Authenticated encryption in civilian space missions: context and requirements

I. Aguilar Sánchez, D. Fischer

Stockholm
05/07/2012

Outline

- Introduction
- Securing Space Missions
    - Space assets protection
    - Mission products protection
    - Spacecraft security services implementation
- Issues, concerns, constraints and requirements
    - Thirteen items to be introduced
- Conclusion

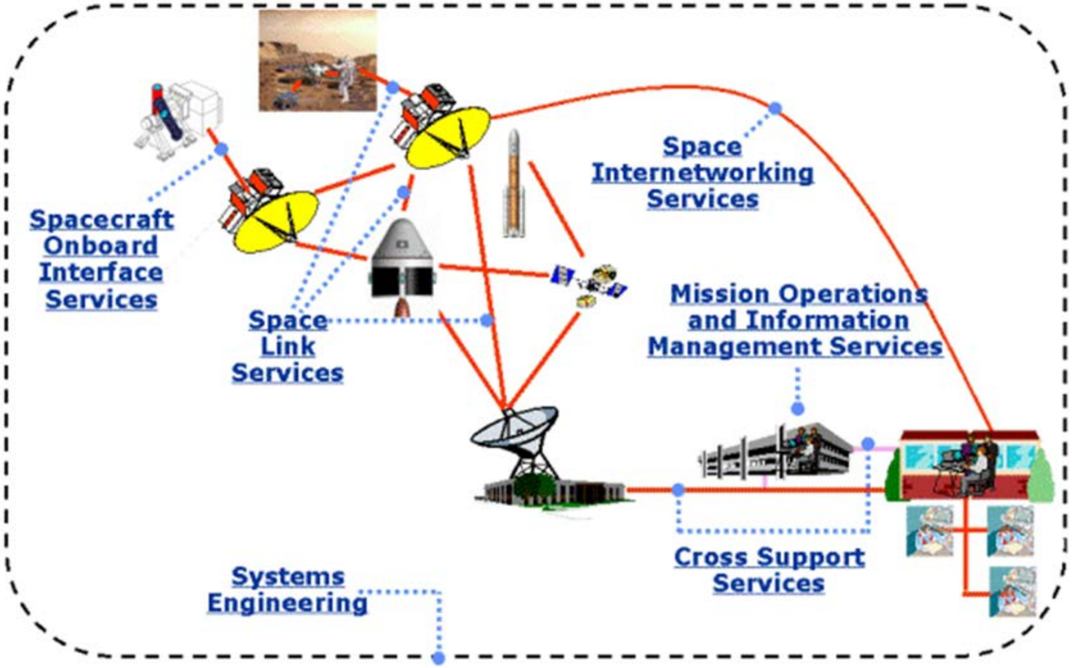
INTRODUCTION

CCSDS background

1. Civilian space agencies cooperate for the development of security concepts applicable to their space missions through CCSDS.
   a. Blue Books (standards)
   b. Green Books (reports)

2. CCSDS has developed over 25 years a set of standard communication protocols & services supporting data transfers within space systems & interoperability:
   a. 60+ standards published;
   b. Serving 500+ space missions.

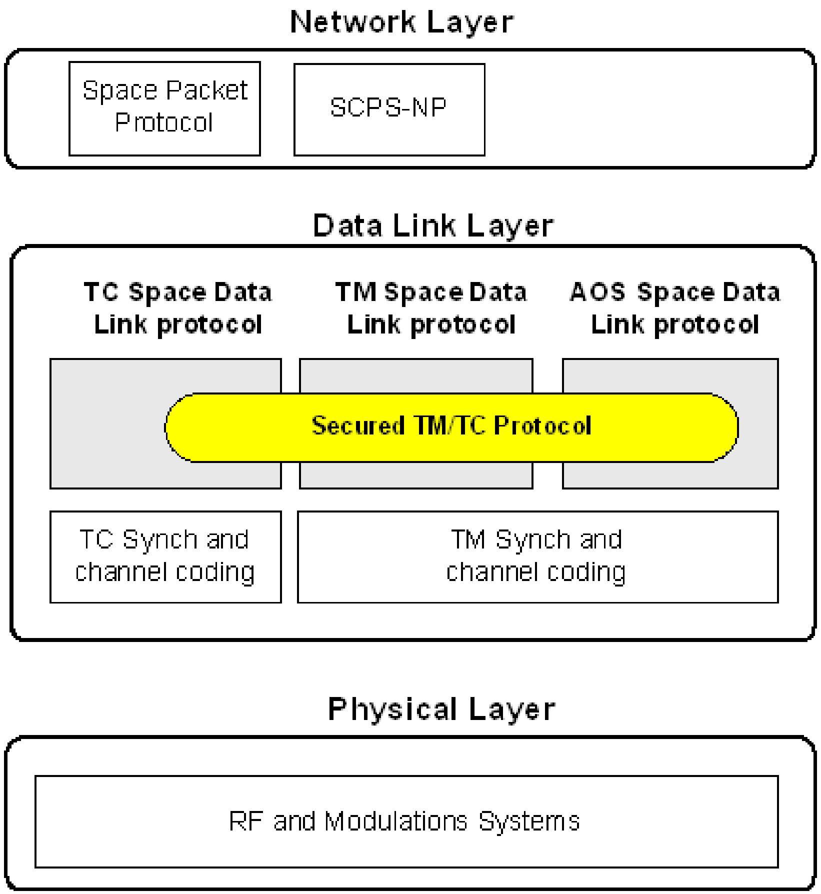
Consultative Committee CCSDS for Space Data Systems


