Command Encryption with the Advanced Multi-Mission Operations System (AMMOS)

Mike Pajevski
AMMOS Architect
AMMOS Cybersecurity Engineer

March 1, 2023
Topics

• Why AMMOS Command Encryption?
• What is AMMOS Command Encryption?
• Concept Diagram
• Internals & Interfaces
• Key Management
• Security Association Management
• Questions & Answers
Why AMMOS Command Encryption?

• Unauthorized commanding could jeopardize a mission, and nearby missions

• NASA now requiring command encryption
  • Announcements of Opportunity call out NASA-STD-1006A, Space System Protection Standard
  • Can tailor to accommodate nature of mission
    • *Deep space missions may choose to limit controls applied to the space link if certain controls (e.g., encryption and authentication) pose significant burden to operability or mission success, and if the threat to the space link is low*

• AMMOS Command Encryption provides a multi-mission software solution for NASA robotic missions
What is AMMOS Command Encryption?

• Part of the Advanced Multi-Mission Operations System (AMMOS) software
• Multi-mission software solution
  • NASA Class B (unmanned space)
  • Distributed under royalty-free licenses
  • Compiled/tested on RHEL 8
• Applies the CCSDS Blue Book standard Space Data Link Security (SDLS) protocol to Telecommand (TC) transfer frames
  • Frame layer security protocol that leaves headers and error correction field in the clear
  • C, Python, and REST interfaces
• Incorporates the “CryptoLib” SDLS implementation from NASA Independent Verification & Validation (IV&V)
AMMOS Command Encryption Capability*

Mission Planning & Sequencing

Crypto Keys (Project-Specific)

AMMOS KMC

Data-Level Crypto

FIPS 140 Validated Crypto Library

Command Encryption Processing

CCSDS SDLS 355.0-B-1

Mission Control System

Telecommand Frames with Command Encryption

Ground Station

Flight System

Mission Operations Center (MOC)

Command Data/Files without Command Encryption

Encrypted

Not Encrypted

Legend

New AMMOS Capability

Modified Existing AMMOS

Off-the-Shelf

No Change

Flight System

Plaintext

Ciphertext

Acronyms
CCSDS = Consultative Committee for Space Data Systems
FIPS = Federal Information Processing Standard
KMC = Key Management and Cryptography
SDLS = Space Data Link Security

*Multi-mission AMMOS capability that works not only with the AMMOS, but with other mission control systems too.
AMMOS Command Encryption Internals

- CCSDS SDLS is applied by CryptoLib
  - CryptoLib was developed by NASA IV&V
  - Now improved and maintained together with JPL/MGSS

Data-Level Cryptography
- Encrypt frame data
- Create authentication data
- Uses FIPS 140 validated cryptography library

AMMOS KMC Software

Legend
- Modified Existing AMMOS
- New AMMOS Capability
- NASA IV&V Software
- Off-the-Shelf (non-AMMOS)

Flight Project Key Management Capability
- Can use KMS and/or Keystore

Key Mgmt. Service (KMS)
- Keys (via KMIP)
- Keystore

Data-Level Cryptography

Command Encryption Processing

CryptoLib (SDLS Engine)

Security Association (SA) records
- SAs specify key, algorithm, anti-replay counter and other control info for applying/processing SDLS

Security Association Database (SADB)
- Tools provided for automated setup of software and database
- Managed via command line and Web browser user interface
AMMOS Command Encryption Interfaces

- AMMOS KMC provides C, Python and REST APIs for SDLS ApplySecurity and ProcessSecurity
  - SDLS REST API provided by KMC Crypto Service
- SDLS capabilities uses data-level crypto of Crypto Service
- Mariadb is used for SADB
Key Management

• Data-level crypto in KMC can use a Key Management Service (KMS) and/or PKCS-12 keystore
  • Interface to the KMS uses the Key Management Interoperability Protocol (KMIP) standard
  • KMS products can be used, but are not provided, by AMMOS
    • Commercial products are available
  • KMC includes a tool to import hex keys into a PKCS-12 keystore
  • Other tools for creating/updating keystores are available in the operating system and commercially available products

• Crypto keys are project-specific
  • Projects must follow institutional requirements, processes etc.
  • Projects must plan, implement, perform & audit key management
  • Understand available institutional support
AMMOS includes tools for managing command encryption “Security Associations (SAs)”

Web GUI

Command Line Interface (CLI)

Security Association (SA) specifies the crypto algorithm, crypto key, and SDLS options to use
Questions?
Backup

- Acronyms
- TC Transfer Frame with SDLS
- Relevant Resources
- Acknowledgements
- Additional Authors
## Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMMOS</td>
<td>Advanced Multi-Mission Operations System</td>
</tr>
<tr>
<td>ARC</td>
<td>Ames Research Center</td>
</tr>
<tr>
<td>CCSDS</td>
<td>Consultive Committee for Space Data Systems</td>
</tr>
<tr>
<td>CLI</td>
<td>Command Line Interface</td>
</tr>
<tr>
<td>DTN</td>
<td>Delay (or Disruption) Tolerant Networking</td>
</tr>
<tr>
<td>GSFC</td>
<td>Goddard Space Flight Center</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>ITOS</td>
<td>Integrated Test and Operations System</td>
</tr>
<tr>
<td>IV&amp;V</td>
<td>Independent Verification &amp; Validation</td>
</tr>
<tr>
<td>LTB</td>
<td>Lunar Trailblazer</td>
</tr>
<tr>
<td>MGSS</td>
<td>Multi-mission Ground Systems &amp; Services</td>
</tr>
<tr>
<td>NASA</td>
<td>National Aeronautics and Space Administration</td>
</tr>
<tr>
<td>RHEL</td>
<td>Red Hat Enterprise Linux</td>
</tr>
<tr>
<td>SA</td>
<td>Security Association</td>
</tr>
<tr>
<td>SADB</td>
<td>Security Association Database</td>
</tr>
<tr>
<td>SDLS</td>
<td>Space Data Link Security</td>
</tr>
<tr>
<td>SMD</td>
<td>Science Mission Directorate</td>
</tr>
<tr>
<td>TC</td>
<td>TeleCommand</td>
</tr>
<tr>
<td>vMMOC</td>
<td>Virtual Multi-Mission Operations Center</td>
</tr>
</tbody>
</table>
TC Transfer Frame With SDLS

