have been screened (e.g., national agency checks) should be provided access to the closed ground system network.

4.3 PASSIVE THREATS

Passive threats do not require an adversary to do anything other than sit back and take advantage of what is already in place and being used.

Passive threats include but are not limited to exploits such as the following:

- tapping of communications links (wireline, RF);
- exploitation of software vulnerabilities; or
- traffic analysis.

An example of a passive threat would be the interception of data being sent via radio frequencies. An adversary would point an antenna and tune a receiver to intercept the data. Rather than trying to break in or cause an upset, this type of passive threat is performed unbeknownst to the entity under attack. Encrypting the data over the radio link would effectively eliminate this threat.

A passive threat may also take advantage of a software vulnerability such as when a worm infects a system and migrates to other systems, all the while disclosing information to whoever cares to listen. Protecting the systems, as discussed in the active threat section, using anti-virus software, firewalls, intrusion detection/prevention systems, etc., will help counter this threat.

Another type of passive attack would be traffic analysis: the ability to determine, in loose terms, what is going on between communicating entities simply by virtue of how and when they are communicating without necessarily being able to see or understand the data being communicated. This threat can be countered by totally obscuring the link communications either by what is called ‘full-period traffic security’, or by frequency hopping and spread spectrum technologies. In full-period traffic security, the link would always appear busy whether or not ‘real’ traffic was being sent. In this way, a passive adversary would not be able to determine when ‘real’ data was being sent since it would appear that data was being sent 100% of the time. Frequency hopping and spread spectrum attempt to hide the transmission by jumping around the frequency spectrum resulting in the passive attacker’s not being able to lock onto the data without the hopping or spreading settings.

4.4 ILLUSTRATIVE MISSION THREATS

4.4.1 GENERAL

The following subsections will illustrate the threat analysis of various mission categories that may be of interest to civil space mission planners. By no means is this an exhaustive or detailed threat analysis; it is meant to provide a top-level description of the kinds of threats that are possible against these types of missions. The categories of missions that will be examined are:

- manned space flight;

- meteorological satellites:
  - Low Earth Orbit (LEO),
  - Geosynchronous Earth Orbit (GEO);
- communications satellites:
  - LEO constellations,
  - GEO;
- science missions:
  - near Earth/Earth orbit,
  - lunar,
  - interplanetary/deep-space;
- navigation satellites.

These classes denote missions in varying orbits. The threats against each orbit type may be different. GEO missions, although at a higher altitude requiring more communications power, can be more vulnerable than a low-Earth mission because they provide continuous visibility in their coverage area. LEO missions on the other hand provide limited view periods but can be reached with low power levels and small antennas.

A special case of LEO mission is the communication constellation (e.g., *Iridium*). Whereas each individual LEO spacecraft provides only limited visibility, there are many spacecraft in orbit, providing almost continuous global coverage with satellite cross links creating a space network. Therefore the LEO communication constellation provides an adversary with more opportunity for attack than does a single LEO mission.

More infrastructure (resulting in higher cost) is required to attack deep-space/interplanetary missions than Earth/near-Earth orbit missions because of the larger antennas and higher power required to communicate with the spacecraft.

4.4.2 MANNED SPACE FLIGHT

The International Space Station (ISS) is a good example of a manned space mission with international cross support and cooperation. Modules aboard the ISS have been built by several different nations and the ISS crews come from a variety of countries. Table 4-1 illustrates a possible threat analysis for the ISS.[3]

[3] These threats, the impacts, and the security mechanisms to counter the threats are illustrative only and do not reflect what is actually being done on the International Space Station.

Table 4-1: Manned Space Flight—International Space Station Threat Analysis

Applicable Threats	Impacts	Probability (1= Lowest, 5= Highest)[4]	Security Mechanisms to Counter Threat
Data corruption	• Modification of information • System damage	2	• Data integrity schemes (hashing, check values, digital signatures) • Resilient hardware (e.g., SOS)
Ground facility physical attack	Loss of command, control, and data	2	Guards, gates, access controls, backup site(s)
Interception	Loss of sensitive data	3	Data encryption, spread spectrum, frequency hopping
Jamming	Loss of command and telemetry link	2	• Multiple uplink paths • Frequency hopping • Spread spectrum
Masquerade	• Potential to disrupt operations (uplink) • Potential to receive false information (downlink)	3	• Strong authentication of uplinked commands and downlinked data • Access control scheme • Vetting of staff • No use of open networks
Replay	System damage (possible safety of life issues	1	Authenticated command counter, timestamp
Software threats	• Undesirable events • System damage • Enable other threats	2	• Acceptance testing • Independent Verification and Validation (IVV) • Code walkthroughs • Automated code analysis • Auditing
Unauthorized Access	• Disruption of operations • System damage (possible safety of life issues)	4	• Encryption of TT&C and mission data • Authentication of commands • No use of open networks • Authentication tokens (e.g., smart card) • Auditing

[4] These probabilities (in this and all subsequent tables) are for illustrative purposes only and will change for specific missions.