Spacecraft Onboard Interface Services
Space Link Services
Space Internetworking Services
Mission Operations and Information Management Services
Cross Support Services
Systems Engineering

CCSDS Security effort

1. **Several reports and standards** like
   a. The Application of CCSDS Protocols to Secure Systems;
   b. Cryptographic Algorithms;
   c. Security Guide for Mission Planners.

2. **Space Data Link Security (SDLS) protocol**. This security protocol offers
   a. security services to the three Space Data Link protocols previously standardized by CCSDS;
   b. security services: authentication, encryption and authenticated encryption;
   c. flexibility in the selection of services and cryptographic algorithms.
   d. 'Baseline modes' in SDLS and their companion cryptographic algorithms as recommend in another key CCSDS standard on security: Cryptographic Algorithms.



Network Layer
Space Packet Protocol
SCPS-NP
Data Link Layer
TC Space Data Link protocol
TM Space Data Link protocol
AOS Space Data Link protocol
Secured TM/TC Protocol
TC Synch and channel coding
TM Synch and channel coding
Physical Layer
RF and Modulations Systems

Pragmatic approach

1. Cryptography:
    a. Rely on civilian research and standardization (e.g., ISO, NIST) and adopt civilian cryptographic standards;
    b. Study and solve adaptation to space context.

2. Regarding Authenticated Encryption:
    a. Advanced Encryption Standard Galois Counter Mode (AES-GCM);
    b. Potential issue for the future: MAC limited to 128-bits;
    c. In no position to research alternatives or determine ground rules for the combination of authentication and encryption.

3. Take this opportunity to express issues, concerns, constraints and requirements perceived by civilian space missions.

SECURING SPACE MISSIONS

General

1. Two security problems are identified and differentiated when considering how to secure a space mission.
   a. The first one concerns the protection of the space mission assets and their infrastructure, e.g., the satellite or the constellation when more than one satellite is involved, the ground stations, the operations control centre(s), the mission control centre(s), the networks that interconnect them and the interface with the user(s).
   b. The second security problem corresponds to the protection of the mission products, that is, the signals and/or data produced by the spacecraft.

CIA Requirements

Confidentiality needed for:

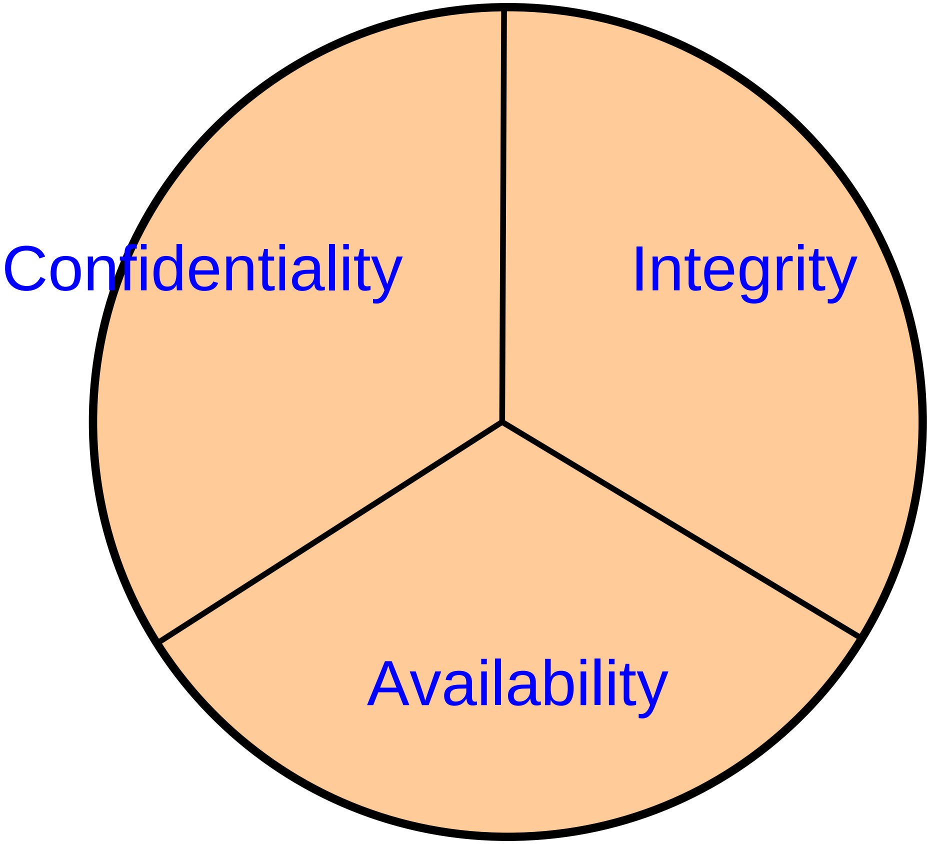
1. Key protection while cryptographic key uploading (TC);
2. Protection Sensitive parameter of security unit in TM, if any;
3. Telecommand protection (optional).

