SDLS SLP (TC) Interaction Issues

Aguilar, Calzolari, Delandelong, Fischer
ESTEC
12/03/2013

Outline

- Background
- Attack Case
- SDLS Problem Case
- Undetected Error
- Looking at similar problems
- Some relevant facts and thoughts
- SDLS Status Information
- Manual vs. Automated Intervention
- Some very preliminary conclusions
- Follow-on

Background (1)

- SDLS Red Book is pretty mature. SDLS and SLPs are being integrated at logical and editorial (Books) levels. SDLS is now almost 'officially' an optional add-on function of SLP.

- Between November 2012 and January 2013, two key issues were identified by ESA and e-mails circulated concerning:
    1. SDLS Security Association (SA) with more than one Virtual Channel (VC) and placement of Interface between Space Link Protocols (SLPs) and SDLS.
    2. SDLS Security Failure Report.

- Issue 2 above included the following questions:
    - which kind of failures?
    - which kind of report?
    - destination of the report?
    - action as a result of the report?

Background (2) & Trigger for this telecon

- Concerning previous four questions and responses given so far, E. Greenberg sent a short e-mail to G. Moury on 5/12/2013 with following text:
  - *I have a simple question. Should there be a flag for the COP if the frame is rejected by security after it was accepted by the COP*.

- This e-mail triggered some additional interactions and the need for further analysis and in particular this telecon. Key points of concern:
  - Distinction (or not) between communications and security failures,
  - Actions at both SDLS and SLP as well as
  - Possible interaction between SLP (COP) and SDLS.

- How could this *failure* condition occur? This *failure* could be caused by:
  - an attack;
  - a problem with SDLS (e.g. wrong key, wrong SA, wrong AR);
  - an undetected error;
  - other?

- Of particular importance is the second case. The operator needs to understand what happens (status of on-board and ground processors), why (causes) and what to do next (recovery actions).

- The three cases are discussed in following slides.

Attack Case

- It is essential to understand the possible attack scenarios and in particular if the legal operator can at least infer **whether or not** the satellite has been subject to attack.

- The reception of a *CLCW* with indications of *RF Lock* and *Bit Lock* would indicate a carrier with data modulation has been locked to at least one of the on-board TC receivers (and bit synchronizers).

- If the legal operator knows the current status of its uplink carriers (human error excluded!) he/she can reach the following conclusions:
  - His/her carriers are OFF--> spacecraft under attack;
  - His/her carriers are ON --> doubt; requires additional information, e.g. at the data link layer.

- Maybe the TC carrier of the attacker has overpowered the carrier of the legal operator. Hopefully if SDLS is working properly the legal operator, although incapable to command, would see rejection by SDLS of all the rogue TC frames. How? By reading a piece of information referring to the status of the on-board SDLS processor and/or the received TC frames.
  - For instance the Anti-replay count of relevant SAs not incrementing!

SDLS Problem Case

- Root causes include those related to misalignment in the configuration of relevant parameters of the SDLS ground and on-board processors. There can be at least the following:
  - Invalid SPI, which in turns subdivides on
    - Not-instantiated SPI
    - Associated SA not active
    - Associated SA active but not valid for the VC/MAP used;
  - wrong AR counter value;
  - wrong cryptographic key.

- In TC it is essential for the Ground to obtain reliable and timely information about the state of the SDLS protocol processor (function) on-board. Obviously the Ground can easily obtain information about the Ground processor.

- Assuming there is an operating TM link, the relevant SDLS information could be downlinked.

- In a similar case as the CLCW for the COP, such information could be 'exploited' by both the TC SLP and the SDLS protocol processors to enable or disable certain actions like TC frame uplink.

- There could be as well failures affecting the SDLS HW/SW implementation on-board and/or in ground leading to misalignment or simply failure to process.

Undetected error

- This case has already been analysed as part of SDLS development.
- There is an admittedly rather small likelihood that a TC frame declared as valid still contains undetected error.
  - Because of the superior performance of a MAC in detecting data integrity, SDLS could fail verification whereas TC SLP declared the frame as valid.
- However, the chances of this event occurring are so small for a given mission (see past analysis for instance in *IEEE 2012 Aerospace Conference Paper*) that no special measures were deemed necessary.
- Can the mission identify this event?
  - It is likely to happen only once, leading to a packet loss;
  - Use of the optional Packet CRC may allow to detect it;
  - Monitoring of packet counters at application layer is likely to help.
- Note as well that without SDLS the chance for an undetected error event is already present on missions using TC SLP. The application would receive data with undetected error at the transmission level. But the application may have means as mentioned above to detect such event.

Looking at similar problems (1): PLOP

- The Physical Layer Operations Procedure (**PLOP)** case
  - It would seem important to ensure that the TC receiver is locked before up-linking TC frames.
  - At least in *Sequence Controlled Service* it would seem necessary to check that the TC receiver is well locked before up-linking.
    - In *Expedited Service* there might not be a TM link; no check should be needed.