4.4.3 METEOROLOGICAL SATELLITES

Meteorological satellite systems illustrate a type of mission that is both scientific in nature as well as being a critical national or international asset. Over the years, these missions have become a necessary part of our climate observation and prediction infrastructure. Meteorological satellites may be in Low Earth Orbit (LEO) or in Geosynchronous Earth Orbit (GEO). Table 4-2 illustrates the possible threats against meteorological satellites.

Table 4-2: Meteorological Satellite Threat Analysis

Applicable Threats	Impacts	Probability (1=Lowest, 5=Highest)[5]	Security Mechanisms to Counter Threat
Data Corruption	• Modification of information • System damage	4	• Data integrity schemes (hashing, check values, digital signatures) • Resilient hardware (e.g., SOS)
Ground facility physical attack	Loss of command, control, and data	2	• Guards, gates, access controls, backup site(s)
Interception	• Loss of sensitive data • Theft of commercial data	3 (LEO) 3 (GEO)	Protection of archive & distribution systems via encryption
Jamming	• Loss of command and/or telemetry link • Commercial impact	2 (LEO) 2 (GEO)	• Multiple uplink paths • Multiple downlink paths • Frequency hopping • Spread spectrum
Masquerade	• Potential to disrupt operations (uplink) • Potential to receive false information (downlink)	2	• Strong authentication of uplinked commands and downlinked data • Access control scheme • Vetting of staff • No use of open networks
Replay	• System damage (possible safety of life issues	1	• Authenticated command counter, timestamp
Software threats	• Undesirable events • System damage • Enable other threats	2	• Acceptance testing • Independent verification and validation (IVV) • Code walkthroughs • Automated code analysis • Auditing
Unauthorized Access	• Theft of commercial data • Disruption of operations • System damage	3	• Encryption of TT&C and mission data • Authentication of commands • Access control in control and dissemination systems • No use of open networks • Authentication tokens (e.g., smart card) • Auditing

[5] These probabilities are for illustrative purposes only and will change for specific missions.

4.4.4 COMMUNICATIONS SATELLITES

Geosynchronous Earth Orbit (GEO) communications satellites have become one of the most ever-present parts of the international communications infrastructure. These satellites are relied upon to relay voice, video, data, paging, etc., all over the world. Outages of these satellites would wreak havoc with the international communications systems (as is best witnessed by the major concerns during periods of high sun-spot activity).

Recently, constellations of communications satellites in Low Earth Orbit (LEO) with satellite cross links, such as *Iridium*, have been orbited. The LEO constellations reduce the communications latency experienced with GEO satellites while still providing extensive Earth coverage previously only available from GEOs. However, the reduced threat to LEO satellites, as discussed previously, 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.

A threat analysis of generic communications satellite systems is illustrated in table 4-3.

Table 4-3: Communications Satellite Threat Analysis

Applicable Threats	Impacts	Probability (1=Lowest, 5=Highest)[6]	Security Mechanisms to Counter Threat
Data corruption	• Modification of information • System damage	4 (GEO) 2 (LEO)	Data integrity schemes (hashing, check values, digital signatures)
Ground facility physical attack	Loss of command, control, and data	2	Guards, gates, access controls
Interception	• Loss of sensitive data • Theft of commercial data	4 (GEO) 2 (LEO)	Protection of traffic (potentially user responsibility)
Jamming	• Loss of TT&C and/or traffic circuits • Commercial impact • Possible safety impact	3 (GEO) 3 (LEO)	• Multiple uplink and downlink paths • Multiple access points • Frequency hopping • Spread spectrum
Masquerade	• Potential to disrupt operations (uplink) • Potential to receive false information (downlink)	2	• Strong authentication of uplinked commands and downlinked data • Access control scheme • Vetting of staff • No use of open networks
Replay	• System damage (possible safety of life issues)	1	• Authenticated message counter, timestamp
Software threats	• Undesirable events • System damage • Enable other events	2	• Acceptance testing • Independent verification and validation (IVV) • Code walkthroughs • Automated code analysis • Auditing
Unauthorized Access	• Disruption of operations • System damage	2	• Encryption of TT&C data • Authentication of commands • Auditing

[6] These probabilities are for illustrative purposes only and will change for specific missions.

