The Protection of Space Missions: Threats and cyber threats

Stefano Zatti [1]

[1] European Space Agency Security Office, 00044 Frascati, Italy
Stefano.Zatti@esa.int

Abstract. Space-based systems play an important role in our daily life and business. The trend is likely to rely on the use of space based systems in a growing number of services or applications that can be either safety-of-life critical or business and mission-critical. The security measures implemented in space-based systems may turn out to be insufficient to guarantee the information assurance properties, in particular confidentiality (if required by the data policy), availability and integrity of these services/applications. The various and possible cyber- attacks on space segments, ground stations and its control segments are meanwhile well known and experienced in many cases.

This paper will first introduce ESA and its constituency, then address the security specific aspects of its space missions. Threats specific to them from the cyberspace will be introduced, and the possible countermeasures briefly addressed. A categorization of the different types of space missions will then lead to the creation of the different protections profiles to be implemented respectively for the different categories.

Keywords: Space Missions, Threats, Countermeasures.

1 Introduction: The European Space Agency and its Missions

The European Space Agency, ESA, was founded in 1975 by merging two existing launch and space research organization, with the aim expressed in article 2 of the ESA Convention "To provide for and promote, for exclusively peaceful purposes, cooperation among European states in space research and technology and their space applications." Composed of 22 Member States, with eight sites/facilities in Europe, about 2200 staff, ESA has in the course of its lifetime designed, tested and operated in flight over 80 satellites.

2

2 A Security-flavoured space

Although they are designed and for peaceful purposes, the space missions of ESA can indeed present security aspects and address security elements.

Such critical elements of space missions can influence the level of sensitivity and consequently the level of threats, each on of those space missions have to face. In particular, the following aspects of "security from space" have been highlighted by the ESA Council as critical for the benefit of European Citizens, leading to the development of specific missions to address them:

Security on Earth:

- Critical Infrastructures Protection
- Maritime surveillance
- Land surveillance
- Humanitarian crisis support and rescue tasks
- Public Safety (incl. Civil Protection)
- Other Emergent security threats (e.g., climate change)

Security in Space:

- Space situational awareness, i.e., real time information of the status of specific objects in space
  - Near-Earth Objects: asteroids, meteorites, in the vicinity of our planet.

- Space weather: phenomena out ide the atmosphere that can affect the Earth, like solar wind
- Satellite tracking: knowledge of position and trajectory and speed of the man-made objects, active and inactive, circling around our planet.

3 Hacking in space: Astro-hackers?

In the past, in order to reach a satellite in orbit to threaten its function, it would have been necessary for the adversary to build or possess an infrastructure to send tele-commands, an expensive and massively complex endeavour. Nowadays, via the omni-pervasive access networks all connected to the Internet, it is sufficient for a hacker to tamper with and bypass the existing protection measures …And this is not just science fiction, cases exist and are documented.

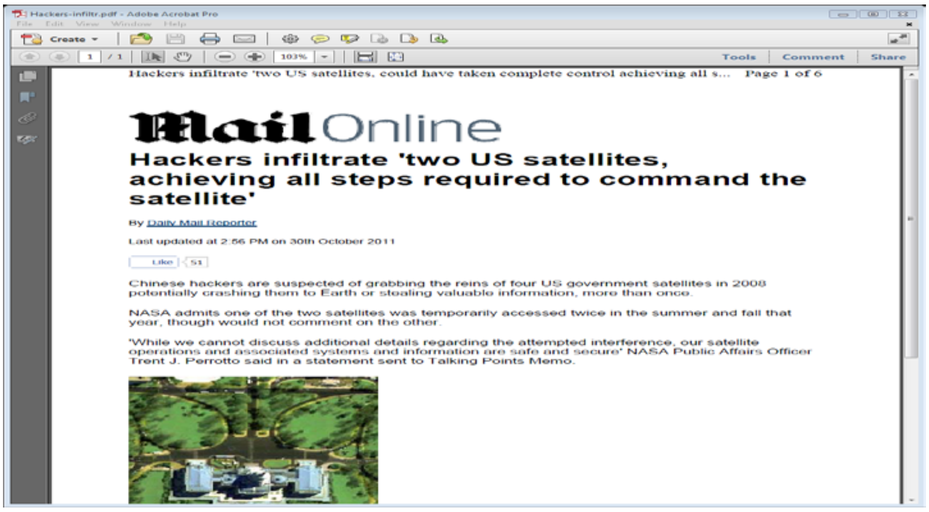
Some unclassified examples from open literature include:

- In 1998, the German-US ROSAT space telescope inexplicably turned towards the Sun, irreversibly damaging a critical optical sensor, following a cyber-intrusion at the Goddard Space Flight Center of NASA in the US.