Integrity/Authentication needed for:

1. Transmission error protection;
2. Anti-spoofing/Command source authorization;
3. Complement to Encryption (optional).

Availability needed for:

1. Protection of Telecommand transmission (spread spectrum, null-steering antennas, high-power up-link).



Space asset protection

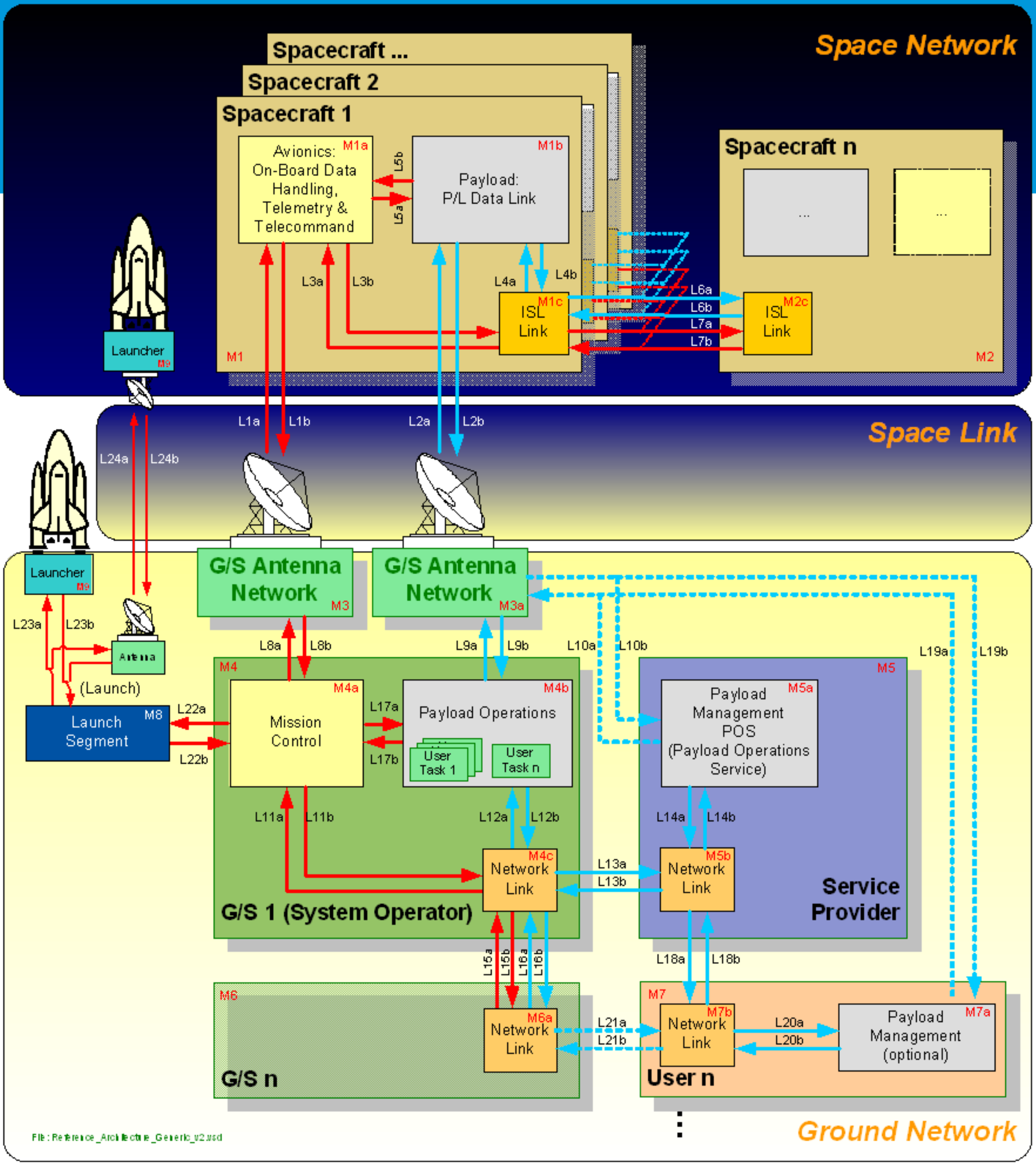
1. Main Threats:
    a. Unauthorized access to spacecraft control;
    b. Denial-of-service on command link;
    c. Traffic analysis.