4.4.5 SCIENCE MISSIONS

Science Missions are a class of missions which are typically not considered operational or part of a national (or international) asset infrastructure. In as much as this is the case, while the threats against such categories of missions are essentially the same as for other missions, the resulting risks are much less than against those where life or infrastructure may be disrupted. In the case of science missions, while money was spent to gather the information, only the monetary investment and the data collection will be lost. Science missions tend to fall into three subclasses:

– near Earth/Earth orbit;

– lunar;

– interplanetary/deep-space.

Near Earth and Earth orbit missions will be similar to other LEO, Medium Earth Orbit (MEO), and GEO missions, although because they are not part of an ‘operational infrastructure’, the resulting risks will be diminished.

Lunar missions and interplanetary/deep-space missions are similar to one another. However, they take on multiple threat characteristics depending on whether they are in Earth orbit before beginning their cruise phase, in cruise, or in some cases, in a sling-shot trajectory where they leave Earth orbit, go into a cruise but come back to near-Earth for a sling-shot effect to a more distant encounter.

While in Earth orbit or near Earth, these missions are just like the other LEO, MEO, and GEO missions. However, their threat characteristics change with time since they will move in and out of Earth orbit.

When they finally leave Earth orbit, they both require more power to communicate with than Earth orbit spacecraft, they both have a non-orbit cruise phase while in transit from the Earth to their target destination(s), and they both will have limited viewing from the Earth once in orbit or when landed at their respective destination(s). However, where these missions differ is in the amount of power and the size of the Earth station antennas required for communication. Interplanetary/deep-space missions require significantly more power and large dishes for reliable communications than do lunar missions. Likewise, interplanetary/deep-space missions suffer from much longer communications latency than do lunar missions. As a result, for interplanetary missions with their longer round-trip communications, the increased power and the size of the dishes required provide immunity from ‘casual’ attack, although not from hostile ‘nation-state’ attacks.

But what must be remembered is that both lunar and interplanetary missions also must take into account the threats faced by Earth orbit and near-Earth missions because they often find themselves in those orbits early in their lives.

A threat analysis for international science category missions is illustrated in table 4-4.

Table 4-4: Science Mission Threat Analysis

Applicable Threats	Impacts	Probability (1=Lowest, 5=Highest)[7]	Security Mechanisms to Counter Threat
Data corruption	• Modification of information • System damage	3	• Data integrity schemes (hashing, check values, digital signatures)
Ground facility physical attack	Loss of command, control, and data	2	Guards, gates, access control
Interception	Loss of sensitive data	1 (deep-space) 3 (lunar) 3 (Earth)	• Evaluation • COTS product use
Jamming	• Loss of TT&C and/or traffic circuits • Commercial impact • Possible safety impact	1 (deep-space) 2 (lunar) 3 (Earth)	• Multiple uplink and downlink paths • Multiple access points • Frequency hopping • Spread spectrum
Masquerade	• Potential to disrupt operations (uplink) • Potential to receive false information (downlink)	2	• Strong authentication of uplinked commands and downlinked data • Access control scheme • Vetting of staff • No use of open networks
Replay	• System damage	1	• Authenticated message counter, timestamp
Software threats	• Undesirable events • System damage	2	• Acceptance testing • Independent verification and validation (IVV) • Code walkthroughs • Automated code analysis • Auditing
Unauthorized Access	• Disruption of operations • System damage • Potential loss of mission	3	• Authentication of commands • Access control in control center • Access control in cross support network • No use of open networks • Auditing

[7] These probabilities are for illustrative purposes only and will change for specific missions.

4.4.6 NAVIGATION SATELLITES

Navigation satellites such as the Global Positioning System (GPS) are irreplaceable for enterprises such as airlines, maritime, trucking, and the military. Similarly, navigation satellites are being used for private use in automobile navigation systems, cellular telephones for emergency locating, and via hand-held units in hunting, exploring, and hiking. Like communications satellites, the loss of navigation satellite systems would result not only in loss of investment dollars; there would also be the high potential for the loss of life, safety, and infrastructure. A threat analysis of such a mission category is illustrated in table 4-5.