- On October 20, 2007, Landsat 7 experienced 12 or more minutes of interference. Again, on July 23, 2008, it experienced other 12 minutes of interference. The responsible party did not achieve all steps required to command the satellite, but the service was disturbed.

- In 2008, NASA EOS AM–1 satellite experienced two events of disrupted control: in both cases, the attacker achieved all steps required to command the satellite, but did not issue commands.

These cases made the news, as shown in figure 1.


Hackers-infiltr.pdf - Adobe Acrobat Pro
File Edit View Window Help
Create
1 / 1
103%
Tools
Comment
Share

Hackers infiltrate 'two US satellites, could have taken complete control achieving all s... Page 1 of 6

Mail Online

Hackers infiltrate 'two US satellites, achieving all steps required to command the satellite'

By Daily Mail Reporter

Last updated at 2:56 PM on 30th October 2011

Like 51

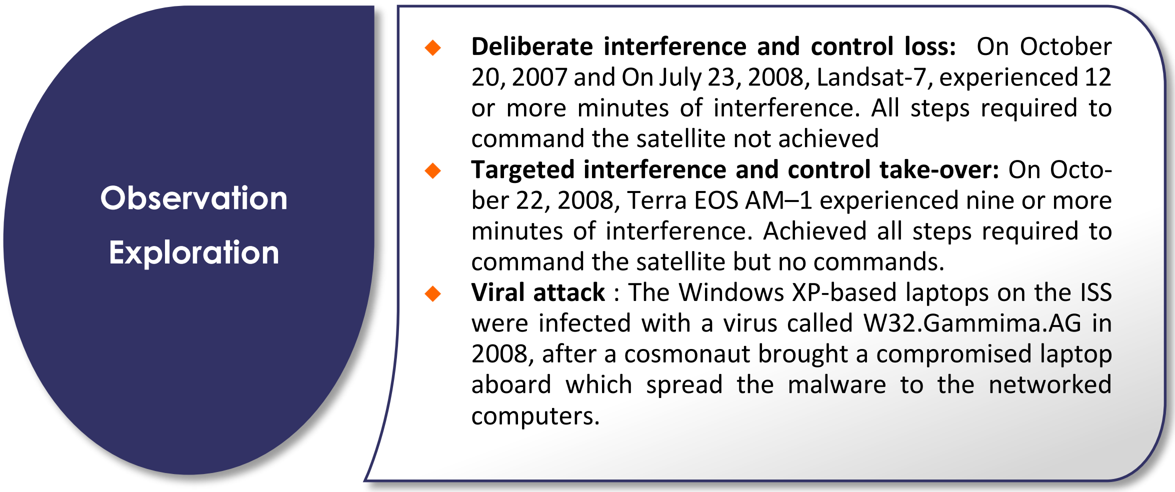
Chinese hackers are suspected of grabbing the reins of four US government satellites in 2008 potentially crashing them to Earth or stealing valuable information, more than once.

NASA admits one of the two satellites was temporarily accessed twice in the summer and fall that year, though would not comment on the other.

'While we cannot discuss additional details regarding the attempted interference, our satellite operations and associated systems and information are safe and secure' NASA Public Affairs Officer Trent J. Perrotto said in a statement sent to Talking Points Memo.

Fig. 1. A news post on Mail Online of 2011, reporting on hacking of US government satellites in 2008