2. Specific mission risk assessment will dictate the adoption of Protection measures like:
    a. Command authentication;
    b. Command and telemetry encryption;
    c. Anti-jam techniques (e.g. cryptographic spread spectrum, antenna null-steering);
    d. Spacecraft autonomy, ground station diversity.

Mission products protection

1. Main Threats:
   a. Unauthorized access to mission data or mission signal on space link;
   b. Unauthorized access to mission processed data at payload data ground segment.

2. Protection measures:
   a. Mission data encryption on space link; decryption keys distributed to authorized users;
   b. User identification, authentication, access control, encryption when interacting with payload data ground segment for mission processed data.



Space Network

Spacecraft ...

Spacecraft 2

Spacecraft 1

Avionics: On-Board Data Handling, Telemetry & Telecommand M1a

Payload: P/L Data Link M1b

ISL Link M1c

M1

Spacecraft n

...

...

ISL Link M2c

M2

Launcher M9

Space Link

G/S Antenna Network M3

G/S Antenna Network M3a

Launcher M9

Antenna

(Launch)

Launch Segment M8

M4

Mission Control M4a

Payload Operations M4b

User Task 1

User Task n

Network Link M4c

G/S 1 (System Operator)

M5

Payload Management POS (Payload Operations Service) M5a

Network Link M5b

Service Provider

M6

Network Link M6a

G/S n

M7

Network Link M7b

Payload Management (optional) M7a

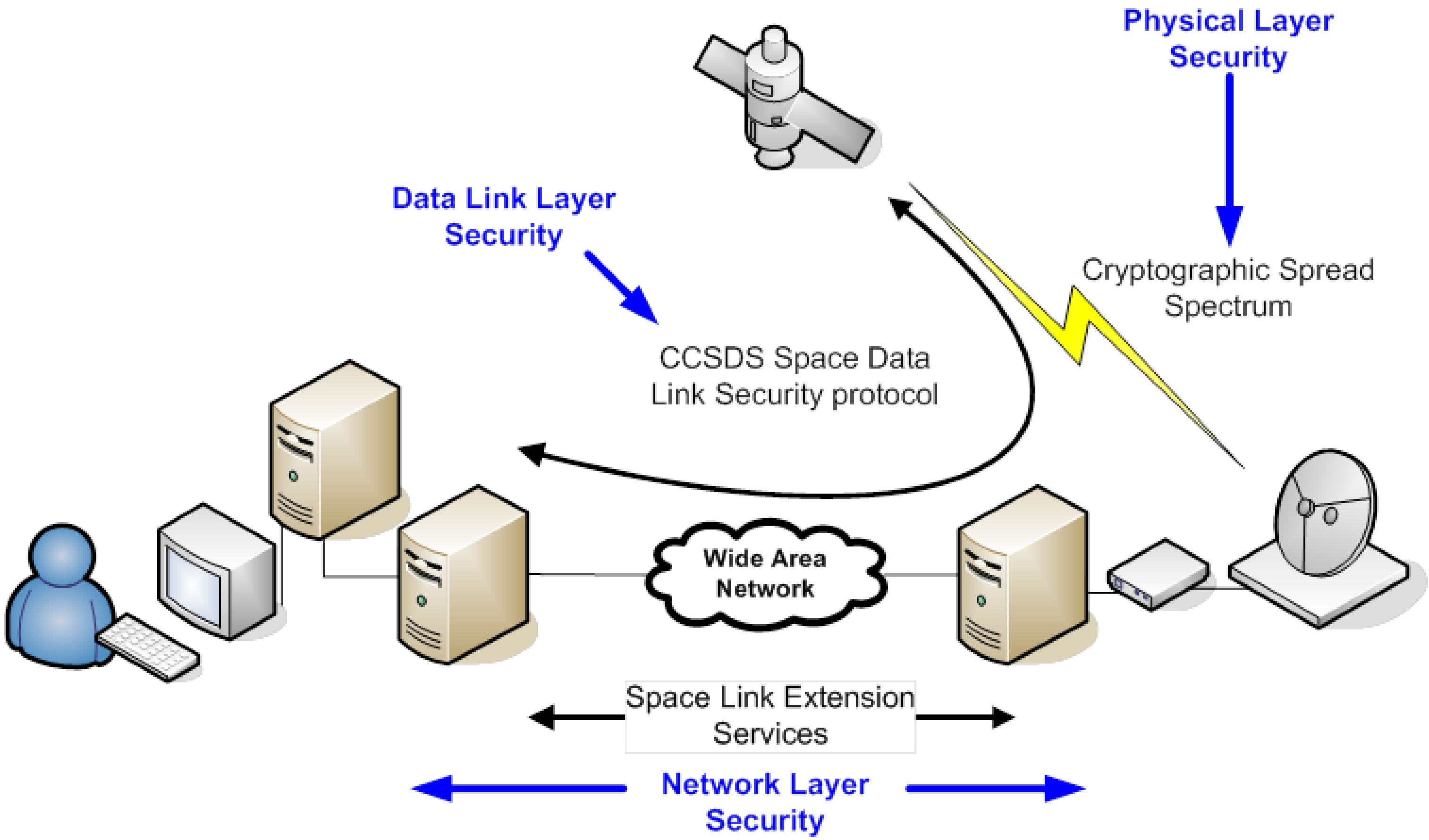
User n

⋮

Ground Network

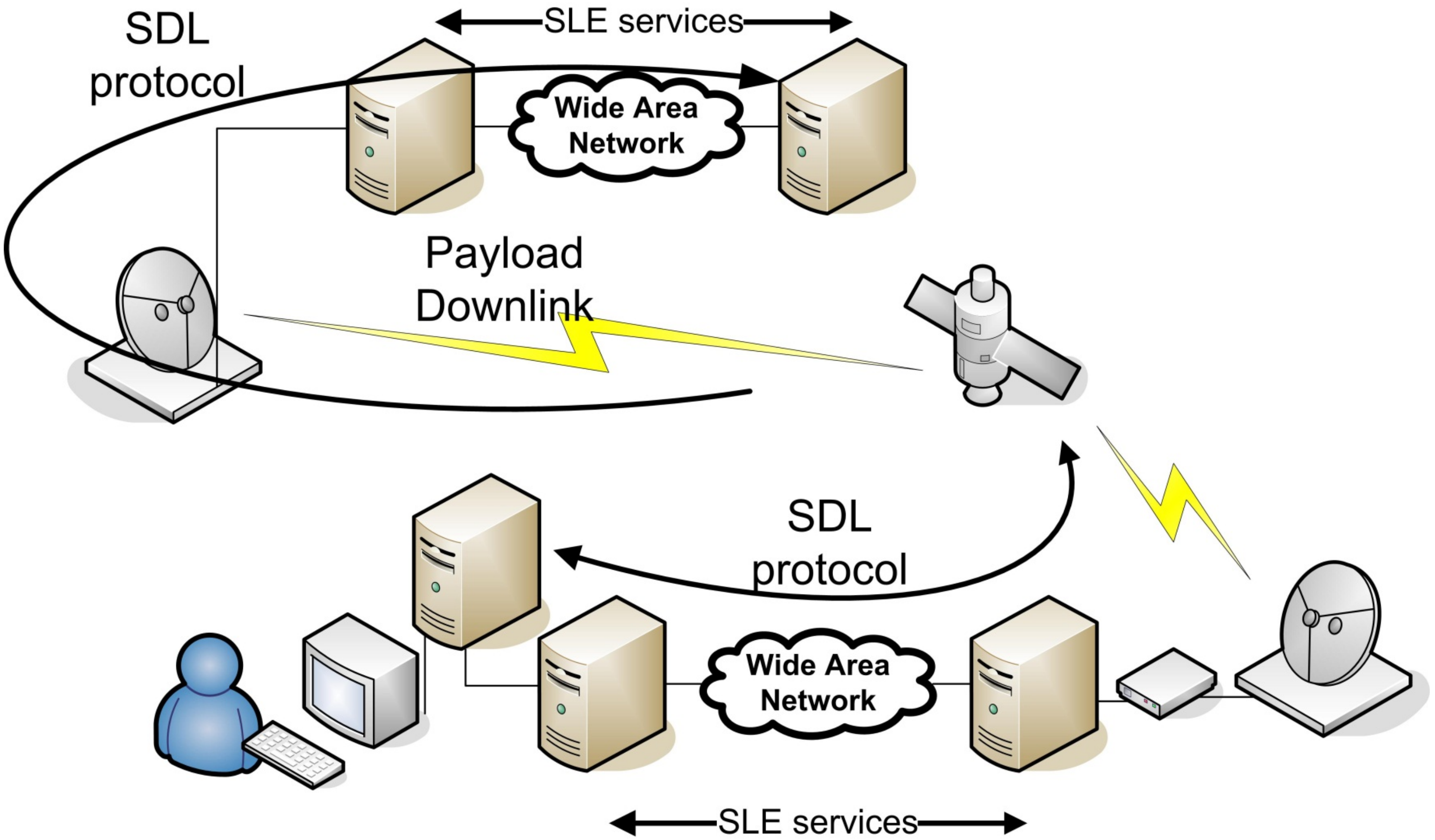
File: Reference_Architecture_Generic_v2.vsd