Table 4-5: Navigation Satellite Threat Analysis

Applicable Threats	Impacts	Probability (1=Lowest, 5=Highest)[8]	Security Mechanisms to Counter Threat
Data Corruption	• Modification of information • System damage	3	Data integrity schemes (hashing, check values, digital signatures)
Ground facility physical attack	Loss of command, control, and data	3	Guards, gates, access control, backup sites(s)
Interception	Loss of sensitive data	1	• Evaluation • COTS product use
Jamming	• Loss of TT&C and/or traffic circuits • Commercial impact • Possible safety impact	3	• Multiple uplink and downlink paths • Multiple access points • Frequency hopping • Spread spectrum
Masquerade	Potential to disrupt operations	2	• Strong authentication • Access control scheme • Vetting of staff • No use of open networks
Replay	System damage	1	Authenticated message counter
Software threats	• Undesirable events • System damage	2	• Acceptance testing • Independent verification and validation (IVV) • Code walkthroughs • Automated code analysis • Auditing
Unauthorized Access	• Disruption of operations • System damage • Potential loss of mission	3	• Authentication of commands • Access control in control center • Access control in cross support network • No use of open networks • Auditing

[8] These probabilities are for illustrative purposes only and will change for specific missions.

4.5 THREAT SUMMARY AND SECURITY MECHANISMS TO COUNTER THREATS

Table 4-6: Threat Summary

Applicable Threats	Security Mechanisms to Counter Threat
Data corruption	• Data integrity schemes (hashing, check values, digital signatures) • Resilient hardware
Ground facility physical attack	• Guards • Gates • Access control
Interception	• Evaluation • COTS product use • Protection of traffic via encryption, frequency hopping, spread spectrum • Protection of archive & distribution systems via encryption
Jamming	• Multiple uplink paths • Multiple access points • Frequency hopping, spread spectrum
Masquerade	• Strong authentication • Access control scheme • Vetting of staff • No use of open networks
Replay	• Data integrity schemes (e.g., authenticated command counter, timestamps)
Software Threats	• Acceptance testing • System evaluation (e.g., IVV, code analysis) • COTS product use • Continuous threat Monitoring, continuous risk management • Auditing
Unauthorized Access	• Encryption of TT&C and mission data • Authentication of commands • No use of open networks • Access control in control center • Access control in cross support network • Access control in control and dissemination systems • Multiple access paths • Auditing

4.6 COMMUNICATION ARCHITECTURE AND SPECIFIC THREATS

Figure 4-1 illustrates threats that are the result of the architecture of the communication links from the principal investigator (or the commercial company selling the satellite product) to the satellite, at each possible link node.