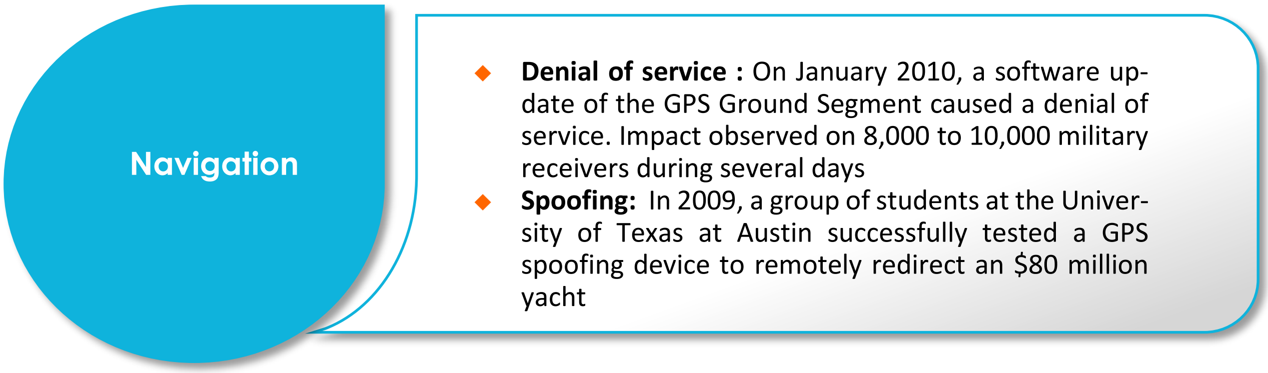
Some more cases are documented in the following figures, that are grouped by the categories of the missions that were affected.



Observation Exploration

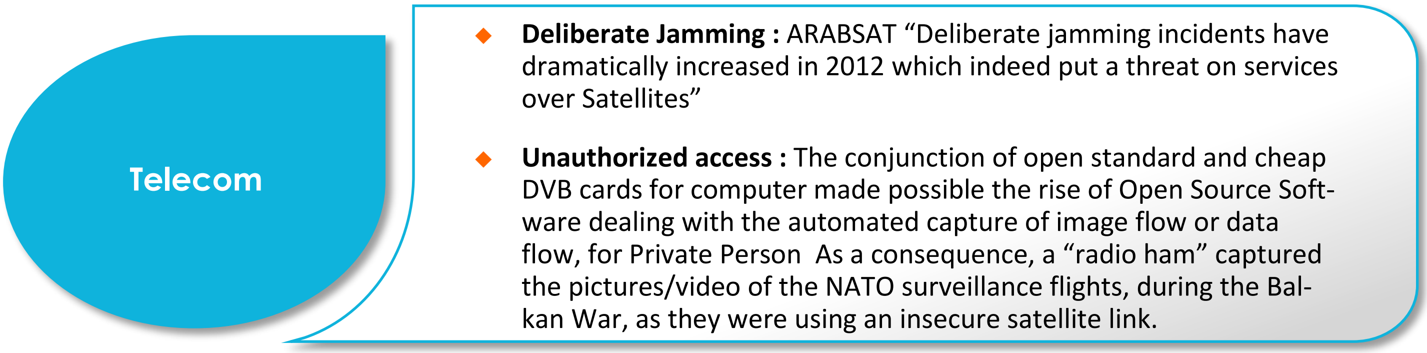
- **Deliberate interference and control loss:** On October 20, 2007 and On July 23, 2008, Landsat-7, experienced 12 or more minutes of interference. All steps required to command the satellite not achieved
- **Targeted interference and control take-over:** On October 22, 2008, Terra EOS AM–1 experienced nine or more minutes of interference. Achieved all steps required to command the satellite but no commands.
- **Viral attack** : The Windows XP-based laptops on the ISS were infected with a virus called W32.Gammima.AG in 2008, after a cosmonaut brought a compromised laptop aboard which spread the malware to the networked computers.

Fig. 2. Cyber attacks on missions of Observation and Exploration



- **Denial of service :** On January 2010, a software update of the GPS Ground Segment caused a denial of service. Impact observed on 8,000 to 10,000 military receivers during several days
- **Spoofing:** In 2009, a group of students at the University of Texas at Austin successfully tested a GPS spoofing device to remotely redirect an $80 million yacht

Fig. 3. Cyber attacks on missions of Navigation.



- **Deliberate Jamming :** ARABSAT “Deliberate jamming incidents have dramatically increased in 2012 which indeed put a threat on services over Satellites”
- **Unauthorized access :** The conjunction of open standard and cheap DVB cards for computer made possible the rise of Open Source Software dealing with the automated capture of image flow or data flow, for Private Person As a consequence, a “radio ham” captured the pictures/video of the NATO surveillance flights, during the Balkan War, as they were using an insecure satellite link.

Fig. 4. Cyber attacks on missions of Telecommunications.

