Studying Risks in Space Mission Communications

Objectives, approach and expected results

Julio Vivero
Consulting Area
GMV
Barcelona, Spain
jvivero@gmv.com

Luca del Monte
Senior Strategy Coordinator
European Space Agency
Paris, France
luca.del.monte@esa.int

***Abstract*—The paper presents the study on cybersecurity risks for space missions launched by the European Space Agency. This one-year study covers all lifecycle phases within civilian space missions and includes all their actors and elements both at the ground and the space. However, the paper focuses in how mission communications are addressed in the study, the approach followed to identify their risks and the expected results.**

Keywords-Risk; safeguards; communications; missions; taxonomy

I. Introduction

Cybersecurity is a growing concern for governments, public and private entities, and citizens [1][2]. Our reliance on information systems and technology for most of our daily activities is a reality. This fact converts Information Technology and Communications (ITC) into a more attractive target for strategic advantage, espionage, fraud, notoriety, etc.

Space missions are not an exception to this general trend [3]. Nowadays, space missions provide valuable services to society in many fields: from navigation, to earth observation, weather forecasting or communication, sometimes even providing significant revenues to the operators. As such, cyber threats to space missions will continue to grow in the near future [4].

The European Space Agency (ESA) has perceived this trend in the last years and has launched a study to analyze cybersecurity risks to space missions and recommend remediation safeguards. The goals of the study are providing tools to mission planners in order to introduce adequate levels of security in missions in an easier and more efficient way and promote awareness on the increasing cybersecurity risks. The study assesses risks during all phases in the lifecycle of space missions [5] and on all elements and actors involved in the mission.

As crucial element in most, if not all, space missions, the communication links and equipment are carefully addressed in the study. Furthermore, ground-space communications are one particularly critical element in space missions due to their exposure as it is based in an open and easily accessible physical media: the radio channel.

Although the study is broad and generic in nature, this paper focuses in the methodology that will be followed to identify, categorize, and mitigate risks on space mission communications.

In Section II, the study main objectives and how they will be addressed will be described. The methodology followed to identify, assess, and manage risks on communication elements will be explained in Section III. The expected outcomes and impact of the study will be defined in Section IV. Finally, Section V summarizes the main conclusions, future work, and milestones of the study.

II. Objectives

The main goal of the study is “to support ESA in the establishment of technical recommendations and a policy” that help mission planners determine which security safeguards shall be implemented within each particular phase of their mission lifecycle.

It is understood that the result of the study is expected to be an important tool for mission planners. With this tool mission planners shall be able to easily understand the threats, vulnerabilities, and resulting risks that apply to their specific mission category, including all communications issues, and more importantly, safeguards they should implement to reduce that risk to an acceptable level.

The concept behind the study is, given the similarities in missions from the same category in the taxonomy developing, a-priori, a risk assessment and risk treatment plan for each category so that it can be reused in all subsequent missions. Tailoring of the results with mission particularities, such as the relative value of the mission (when compared with its peers in the same mission category) will be possible.

Another complementary objective is to “raise awareness in the space community about the cyber-security issues”. In this sense, both the final report and the executive summary will present the information in a way that is easily readable, understandable, and usable by a broad audience in the field of space operations.

To accomplish the above objectives a new risk assessment methodology has been designed specifically for the study. The following section describes in detail this methodology focusing on how space mission communication aspects are addressed.

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-317-9

III. METHODOLOGY

A. *Principles*

The proposed approach leverages IT-Grundschutz [6] risk assessment methodology, defined by the German Federal Office for Information Security, and adapts it to the particular needs of the study. IT-Grundschutz is based on the modules concept. Modules are representations of threats, safeguards, and ultimately risks for technological components that can be easily applied by organizations saving the effort of performing risk assessments for these technological components since these assessments are done beforehand and reflected in the modules.

Our methodology follows this concept and creates modules for each mission category and lifecycle phase which can be tailored in a number of ways to fit in mission particularities. This approach provides some benefits in respect to other risk assessment and risk management approaches, namely the possibility to customize and tailor the risk assessment to the concrete particularities of the space mission and the ease of use from the mission planner perspective.