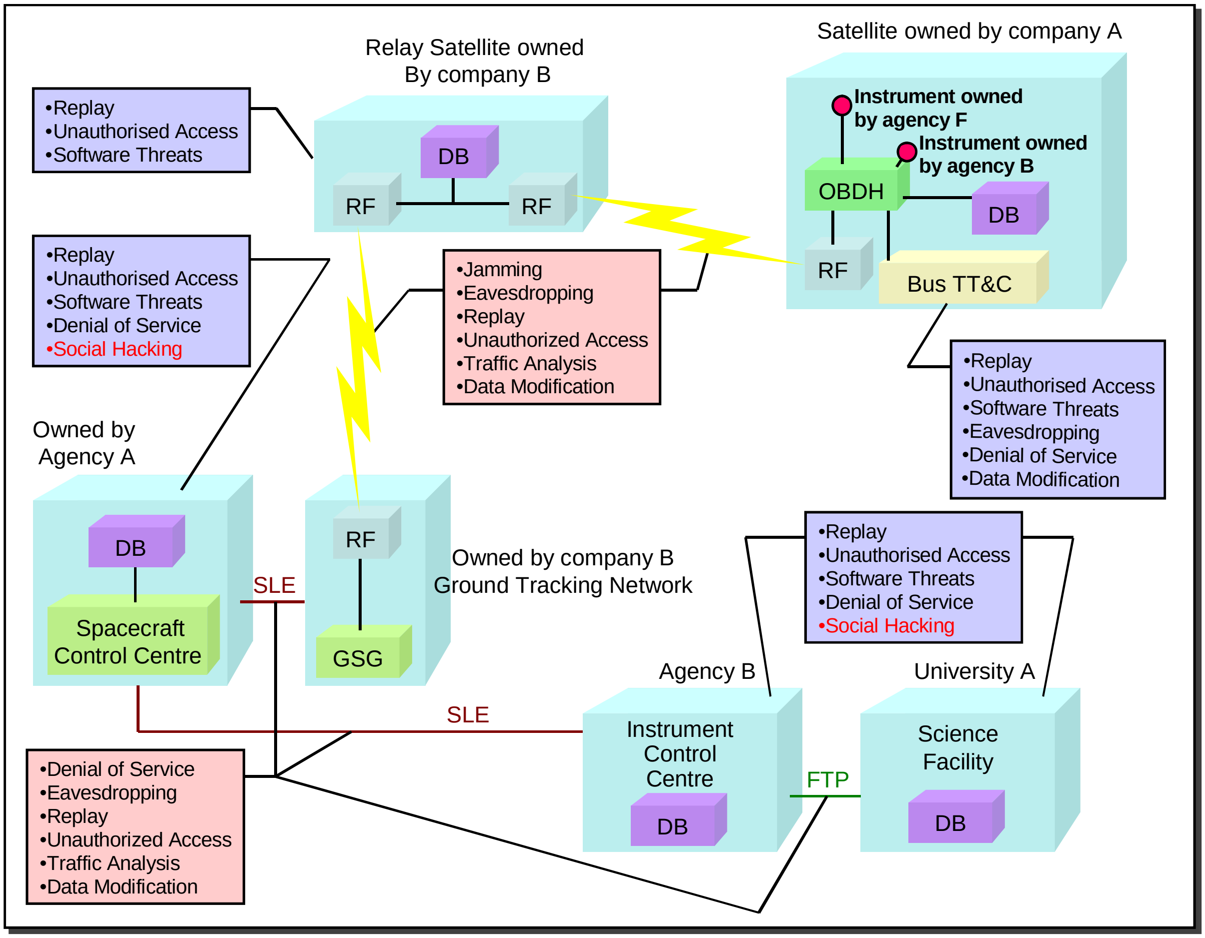

Figure 4-1: CCSDS Security Communications Threats

5 SUMMARY

This document provides a top-level threat analysis of various categories of civil space missions. From this analysis, it is recognized that there are several high potential threat areas.

Unauthorized access is a potential threat against all mission types. However, because it is also a threat against all information technology infrastructure, there are many existing means by which this threat can be countered (e.g., identification and authentication to mediate access control).

Data corruption, while not entirely a security issue, is a major threat. Data corruption may occur because of communications problems which can be solved by coding techniques. However, data corruption may also occur as a result of hostile attacks aimed at denying service. Various data integrity schemes such as integrity check values and digital signatures help prevent this from occurring.

Interception of data leading to loss of data confidentiality or replay of data is also a major threat. However, this is also a well recognized threat against other information technology systems, whether communicating via landline or radio frequency. Encryption technology along with key management and distribution will prevent the disclosure of the data to unauthorized entities. In addition, the use of spread spectrum and frequency hopping technologies can help to prevent data interception as well as prevent link jamming.

Encryption and authentication also help prevent masquerade attacks. Encryption of sequence counters helps prevent replay attacks.

Software problems are also major threats. Software problems may result from bad design, poor coding practices, lack of reviews, or lack of testing. While flight-grade software is typically designed, developed, and tested under exacting processes, development methodologies such as promulgated by the Carnegie Mellon University Software Engineering Institute’s Capability Maturity Model Integration (CMMI) (reference [2]) help to standardize and formalize the development environments to eliminate such threats. However, there is another class of software threat which is the result of malicious attackers in the form of such entities as viruses, worms, and attacks against buffer overflows. These types of threats will continue to be a problem because the ground-based information technology infrastructure has not yet successfully dealt with them to any satisfaction. But with operational configuration management processes in place and with policies such as prohibiting the use of open networks, this threat can be managed.

ANNEX A

ACRONYMS

CCSDS	Consultative Committee for Space Data Systems
CMMI	Capability Maturity Model Integration
COTS	Commercial-Off-The-Shelf
DDOS	Distributed Denial-Of-Service
FTP	File transfer protocol
GEO	Geosynchronous Earth Orbit
GPS	Global Positioning System
ISS	International Space Station
IT	Information Technology
IVV	Independent Verification and Validation
LEO	Low Earth Orbit
MEO	Medium Earth Orbit
RF	Radio frequency
SOS	Silicon-on-Sapphire
TT&C	Tracking, Telemetry, and Command
VPN	Virtual Private Network