4 Threats and countermeasures

The infrastructures supporting space missions can be characterized by a *Ground Segment, a Space Segment , and a Control Segment.* The control segment is used by the mission controllers, who issue Telecommands (TC) that via the ground segment can be uploaded all the way up to the space segment, a set of spacecraft that circles in space at possibly different altitudes, depending on the mission type. In the other direction, the spacecraft send back to Earth Housekeeping Telemetry (HKTM) to indicate the status of the various instruments and on-board parameters, and the Payload, that is the *raison d'etre* of the mission.

The threats that can face a spacecraft in orbit can be characterised by the different ways that adversaries can use to tamper with the Telecommands that are normally sent from the on-Earth control centre to the spacecraft to perform specific mission related actions, and with the data that returns to Earth, be it either payload related to the mission or house-keeping telemetry that informs ground control of the status of the instruments on board.

5 End-to-end cybersecurity

In order to ensure the proper protection of all the assets related to a space missions, the segments described above, material and human, as well the mission data, it is necessary to tackle the various aspects of security as a process that spans end-to-end.

This implies the consideration of the security pillars and the respective countermeasures, as follows.

- Physical: zoning, access control for data centers, perimeter and internal fencing
- Personnel: vetting, clearances, trust, peer control
- Information protection: classified vs unclassified data and parameters
- Information assurance (IA) properties:
    - Confidentiality - encryption
    - Integrity - MAC
    - Availability - redundancy
    - Authenticity - identity management, cross check, access control, signature of data
    - Non-repudiation - notarization, certificates

It is essential, in order to be able to apply security measures on the ground-to-orbit link, that a set of cryptographic functionalities is installed on board, what normally goes simply under the term "Crypt0-chip", before the launch. This function is able to perform on the Telecommands and on the Telemetry all the functions necessary to implement the Information Assurance properties, as required by the mission designers on the basis of the risk assessment specific to that mission (see next section).

In addition, some missions may require that also the payload should be protected (property of Confidentiality). This implies the encryption of the whole payload, with the consequent need to renew the keys used for the encryption on a periodic basis, determined by the amount of the data to be transmitted.

6 Mission categories and security protection profiles

There is a difference in the threats that different categories of mission can be subject to. Different mission types have actually different security requirements based on the need to protect one or more of the five property of Information Assurance, plus and with priority the well-being of humans (Safety of life applications and manned space-flight).

Missions categorized by different categories of risks, with increasing depth and level of concerns:

- Scientific
- Earth Observation
- Navigation
- Communications
- Space Situational Awareness
- Manned spaceflight and exploration

In order to approach the cyber-security of missions in a systematic way leading to a streamlined engineering, five different protection profiles of Tele-commands and Telemetry, that have been developed, to be applied to the different mission categories (from 0 to 4).

Profile 0: No specific security

No TC authentication and encryption

No House-Keeping Telemetry or science data encryption

Standard terrestrial links security (firewalls, IDP, SIEM etc…)

Implemented in ERS/ENVISAT and Earth Explorers

Profile 1: Static Tele Command protection

TC authentication and anti-replay

Authentication key pre-loaded on board

TC authentication can be enabled/disabled automatically or by ground

Currently implemented on MetOp and ATV

Profile 2: Dynamic TC protection

TC authentication and anti-replay

Authentication keys are loaded by ground using preinstalled Master Keys for the encryption of the related TCs

TC authentication can be enabled/disabled automatically or by ground

Implemented in the Sentinels of the Copernicus programme.

Profile 3: Dynamic TC + payload data protection

Payload data is encrypted

4 types of keys: Master key, TC authentication key, payload data encryption key, TC encryption key

Payload data encryption can be enabled/disabled automatically or by ground

Profile 4: Dynamic TC + payload + HKTM data protection

HKTM data is also encrypted

5 types of keys: Master key, TC authentication key, data encryption key, HKTM data encryption key, TC encryption key

HKTM data encryption can be enabled/disabled automatically or by ground

7 Conclusions: new space – new cyber threats!

- The cybersecurity of space missions is a matter of competiveness for the European space industry, and, at the same time, is a vital subject for the European Union, as owner of the Copernicus and Galileo programmes.

- The need to guarantee high production rates (e.g. 4 satellites per day in the case of the densest constellations) requires the system integrators to stretch globally the existing supply chain, and to include new components providers.

- The globalization of manufacturing capabilities and the increased reliance upon commodity software and hardware for space and ground segments has expanded the opportunities for malicious modification in a manner that could compromise critical functionality. This is introducing additional risks.