Poster: Spacecraft operations with a security aspect

Michael Koller, Daniel Fischer
Data System Managers
Ground Systems Engineering Department
European Space Agency ESA/ESOC
Darmstadt, Germany
michael.koller@esa.int

***Abstract*—The series of Sentinel spacecraft are the first European Space Agency spacecraft to implement authentication of commands. In this poster, we highlight the security operations concept, the way how security is introduced into the commanding link, the implementation of the key management and the precautions taken to guarantee access to the spacecraft.**

Keywords—authentication; space communication; key management; secure operations concept

I. INTRODUCTION

Over the last years, the number of threats to a space mission's infrastructure has increased dramatically. This is considerably due to the ease of access to and misuse of communication hardware. As stakeholders rely on the continuous availability of the spacecraft mission products, the mission assets need to be protected from unauthorized access. To address the increased threat, current space missions specify security requirements for the communications link.

ESA is implementing the space component for the European Commission's Program for the establishment of a European capacity for Earth Observation – Copernicus (formerly known as GMES). The main objective of Copernicus is to support Europe's goals regarding sustainable development and global governance of the environment. The ESA Sentinels spacecraft constitute the first series of operational satellites of the Copernicus program. As those spacecraft constitute critical infrastructure for the overall program, the need for command authentication and integrity has been one of the main design drivers in order to ensure that only genuine and authentic commands are accepted and executed by the spacecraft.

Whilst the actual authentication is straight forward with today's cryptographic algorithms, other challenges arise from the peculiarities of the space domain: currently, no end-to-end security protocol exists for protection of the space-link and terrestrial protocols cannot be applied. Further, the spacecraft is not physically accessible after launch, so key management is a specific area of concern, considering a mission life time of seven years, not including possible extensions. At the same time, legitimate operators must not be shut out from the spacecraft which could happen due to compromised keys. Cryptographic keys on-board can be compromised for example by single bit events which are not uncommon in the space environment. This aspect requires some interesting trade-offs between security and accessibility.

This poster presents the security operations concept, i.e. the way how security is introduced into the commanding link and the precautions taken to guarantee access to the spacecraft and finally the implementation of the key management.

II. SECURITY OPERATIONS CONCEPT

As indicated above, authentication and integrity of all commands sent to the Sentinel spacecraft is an essential driver for the spacecraft design. This ensures that the spacecraft only accepts and executes commands coming from legitimate sources which have not been tampered with on the communication path.

Being a packet based mission [1], the best protocol stack layer to include the security features is between the data-link and the segmentation layer. This puts security far enough down in the protocol stack to reduce overhead, and far enough up in the stack to keep security transparent to lower level equipment on the communication path. This is due to the layout of the protocol stack in use, which packages segments into commanding frames. All communication equipment on the path is dealing with the commanding frames, therefore security is transparent.

Authentication and integrity are achieved by appending a so-called Authentication Trailer to all command segments. This trailer is composed of a 30-bit Logical Authentication Counter (LAC) and the 128-bit Message Authentication Code (MAC).

The LAC serves to counter replay attacks. It is increased with every command segment released to the spacecraft and included in the calculation of the MAC. The spacecraft will accept a command as long as its LAC falls into the current sliding window for the LAC values. The size of the LAC in combination with frequent re-keying ensures that even with a wrap-around of the counter, a replay attack is not likely to succeed.

The MAC is calculated using the CMAC algorithm based on AES [2]. The data block used as input is the full command segment including the LAC and the active authentication key. The MAC is appended to the segment and transferred to the spacecraft. The spacecraft calculates the MAC from the transferred segment and the stored authentication key and compares the calculated MAC to the transferred MAC. If they match, the command is accepted and executed. The LAC has to

be included in the calculation of the MAC in order to counter replay attacks which merely increase the LAC.

The secure commanding implementation must not lock out the legitimate operators in case of adverse circumstances. Such adverse circumstances may be caused by compromised keys, mostly due to bit flips in the on-board memory caused by cosmic radiation, or by failure of the on-board authentication unit.