- This is a somewhat similar interaction between a protocol and TC SLP. Thus, it could be useful to see how CCSDS has treated this case.

Looking at similar problems (2): PLOP

- The CCSDS document covering the PLOP-1 and PLOP-2 is the *TC S&C Blue Book* (231.0-B-2).
  - Concerning the definition of the *'No RF Available*' and the *'No Bit Lock'* flags CCSDS 232.0-B-2 implies the following:
    - No RF Available is mandatory and indicates whether the physical layer is ready to process frames;
    - No Bit Lock flag is optional;
    - Same note for both: "This field may be used by Agencies for local enhancements to operations of this protocol and is not part of the COP".

- Thus, the use of those two flags in the CLCW is left up to mission implementers. Based on the *TC S&C Blue Book* it appears that CCSDS was/is not prescriptive about establishing interaction between physical and data link layer procedures. The FOP-1 could exploit knowledge of the status of the *'No RF Available'* flag to avoid transmitting TC data but it does not.

Looking at similar problems (3): SLE FCLTU

- However, the CCSDS *SLE FCLTU Blue Book* (912.1-B-3) allows the user, if he/she wishes so, to establish such connection between physical and data link layer operations. Some relevant excerpts:
  - Page 2-4, *"Based on the values in the CLCWs, the Forward CLTU service determines whether the physical channel is available"*.
  - Page 2-15, "*The provider monitors equipment readiness, the status of the physical channel and (when configured to do so) the uplink status. When production status changes to operational' the provider sends CLTU-ASYNC-NOTIFY to the user*".
  - Table 3-11,

Parameter	Description
bit-lock-required	If the value is 'yes', the 'No bit lock' flag in the CLCW must be false in order for the provider to set production-status to 'operational'.
rf-available-required	If the value is 'yes', the 'No RF available' flag in the CLCW must be false in order for the provider to set production-status to 'operational'.

Some preliminary thoughts

- It appears, therefore, that within CCSDS, it is at an *SLE Book* and not at the *SLS Protocol Books* the place where such expected interaction is well taken into account.
  - Does this point towards an ‘integration’ of SDLS within the relevant SLE Books?
  - It would make (a lot of) sense but first we should identify and define the SDLS reports and mechanisms for their transport to Ground.
    - *SDLS Extended Procedures* may have to tackle in-depth the SLE interface.
      - The approach could be similar to the one discussed in previous slides.

Looking at similar problems (4): The 'Wait' mechanism

- The *'Wait'* mechanism is used by the *FARM-1* to inform the *FOP-1* that the on-board system does not have enough resources to process the incoming data.
  - Understood to be a precaution of the past, aimed to cope with the processing performance of on-board data handling electronics of first avionics implementing FARM-1.
  - Nowadays in a properly designed on-board data handling system the processor cope with no 'waits' with all incoming data stream and keep frames flowing at highest throughput.

- Conclusion: **not relevant**.

Some relevant facts and thoughts (1)

- Distinction between SLP and SDLS objectives:
  - SLP takes care of data *transmission*;
  - SDLS takes care of data *security*.

- The COP is a *re-transmission mechanism* of the TC SLP aimed to guarantee delivery and maintain sequence (no omissions, no repetitions, sequence order) of received TC frames for the VC that is applying Sequence-Controlled Service.
  - Highest quality of data transmission;
  - Almost no business with security (only data integrity protection against random errors).

Some relevant facts and thoughts (2)

- Failure Modes of SLP and SDLS are expected to be different. Failure detection, isolation and recovery as well.

- Protection against attacks is the business of SDLS. Are attacks to be treated as failures? Some very similar analysis techniques although very different initial events (threats vs. random failures).
  - When SDLS stops a rogue TC frame or a frame with undetected error it is NOT failing; it is working!
    - So both opening the gate for the good guys and closing it for the bad guys (assumes Authentication presence!) is part of the job of SDLS.
  - If the opposite occurs then SDLS would be failing.

- Selecting the add-on SDLS for a mission means one is giving data security a high priority among the services provided by SLP.
  - Ready to accept some consequences.

- Forcing interaction beyond what is unavoidable (functional interface) may lead to a more complex and less reliable SLP.
  - Keep separation of data transmission and security jobs as much as feasible!
  - Try thoroughly this approach first.

SDLS Report on Status Information (1)

- Which information?
- Who needs this status information and for what purpose?
- How will it be transported from source to destination?

  - For this discussion one has to differentiate between the status of the SDLS processor and of the received TC frame.
    - A priori the status of the SDLS processor appears more important. Need to sync and re-sync according to physical and data link operations. Several sync parameters (e.g. SA/SPI, cryptographic key(s), anti-replay count).
    - Furthermore, it seems difficult to be able to map an SDLS TC frame rejection with a given TC frame.
  - Certain parallelism with CLCW is unavoidable.