- SDLS adds a Security Header and (if authentication is used) a Security Trailer.
  - Lengths are set by each project, and remain constant for a virtual channel
- SDLS (if encryption is used) encrypts the frame data (i.e., payload)
  - Error Correction Field (ECF) left in the clear
- Authentication (if used) is done for headers and (encrypted) payload
- SDLS has the following Security Types (i.e., crypto to perform):
  - Authentication, Encryption, and Authenticated Encryption (i.e., both)
  - Also a Plaintext type, with Security Header but no encryption/authentication
Relevant Resources

- Some relevant CCSDS documents are:

<table>
<thead>
<tr>
<th>Title and URL</th>
<th>Document Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Space Data Link Security Protocol (<a href="https://public.ccsds.org/Pubs/355x0b1.pdf">https://public.ccsds.org/Pubs/355x0b1.pdf</a>)</td>
<td>Blue Book 355.0-B-1</td>
</tr>
<tr>
<td>CCSDS Cryptographic Algorithms (<a href="https://public.ccsds.org/Pubs/352x0b2.pdf">https://public.ccsds.org/Pubs/352x0b2.pdf</a>)</td>
<td>Blue Book 352.0-B-2</td>
</tr>
<tr>
<td>The Application of Security to CCSDS Protocols (<a href="https://public.ccsds.org/Pubs/350x0g3.pdf">https://public.ccsds.org/Pubs/350x0g3.pdf</a>)</td>
<td>Green Book 350.0-G-3</td>
</tr>
<tr>
<td>CCSDS Space Data Link Security Protocol--Summary of Concept and Rationale (<a href="https://public.ccsds.org/Pubs/350x5g1.pdf">https://public.ccsds.org/Pubs/350x5g1.pdf</a>)</td>
<td>Green Book 350.5-G-1</td>
</tr>
</tbody>
</table>

- Also see the following relevant websites:
  - NASA AMMOS Website
    - https://ammos.nasa.gov
  - CCSDS Systems Engineering Area - Security Working Group (SEA-SEC) Home
    - https://cwe.ccsds.org/sea/default.aspx#_SEA-SEC
  - NASA IV&V CryptoLib GitHub Wiki
    - https://github.com/nasa/CryptoLib/wiki
Acknowledgements

- NASA Independent Verification & Validation (IV&V)
  - Developed CryptoLib and now jointly improves with JPL/MGSS
- Goddard Space Flight Center (GSFC)
  - Participated in design review, and continue to collaborate
  - virtual Multi-Mission Operations Center (vMMOC) integrated AMMOS Command Encryption with their Integrated Test and Operations System (ITOS)
- SunRISE and Lunar Trailblazer projects at JPL
  - First adopters of AMMOS Command Encryption
  - Demonstrated capability/interoperability in end-to-end testing
- VIPER project at NASA Ames Research Center (ARC)
  - Evaluating AMMOS Command Encryption for likely usage, and collaborating on necessary capabilities, interfaces, etc.
Additional Authors

• The following people are major contributors:
  • Ken Gieselman; AMMOS Application Security (ASEC) Task Manager and Systems Engineer, Jet Propulsion Laboratory, California Institute of Technology; kenneth.g.gieselman@jpl.nasa.gov; (818)354-1251
  • Kam Tso; CAM/KMC/SSM Software Developer, Jet Propulsion Laboratory, California Institute of Technology; kam.s.tso@jpl.nasa.gov; (626)390-9838
  • Ibraheem Saleh; KMC Software Developer; Jet Propulsion Laboratory, California Institute of Technology; ibraheem.y.saleh@jpl.nasa.gov; (626)517-3943
  • JP Pan; KMC Software Developer; Jet Propulsion Laboratory, California Institute of Technology; james.paul.j.pan@jpl.nasa.gov; (818)354-8739
  • Robert J. Brown; Software Developer; NASA Independent Verification and Validation (IV&V), Independent Test Capability (ITC) Team; robert.j.brown@nasa.gov
  • David C. Cutright; Software Developer; NASA Independent Verification and Validation (IV&V), Independent Test Capability (ITC) Team; david.c.cutright@nasa.gov
  • John P. Lucas; Computer Engineer; Deputy ITC Lead; NASA Independent Verification and Validation (IV&V), Independent Test Capability (ITC) Team; john.p.lucas@nasa.gov
  • Justin R. Morris; Computer Engineer, ITC Lead, NASA Independent Verification and Validation (IV&V), Independent Test Capability (ITC) Team; justin.r.morris@nasa.gov
  • Scott A. Zemerick, PhD; Systems Engineer, ITC Lead; NASA Independent Verification and Validation (IV&V), Independent Test Capability (ITC) Team; scott.a.zemerick@nasa.gov