Spacecraft end-to-end security (1)
Single space link topology


Physical Layer Security
Data Link Layer Security
Cryptographic Spread Spectrum
CCSDS Space Data Link Security protocol
Wide Area Network
Space Link Extension Services
Network Layer Security

ESA UNCLASSIFIED – For Official Use

Spacecraft end-to-end security (2)
Separate payload link topology



Spacecraft security services implementation (1)

1. Typical implementation for spacecraft security services and key management is based on hardware.
   a. Quality and reliability are critical.
   b. Choice of technology is driven by those two plus complexity and non-recurrent cost.
   c. Integration with other spacecraft data handling functions is possible. ASIC could be favoured.

2. For the ground counterpart implementation can be based on software.

Spacecraft security services implementation (2)

3. Security evaluation needs may call for a physically segregated security module/unit.
    a. Decouples most of spacecraft integration and testing activities from security function evaluation and testing.
    b. Still a later integration/end-to-end connectivity test with ‘flight keys’ is required.

4. Secure partitioning, a software based concept inherited from aeronautical industry, is being considered for future implementation of security functions at low data rate.
    a. One virtual machine among many running on a common processor will implement security functions;
    b. Security assurance, i.e. no data leakage between virtual machines, is critical.

ISSUES, CONCERNS, CONSTRAINTS AND REQUIREMENTS

Payload vs. platform space links

1. Platform links support spacecraft operation control and monitoring.
   a. Telecommand and Housekeeping telemetry are typically channeled through a particular radio link.
   b. The data rate requirements are generally modest, with telecommand of the order of a few kbps and telemetry slightly higher to tens or few hundreds of kbps.

2. Payload links are used to download instrument data.
   a. For very large volumes of data, as generated by optical instruments or microwave radars, a separate radio link is typically used.
   b. Data rates can range to several hundreds of Mbps and are expected to reach close to 2 Gbps and possibly up to 6 Gbps in future space missions.
   c. The volume of data to be secured is potentially much, much larger than for spacecraft platform data links.

3. Two separate security functions with different operational concepts in terms of cryptographic key management will continue to be required.
   a. Note that the platform security function provides a secure channel for the control and monitoring of the payload security function. Among other things this channel supports cryptographic key management.

Telecommand vs. telemetry links (1)

1. The telecommand link communicates the commands to the spacecraft.
    a. The most critical space link for the spacecraft protection as an asset.
    b. Thus, telecommand security is a first priority in securing space missions.
        - Authentication service applied to spacecraft telecommand frames provides the assurance that the spacecraft (space asset) can only be controlled/ commanded by an authorised control centre. In other words, the spacecraft would reject commands that cannot be validated to originate from a genuine source.
2. In addition, certain telecommands will require that the data they contain is encrypted.
    a. In order to support over-the-air-rekeying (OTAR), telecommands with encrypted packet data field will be used to upload new session (or traffic) keys.
3. Some missions may want to avoid eavesdropping of their telecommand.
    a. All telecommands will be encrypted at frame level.

Telecommand vs. telemetry links (2)

4. In contrast to telecommanding, telemetry links are most concerned by the second security problem: protecting the data generated by the spacecraft.
    a. The priority is to make sure that only those entities which are authorized to read the telemetry data can actually do this.
    b. The confidentiality service, based on encryption, coupled with a proper encryption/decryption key management/distribution concept will provide such assurance.
    c. Depending on the telemetry distribution mechanism of the particular mission, key management may pose a complex problem.
5. In line with CCSDS, in order to protect against undetected data manipulation, we recommend for space missions the use of the authenticated confidentiality service.
    a. This service employs an authenticated encryption algorithm.

Limited or absent in-flight maintenance capability (1)

1. Once spacecraft data processing functions are implemented, validated, tested, and the spacecraft is launched, it is not possible to perform maintenance tasks in flight (exception for on-board software).
    a. The security function, which is a data processing function, has to be conceived to be robust and reliable with no allowance for failure or degradation of the security level provided.

2. Cryptographic techniques and attacks progress with time and technology improvements in the 'ground' (e.g., computing power).
    a. Cryptographic solutions planned to be embarked in long-term space missions require to be effective until the end of life of the space mission or beyond.
    b. Usually mission lifetime is extended beyond the initially planned duration.

