Integration of Generic Data Security Features in the CCSDS Packet TM/TC Standards

Daniel Fischer (University of Luxembourg / ESA),
Thomas Engel (University of Luxembourg),
Mario Merri (ESA)

Ground System Architectures Workshop 2006
(GSAW 06)
Presentation Structure

- Introduction & Motivation
- Authentication Localization
- Confidentiality Localization
- Impact & Options
- Conclusions
Motivation

- Information security is an issue of growing importance in civilian space missions
  - More intensive use of open techniques and protocols
  - Reuse of mission infrastructures
- Most operational civilian space missions do not have any security implemented
  - An easy approach to introduce end-to-end security is required
  - High level of transparency desired
    - Only a small set of modifications to the existing infrastructure should be necessary
  - Short Term solution required
- Packet TM/TC protocol family as the most popular space link protocol suite should be the basis
Introduction of security features

- Two possible approaches to introduce security
  - Option 1: Switch to alternative, security supporting protocols e.g. SCPS
    - Security being an integral part of the design procedure
    - Migration process requires a huge effort
    - Migration means moving away from long-time proven legacy systems
    - Maybe a long term solution
  - Option 2: Modify protocol standards that are currently in use
    - For ESA this is mainly CCSDS Packet TM/TC protocol family
    - Many modifications can be kept transparent to the infrastructure
    - Short term solution and focus of this presentation
Kick-off

- CCSDS has published a green book on security (CCSDS 350.0-G-2)
  - Several options for security localization in Packet TM/TC are proposed and investigated in this presentation
- Physical Layer Security not an option for civilian missions
  - Completely prohibits the usage of supporting services
- Generic security standard for civilian space missions shall be developed
- Some guidelines:
  - Minimization of security related overhead
  - Complexity is the arch enemy of security
Security Requirements

- **Telecommand Authentication**
  - Authenticates telecommands to prevent malicious commands sent to the spacecraft by an attacker
  - Ensures integrity of telecommands

- **Confidentiality**
  - Confidentiality of payload telemetry
    - Ensure commercial exploitability of data
    - Ensure exclusive rights to recorded science data
  - Confidentiality of selected telecommands
    - Protect sensitive commands e.g. for key upload

- **Other requirements such as non-repudiation possible**
TC Authentication

- Provides both Telecommand authentication and integrity
- Requires additional authentication layer in TC stack
  - Introduction of an authentication field
    - Signature, Anti-Replay Counter and other fields

Overhead Calculation Example

- Modern secure hashing algorithms provide hashes with at least 160 bit
- Freshness information must not recycle during a keys lifetime \(\rightarrow\) at least 30-32 bit
- Together with some arbitrary fields we get an overhead of at least 200 bit (= 25 octets)
Possibilities (according to CCSDS green book):
- Data Link Layer (Option A - complete frame)
  - Protection of FARM-1 control commands (BC frames)
- Segmentation Layer (Option B)
  - Current ESA approach
  - MAP Ids provide a selective tool for segments

Authentication on packet level not applicable as it leaves too many vital data fields unprotected at lower layers
Signature Overhead Reduction

- Signature overhead is quite big especially for short telecommands
- Overhead reduction is desirable
- Various Techniques
  - Signature Truncation (e.g. from 160 to 96 bit)
    - Loss of security (Signature function gets more non-injective)
  - Direct TC encryption (if TC data structure is smaller than the signature)
    - Hashing function would increase length rather than reducing it
  - Usage of compression techniques may reduce length of TC data structure
Confidentiality

- Assuming usage of symmetric block ciphers
- Requires additional confidentiality layer in TM/TC stack
  - Introduction of a Security Header data field
  - Initialization Vector (IV) and other fields (e.g. key identifier) possible

- Overhead Calculation Examples
  - Block ciphers in CBC mode need an IV and padding (worst case: 2x block length)
  - Other header information may additionally increase overhead
  - If counter mode is used, the overhead is the length of the counter
    - Counter may be combined with a layer specific counter
Confidentiality Localization

- Situation more complex than with authentication
  - Application dependent
  - Impact on availability of services (e.g. SLE)

- Network Layer
  - Application driven (APID) encryption possible
  - Encryption of packet data field
  - Use Packet secondary header to make security transparent
  - Alternative: Use CCSDS encapsulation packet standard

<table>
<thead>
<tr>
<th>Packet Primary Header (6 octets)</th>
<th>Packet Security Header (N octets)</th>
<th>Encrypted Transfer Frame (variable)</th>
</tr>
</thead>
</table>

Encrypted Packet
Confidentiality Localization

- **Data Link Layer Option A**
  - High level of Security
  - No Transparency

<table>
<thead>
<tr>
<th>Transfer Frame Security Header (N octets)</th>
<th>Encrypted Transfer Frame (variable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option A encrypted Transfer Frame</td>
<td></td>
</tr>
</tbody>
</table>

- **Data Link Layer Option B**
  - TM: Full transparency through usage of secondary header
  - TC: Limited transparency but more availability then in Option A

<table>
<thead>
<tr>
<th>Transfer Frame Primary Header (5 octets)</th>
<th>Transfer Frame Security Header (N octets)</th>
<th>Encrypted Transfer Frame Data Field (variable)</th>
<th>Frame ECF (16 octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option B encrypted Transfer Frame</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Further Options

- Combined Authentication and Encryption
  - Merging Confidentiality and Authentication Layers
  - Special focus must lie on the cipher mode (Counter, CBC and other modes have weaknesses when used for providing integrity)
  - Reduction of overhead and complexity is achieved with this technique

- Payload Data Masses
  - Some science spacecrafts payload telemetry downlink may occupy huge bandwidths
  - Encryption must be parallelizable to be fast enough → Counter or other parallelizable modes required

- Combining space link security with ground data dissemination systems
  - End-to-End protection from spacecraft to customers
Data link layer encryption (both options) can have impact on the availability of SLE services

Cross Support Services must access relevant data fields to provide functionality

Traditional conflict between security and availability

Example situation: R-CF trying to access virtual channel information

Impact & Options

Cross Support Services

- Data link layer encryption (both options) can have impact on the availability of SLE services
- Cross Support Services must access relevant data fields to provide functionality
- Traditional conflict between security and availability
- Example situation: R-CF trying to access virtual channel information
Conclusion & Future Work

- Introduction of security to CCSDS TM/TC standards possible with justifiable effort
- A good trade-off between security and overhead can be found for both authentication and confidentiality
- Proper set of security standards eliminate the need for proprietary security solutions
  - Security Level classification required
- Future Work will focus on
  - Definition of a complete set of security protocol standards for ESA
  - Confidentiality and authentication overhead reduction
  - Emergency Commanding Solutions
Any Questions?

Thank You!