The obvious approach is redundancy, which means in the case of the Sentinel spacecraft to include two security units on-board which can operate completely independently and have separate key stores. This gives essentially two completely independent commanding paths on-board.

III. Key Management

Key management is an issue in any security environment. Key management means generation, distribution, and synchronization of cryptographic keys to support the primary security functions. Especially in the space context, key distribution has to be performed via an insecure channel once the spacecraft is flying as no physical access to the spacecraft is possible. On the other hand, the limited number of parties involved in the communication and the lack of physical access to the spacecraft make key management easier in some aspects.

All keys are generated and stored in an isolated unit on ground. This unit is located in a physically access controlled area, locked in a secure computer housing and not connected to any network. Key generation is done using a physical true random number generator. All keys that have to be put into the life system from the repository, are exported as an encrypted container on an encrypted USB memory stick.

The security concept for the Sentinel spacecraft foresees a two-level key hierarchy: Master keys and Session keys. All keys are random 128-bit numbers. Master keys are static keys [3]. They are permanently saved into the programmable read-only memory (PROM) before launch of the spacecraft and cannot be changed. They serve as key encryption keys to create a secure communication channel on the unsecure link to uplink the actual communication keys. Session keys are the keys used for the actual command authentication. They are dynamic [3] and saved in the random-access memory on-board. They are regularly replaced by newly uplinked session keys.

In order to securely uplink new session keys, a secure communication channel is established using a master key. The session keys to be uplinked are encrypted with master keys, and the cipher is included in a command addressed to the security unit. The uplinked command segment is authenticated. The spacecraft can verify the legitimacy of the command, decrypt the cipher and utilize the new keys for operations.

Each of the two security units on-boards knows several active keys: an active session key for normal command authentication, an active session key for authenticating commands addressed to the security units, an active master key for recovery commanding and an active master key for key upload. Obviously, the active keys configured on-board have to match the keys in used on ground.

The session key for normal commanding is the key used for the generation and verification of the MAC for any of the commands sent to the spacecraft which do not address the security unit. The latter commands are authenticated with the second active session key. The recovery master key has been put in place to make a lock-out from the spacecraft due to key corruption less likely. It can be used to recover the spacecraft if any of the active session keys has been compromised. This recovery key basically provides another redundant access point for the operators to recover from key corruption in addition to the measures highlighted in section II.

Any active key can be changed by an authenticated command addressed to the security unit, authenticated with the session key for commands addressed to the security unit.

IV. The Future of Secure Space-link Communication

The Sentinel secure communications design has paved the way for the specification of a generic data-link security protocol for the space link. Such a protocol, re-using a lot of the Sentinel design, is currently being specified by a group of technical representatives from various space agencies. The protocol will allow interoperable security operations, which is an important objective, given the increasing amount of international collaboration in the space business.

This Space Data-Link Layer Security Protocol (SDLS) specifies security operations (authentication and/or confidentiality) for the most important space-link protocols. Similarly to IPSec, it uses the concept of security associations to govern the individual security channels.

The protocol is in its final stage of development and will be available in late 2013, as an ISO standard.

V. Conclusion

The Sentinel spacecraft address the need for command authentication and integrity. The way this feature has been implemented, ensures a maximum of interoperability with existing equipment by ensure a high degree of transparency to the entities involved in the communication path. Established algorithms are used to ensure a secure approach. The needs of a long-term mission (7+ years) and the specific issues in the space domain are sufficiently addressed by a hybrid key management schema which utilizes static and dynamic keys.

The concept is currently under final validation, first test campaigns including the final flight hardware have been successfully passed. The first Sentinel spacecraft is scheduled for launch in October 2013.

References

[1] The Consultative Committee for Space Data Systems, “Packet Telemetry”, CCSDS 102.0-B-5 Blue Book, November 2000.

[2] The National Institute of Standards and Technology, “Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication”, NIST Special Publication 800-38B, May 2005.

[3] The National Institute of Standards and Technology, “Recommendation for Key Management – Part 1: General (Revision 3)”, NIST Special Publication 800-57, July 2012.