In addition to this modularity and customization principles, the methodology is also systematic, to guarantee that no relevant aspect is left aside. Efficiency is essential to optimize the effort required to produce the modules. Commonalities of space missions, even in different categories, shall be exploited to minimize the effort required. Finally but no less important, the methodology and its instantiation shall be well documented to provide evidences and justifications for decisions taken and to guarantee that results are consistent among methodology instantiations.

B. *Phases*

Fig.1 shows the methodology phases and their interactions.

The first phase is the taxonomy definition. This is a crucial activity in the study since a great percentage of the results applicability and study success depends on how missions are categorized. All missions falling with the same category shall share attack motivations for attackers, threats, mission elements, vulnerabilities, resultant risks. Also, identified safeguards shall be applicable to all of them. There shall not be too many categories because the effort efficiency principle would be lost, neither too few because the risk of results not being applicable to all missions that fall within that category.

There are several aspects which are security relevant but do not depend on the mission category, but rather on business models, or mission specific design decisions. Examples of these aspects are subcontracting of mission facilities, sites or even operations, or more relevant to the current paper, the type of communications present in the mission: ground-space, ground-ground or space-space. To address these aspects additional packages will be defined to complement modules with the threats, vulnerabilities, risks, and safeguards linked with them. Hence, the mission planner will select the main mission module applicable for its mission category plus the additional packages applicable to that mission.

Ground-space communications is considered applicable to almost all space missions and hence will be included in the mission category modules. However, ground-ground and space-space communication packages will be developed covering all the risk relevant elements for this kind of communications.

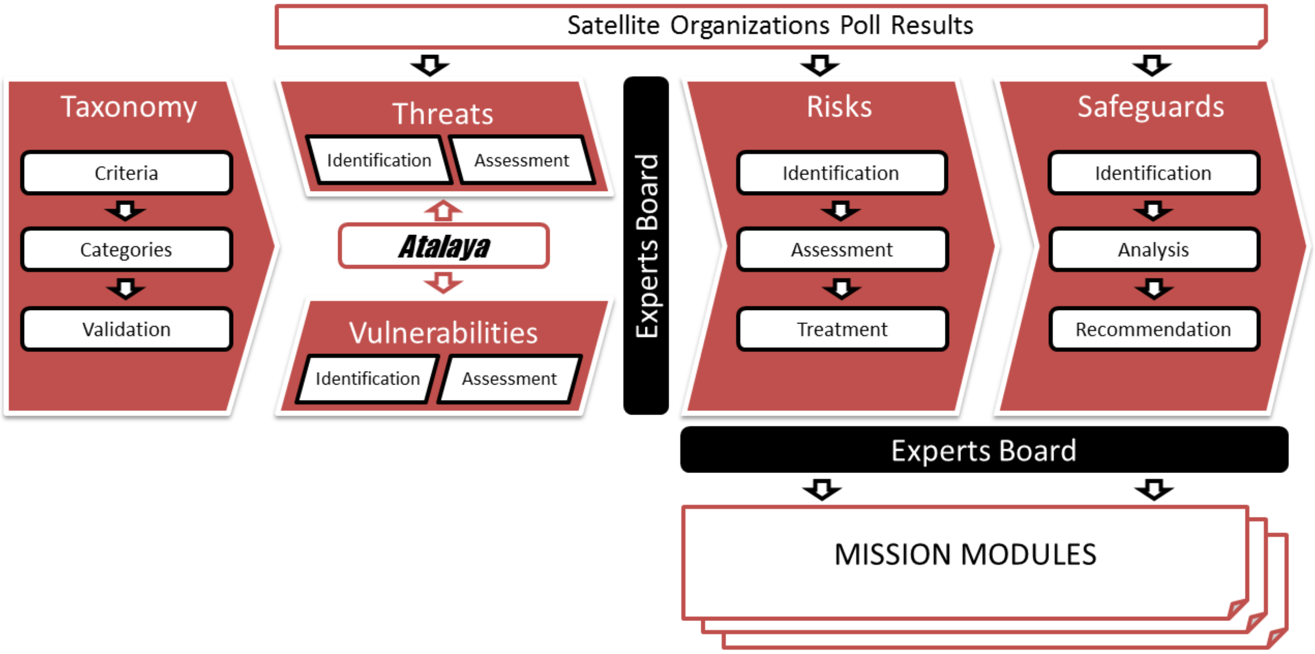

Figure 1. Cybersecurity Study Methodology.