3. Example: an advanced telecommunications satellite may remain operational up to 15 years in orbit. Depending on the maturity of the technology, 4 or 5 years before the launch the security function design may have been established. The manufacturer will plan to use such product for a number of years, maybe 5 to 10 years.

4. Space missions can easily take 'security' commitments that could last 20 to 30 years.

Limited or absent in-flight maintenance capability (2)

1. We currently address this issue with substantial ‘margins’, if one can say so in the security domain, in defining the security functions.
    a. Longer MACs and longer cryptographic keys than are actually required as a result of the attack models are employed.
    b. More keys than initially anticipated are embarked and planned for. The view is that one can adjust (reduce) the cryptographic period of critical keys according to time (date). However, it is clear that the protection resulting from this approach is limited to evolution of computational capacities as described by Moore’s Law.
    c. But margins cannot protect against a total breach of the cryptographic algorithm, i.e. by discovering a flaw in one of its processing functions or if it is discovered that certain keys are insecure.

Limited scope for side channels

1. As long as the security function design, development, qualification and testing is ensured in a controlled manner, there is no need for side channel attack protection for the implemented spacecraft security functions.
2. Human beings cannot (within effort that could be considered feasible) access flying spacecraft (astronauts are an exception!).
3. Flight cryptographic keys are injected shortly before launch under a secure procedure so their exposure before flight is very limited.
4. However, the same cannot be said for the corresponding implemented security function in the ground segment in charge of the mentioned spacecraft.
5. Thus, while not a priority for flight units, <u>it might still be interesting to protect ground cryptographic units against side-channel attacks</u>.
    a. Note: access to cryptographic units will be generally controlled and protected. Having said that, the scope for insider attack is always a possibility. And defence-in-depth philosophy is very much liked in space system security engineering.

Unique crypto-period

1. Spacecraft operations are complex, delicate and rely on a long tradition of proven approaches and concepts. The arrival of security functions and cryptography to civilian space missions has been met with reluctance by stakeholders, developers and operators. As any novel ‘thing’ in space mission engineering it is perceived as a potential ‘troublemaker’.
2. Therefore, it is crucial that proposed security functions and concepts are easy to operate, reliable and predictable.
3. Maintaining effective security and in particular valid cryptographic keys is a new operational burden for spacecraft operators although some telecommunication satellite operators have already some experience. The simpler it is, the better for its acceptability.
4. In considering the combination of authentication and encryption, an ideal design should provide similar crypto-period for both authentication and encryption. One could even explore the possibility to share the length of the cryptographic material between authentication and encryption such that this is achieved. Imagine for instance having 512 bits of an ‘equivalent’ authenticated encryption key to be shared. Perhaps one could find that say 128 bits for encryption and 394 bits for authentication achieve that result. Flexibility in apportioning these values considering the specifics of a particular mission context could be valuable.

Flexible MAC length

1. In applications like telemetry protection, the additional overhead incurred by including a MAC in a frame is acceptable given the generally long length of the frames (a few thousand octets).
   a. Hence, exploiting the theoretically possible longest MAC given a cryptographic key length is possible.

2. In contrast, in applications like telecommand protection where the message to be protected, a TC transfer frame, has variable length ranging from 64 bits up to 1024 octets, the pressure to reduce overhead to the strictly minimal to guarantee security may win the day.
   a. Short telecommand frames, also called High-Priority Commands (HPCs) are essential in off-nominal conditions to recover space missions.
   b. Communications may be extremely unreliable (e.g. tumbling spacecraft, no telemetry, blind commanding).
   c. In such conditions short messages have higher chances to be received than long messages. These messages could contain just a single HPC. Short MACs and frequent rekeying may be preferred.

3. However, given the long duration of space mission development and operational lifetime, a provision to increase such MAC length with time could be attractive to some extent.
   a. For instance a mission may initially fly with a 128 bit MAC and evolve with time to longer value like 196 bit or longer.

Intermittent contact and latency

1. In some space missions radio contact can only be established for short period of times.
    a. Typical example is the so-called Low Earth Orbit (LEO) Earth Observation missions where once per orbit a period of about six to twelve minutes is available to exchange data with a ground station.
    b. The particular contact times/duration depend very much on the orbital parameters of the mission, the available ground stations to communicate with the spacecraft and the spacecraft –ground station geometry for a particular pass.

2. However, in other cases such as missions with geostationary orbits, the contact time may be continuous.
    a. This offers more scope for attacks directly to the spacecraft but also more monitoring capability by the legal space mission operator.

3. For deep space missions, the data latency is substantial.
    a. This is particularly relevant for communication protocols that include re-transmission loops.
    b. However, deep space missions are so far not particularly troubled by security issues, maybe at their own peril! After all, as any other space mission deep space missions include the so-called launch and early orbit operation (LEOP), which follows the launch phase and is particularly critical for all space missions.