SDLS Report on Status Information (2)

- Who needs this status information and for what purpose?
  - In a TC scenario, the '*Master*' (i.e. the Ground) needs information about the status of the SDLS protocol processor on-board (in addition to the status of the SLP processor on-board which is given with the CLCW).
    - Reporting AR number, SA (VC?), last validated TC frame, Key ID?

    Purpose: Decide between attack or something else. Take action accordingly.
  - Between SLP and SDLS processors on-board;
    - FARM requiring some information from SDLS?
      - Perhaps if for instance unused flags of CLCW were to be used to support SDLS status reporting.
      - However, this does not mean an entry to the state machine but rather the exploitation of unused flags during CLCW generation (out of the state machine).
        - Similar to what is done to integrate the physical layer flags into the CLCW.

SDLS Report on Status Information (3)

- Who needs this status information and for what purpose (cont'd)?
  - Between SLP and SDLS processors in Ground.
    - FOP requiring information from SDLS?
      - See previous discussion on SLE integration. Tackle the interaction at SLE rather than at SLP.
    - *SLE FSP Service Specification* (912.3-B-2) mentions FOP.
      - Page 2-3: "For each VC, one service instance can invoke Frame Operation Procedure (FOP) directives, even though FOP directives will in general affect multiple service instances. Some FOP directives also affect the space element and are therefore regarded to be integral part of a telecommand service and not part of the management of such service".

SDLS Status Information (4)

- How will it be transported from source to destination?
  - Between space and ground:
    - Question already formulated and preliminarily discussed at last CCSDS Fall Meeting.
    - General options ranging from exploiting existing PDUs (e.g. unused flags in CLCW) to creating a new PDU at data link layer or application layer.
    - Recommended to tackle this question on *Extended Procedures* work.
  - Other cases (between SDLS and SLP either on-board or in ground) already covered with Core SDLS update.

Manual vs. Automated Intervention

- Security (Authentication) failures are by definition **not recoverable without human intervention**.
  - *Good guy* frame rejected;
  - *Bad guy* frame accepted (!!).

- Could we at least aim to automate part of the SLP response in case of SDLS anomalous behavior?
  - At least block up-link transmission on ground until SDLS problem solved?
    - **NO**. The SLP can multiplex TC control and data frames on different VCs and with different Service (Expedited, Sequence-Controlled), with and without security. There is no apparent reason to stop **legal** TC frame up-link.

- Distinguish between nominal and off-nominal, with and without a telemetry link.
  - Without a TM link we surely want to be able to uplink whenever is convenient. No stops.

Some very preliminary conclusions

- SDLS is an enhancement of the SLPs. Thus, it would seem natural that there is more integration between SDLS and SLP standard than between two CCSDS protocols at different layers.
  - However, fundamentally different objectives and behavior.
- Keep separation of SLP and SDLS as much as feasible.
  - Avoid interaction SDLS-COP.
  - Treat anomalies, failures, attacks and the like separately.
- SLE is currently the place in CCSDS where both physical and data link layer management/operations converge.
  - SDLS to follow this path?
- Classification of issues/actions according to groups (see follow-on slides). Take into account limited resources and the need to close the Red Book!

Follow-on (1)
SDLS Core Protocol

- Document interaction between SDLS and SLP only at functional level.
  - Identify and define well the required SDLS reports (almost done);
    - destination is SLP interface (nothing else!).
  - Defer further processing of SDLS reports to
    - SLP (towards user) and
    - SDLS Extended Procedures

Follow-on (2)
Green Book

- Introduce protocol as an optional function.
  - Explain that the protocol is in general compatible with SLPs but
  - Emphasize its objectives and its expected behaviour in contrast to SLP.
- Discuss some scenarios with interaction between TC SLP and SDLS.
  - Address briefly some possible events like the SDLS frame rejection (whereas no transmission/reception problem).

Follow-on (3)
SLP Books

- Recommend to define interaction with user caused by SDLS.
  - Cover the SDLS *failed frame verification* only (frame rejected by SDLS)

Follow-on (4)
Extended Procedures

- Investigate carefully the ground-space interaction (e.g. reports on both sides, actions on both sides, contingencies, attacks, management).
  - Failure analyses:
    - Legal frame rejected;
    - Successful attacks? Vulnerabilities?
  - Attack detection;
  - SDLS Reports;
  - Transport mechanism for SDLS Reports.
- Prepare ourselves for a future interaction/integration of SDLS into the SLE world where actual management of space links is taking place. **Not a minor task**.
  - Consider how the physical and data link layer operations interact as possible model; see previous discussion on SLE FCLTU.

Follow-on (5)

- What do other protocols (e.g. IPSec, TLS) do in case of security event?
  - Anything we could learn?