The second phase in the study is the threats assessment for each lifecycle phase of each mission category. The identification of threats will be developed based on threat catalogues (such as IT-Grundschutz catalogue [7], ISO27005 threats catalogue [8] or CCSDS 350.1-G-1 [9]), knowledge of the study team members and the results of a poll among different satellite organizations. These threats, and especially those affecting communications, shall be tailored to space mission particularities. Aspects, such as jamming, protocol efficiency, lag, and space and earth weather shall be taken into account. Jamming is clearly the main threat in relation with space-ground communications but there are other threats which shall not be neglected neither, e.g. eavesdropping, replay attacks or even man in the middle types of attack.

Vulnerabilities will be identified for each asset at each lifecycle phase of the space mission categories. Common weaknesses, insecure configurations, safeguard gaps or implementation flaws will be analyzed as sources of vulnerabilities. The lack of encryption and authentication in messages, weak cryptographic key management practices, single points of failure in communication channels, lack of Denial of Service (DoS) resilience, inexistent or insufficient anti-jamming safeguards and other issues will be examples of vulnerabilities considered from the communications standpoint.

GMV Atalaya service will support the previous phases by providing evidences that justify threat and vulnerabilities values. Atalaya monitors the internet to identify potential attack information, data of interest to attackers or vulnerabilities evidences.

When a threat has been identified with the potential to exploit existing mission vulnerabilities a risk is derived. Resulting risks are assessed based on safeguards traditionally implemented in missions, and then aggregated and prioritized.

During the last phase of the methodology, a set of safeguards will be recommended to mitigate identified risks. As with threats, safeguards will be obtained from catalogues [7][9][10][11], study team knowledge and the satellite organizations poll. Several safeguard implementation alternatives will be proposed, each with a cost-benefit analysis and a description of the remaining residual risk. Also, safeguards will be classified in basic safeguards (recommended for all kind of missions within the category) or high protection safeguards which would be applicable for those missions with higher protection requirements. In some cases areas of further research will be pointed out for investigating more efficient safeguards for particular threats, e.g. innovative anti-jamming techniques, new telemetry, tracking and commanding (TT&C) approaches, etc.

IV. EXPECTED RESULTS

The main results of the study are the modules and additional packages. Each module will contain the risk assessment and risk treatment result for a lifecycle phase of a mission category.

Contents of the modules include the list of applicable threats for each asset and actor, the vulnerabilities, the associated risks, and the recommended safeguards.

Additional packages present the same contents as modules but focused in aspects which are specific of each mission and cannot be extrapolated from the mission category. It is planned to produced additional packages for space-space communications, ground-ground communications, multi-organizational missions, outsourced mission elements, missions with high public visibility and for the type of spacecraft bus used (serial or ad-hoc).

Mission planners will then need to select the appropriate module and complement it, as needed, with the additional packages to get the list of recommended safeguards to include in the mission so that cyber-security risks are mitigated.

The mission taxonomy elaborated during the first phase of the study is another interesting result by itself. It provides a classification of space missions per their cyber-security properties.

At this date, the mission taxonomy phase of the study has been concluded. The following mission categories have been identified:

- Launchers
- Space Tourism
- Manned In-Orbit Infrastructure / Planetary Exploration
- Supply and Re-Entry Vehicles.
- Navigation
- Communications
- Weather Forecast
- Earth Observation Mapping
- Earth Observation Surveillance
- Earth Observation Environmental Monitoring
- In-Orbit Servicing
- Scientific – Up to GEO Orbit
- Scientific – Above GEO Orbit
- Space Situational Awareness (SSA)

Fig.2 below shows the percentage of past, present, and future ESA missions that fall within each mission category according to public information at ESA website (www.esa.int/ESA/Our_Missions).