Anti-replay

1. Protection against replay attacks is a mandatory requirement for space mission telecommand when implementing authentication or authenticated encryption.
    a. A replay attack consists on recording a previously sent telecommand and up-link it with the intention of having it executed.
    b. The usual protection approach is to include a time-dependent information element, generally a counter value, as part of the message to be authenticated.

2. In contrast, anti-replay is not perceived as critical for telemetry in civilian space missions.
    a. The generation of rogue telemetry and reception by a ground station without raising suspicion to the operators is a very difficult proposition.
        - The TM spoofer would need to make sure to replicate certain analogue signal performances like the Doppler and amplitude profile, typical of a pass, experienced by the ground station receivers.
        - Those receivers are coupled to very directive antennas, whose maximum gain is limited to a very small solid angle of their radiation pattern and whose pointing is often controlled by the received RF signal (auto-tracking) or by a program based on the predicted azimuth and elevation parameters for the pass.
    b. For certain very high data rate TM downlinks, due to both the very high data rate and antenna directivity, it becomes even harder.

Operation both in connection and connectionless protocols

1. In designing security for space link protocols a central consideration has been the compatibility with communication scenarios where there is no guarantee of repetition, omission or sequence in a group of messages.
2. Unfortunately, in off-nominal conditions telecommand to a spacecraft may be carried out in a ‘blind’ mode, that is, without telemetry to supervise spacecraft operation and in particular re-transmission mechanisms inherent to the sequence-controlled service offered in nominal condition.
3. Because of these two scenarios the adopted approach has been to rely on sequence counters with some flexibility in the values that can be accepted by the receiving processor.

Graceful transition from secure to clear mode

1. Given the prevalence of safety over security in civilian space missions, the demand of a so-called CLEAR mode, which implies bypassing the security functions, is a must.
2. Passing from authenticated encryption to authentication only to clear mode could be a new transition model between SECURE and CLEAR modes.
    a. It is unclear, though, to what extent such property could be attractive.
    b. Certainly being able to maintain always authentication in applications like telecommand could provide an advantage in avoiding periods in which a spacecraft is vulnerable to unauthorized telecommand.

Forensic analysis of secure data

1. It is anticipated the possible need to be able to decrypt telemetry frames totally or partially even if they cannot be authenticated.
   1. Failure analysis. Example: the last US Space Shuttle Columbia required investigators to be able to extract meaningful data from telemetry frames initially rejected by frame processors given they contained too many symbol errors but partially recovered afterwards.
2. Certain cryptographic algorithms/modes limit the error propagation caused by communication channel errors (e.g. CTR).
   1. To maintain such limited error propagation will be desirable for future cryptographic algorithms/modes used in space communications.
3. Nevertheless, the ability to extract some meaningful data from noisy data may be at odds with attempting to secure the data in the first place.
   1. Unfortunately, the trade-off between safety and security is recurrent in many a space mission design, development and operations concept.
   2. No valid answer or general recipe has been found so far. What experience has shown is that civilian space missions tend to privilege safety over security.

High number of invocations with a given key

1. In space missions, cryptographic keys are limited resources. As a consequence cryptographic keys should be used in the most efficient manner.
    a. Current cryptographic key management concepts for simple space mission network topology rely on Symmetric Key Infrastructures (SKIs).
    b. A limited number of static keys, so called Master keys, are pre-loaded with PROM/EEPROM before a spacecraft is launched.
    c. Those Master keys can be used as Key Encryption Keys (KEKs) to support the secure transfer from ground to space of Session keys (or Traffic keys), which are actually used to secure the data transmitted on the space links.
2. Agencies like ESA are researching symmetric key infrastructures for space missions with particular research action, aimed to optimize the number of master and session keys considering the particular mission constraints.

Arrangement of encryption and authentication operations

1. From our understanding, there are several ways in which encryption and authentication operations can be combined:
   a. authenticate-then-encrypt,
   b. authenticate-and-encrypt,
   c. encrypt-then-authenticate.
2. Our preference, in line with the conclusions highlighted by cryptographic research, has been encrypt-then-mac. AES GCM fulfils that order of operations. AES CCM does not. Mainly for this reason, AES GCM has been considered more secure and, therefore, preferred for CCSDS standardization.

CONCLUSION

Space agencies rely on the civilian cryptography research community and standardization bodies to develop advanced cryptographic algorithms for their future civilian space missions. This white paper has briefly addressed a number of topics considered relevant for the evolution of cryptographic algorithms, in particular authenticated encryption, used to implement security services on space communications links supporting space mission operations. It is hoped that such paper will provide further input to stimulate cryptographic research.