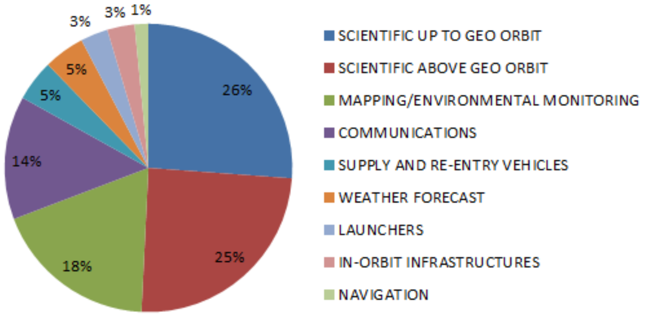

Figure 2. Percentage of ESA missions per category

The above deliverables are clearly presented, described, and explained in a final report and executive summary. These reports will summarize all information in a way to be easily readable, understandable, and usable by a broad audience in the field of space operations

One element included in the methodology, and relevant to the expected results, is the Experts Board concept. To guarantee the quality, applicability, and accuracy of all results, an Experts Board formed by highly qualified and experienced GMV personnel has been formed to review all study deliverables before they are published. In this way, threats, vulnerabilities, risks, and safeguards will be fully useful and applicable to mission planners.

V. Conclusions and Future Work

GMV and ESA are convinced of the potential benefits which can be generated by the study results. Namely, increasing awareness in cyber-security among space mission stakeholders and actors, enhancing the security of current and future missions and thus mitigating their cyber-security risks and finally reducing the effort and knowledge required for mission planners to decide what safeguards shall be implemented in the mission and how.

These benefits will only be achieved if certain conditions are given. First, and most important, the results shall be very easy and intuitive in their exploitation by mission planners. That is, the effort to learn how to use them and apply them shall be as low as possible. Second, risk modules shall be fully applicable to every mission according to its category. If a high percentage of threats, vulnerabilities and safeguards within a module are clearly not applicable to the mission; then mission planners will be discouraged and discard its use. Third and last, recommended safeguards included within the modules shall be effective in the mitigation of space mission risks. Otherwise, the study results would be either complemented or replaced with a different approach.

Looking further into the future it is also important to consider that results shall be simple to maintain and easily updateable with new modules and additional packages to accommodate new mission categories or aspects to consider in terms of cybersecurity. To facilitate these maintenance tasks the methodology shall be described in detail, including guidelines on how to implement the methodology, criteria to consider and rationale followed.

The study started in July 2013 and is expected to be executed during one year, until July 2014.

References

[1] European Commission, “EU Cybersecurity plan to protect open internet and online freedom and opportunity – Cyber Security strategy and Proposal for a Directive,” Digital Agenda for Europe, February 2013

[2] National Institute of Standards and Technology (NIST), “Cybersecurity Framework,” Information Technology Laboratory, February 2013.

[3] Staff Writers, “The State of NASA’s Cybersecurity,” Space Safety Magazine, March 2012.

[4] Kris Osborn, “Air Force Faces Increasing Space Threats: Shelton,” DefenseTech, September 2013.

[5] European Coordination for Space Standardization, “Project planning and implementation,” ECSS-M-ST-10C rev1, 3rd issue rev. 1, March 2009.

[6] German Federal Office for Information Security, “Methodology for evaluating usage and comparison of Risk Assessment and Risk Management items,” Deliverable 2 version 1, April 2007.

[7] German Federal Office for Information Security, “Reference source for threats, vulnerabilities, impacts and controls in IT risk assessment and risk management,” Deliverable 3 version 1, April 2007.

[8] International Standards Organization, “Information technology — Security techniques — Information security risk management,” ISO/IEC 27005, 1st ed., June 2008.

[9] Consultative Committee for Space Data Systems, “Security Threats Against Space Missions,” CCSDS 350.1-G-1, October 2006.

[10] National Institute of Standards and Technology, “Recommended Security Controls for Federal Information Systems and Organizations,” SP800-53 rev.3, August 2009.

[11] International Standards Organization, “Information technology - Security techniques - Code of practice for information security management,” ISO/IEC 27002:2005, 2nd ed., June 2005.