CryptoLib Req.

Tuesday, January 3, 2023 1:14 PM

20240123 - Requirements

- What has CryptoLib set out to do?
  - Provide a software-only solution using the CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP) to secure communications between a spacecraft and a ground station.
- How are we going to do it?
  - Draft requirements
  - Select feature
  - Make it work
  - Create unit tests
  - Repeat
- Features
  - FSW integration
  - GSW integration
  - Standalone implementation
  - Unit tests
  - System tests
- Reference Breakdown
  - NASA-STD-1006A
    - 4.1 - Maintain Command Authority
      - Objective: Missions need to maintain command authority to prevent unauthorized access and to ensure data integrity. Unauthorized access could result in mission loss and/or damage to other space systems.
      - 4.1.1 - Command Stack Protection
        - **[SSPR 1] Programs/projects shall protect the command stack with encryption that meets or exceeds the Federal Information Processing Standard (FIPS) 140, Security Requirements for Cryptographic Modules, Level 1.**
      - 4.1.2 - Backup Command Link Protection
        - [SSPR 2] If a project uses an encrypted primary command link, and backup command link shall at a minimum, use authentication.
      - 4.1.3 - Command Link Critical Program/Project Information (CPI)
        - [SSPR 3] The program/project shall protect the confidentiality of command link CPI as controlled unclassified information (CUI) to prevent inadvertent disclosure to unauthorized parties.
    - 4.2 - Ensure Positioning, Navigation, and Timing (PNT) Resilience
      - Objective: Missions dependent on external PNT services need to be able to recognize and survive interference to ensure PNT resilience. Extended loss of PNT services could result in mission degradation or loss if no mitigations are available.
      - [SSPR 4] If project-external PNT services are required, projects shall ensure that systems are resilient to the complete loss of, or temporary interface with, external PNT services.
    - 4.3 - Report Unexplained Interference
      - Objective: Missions need to detect and report instances of unexplained interference to enable Agency awareness of the contested space environment and to develop appropriate mitigations. Lack of Agency awareness of unexplained interference events could deprive NASA of indications and warning of adversary actions and increase the vulnerability of NASA systems.
      - 4.3.1 - Interference Reporting
        - [SSPR 5] Projects/Spectrum Managers/Operations Centers shall report unexplained interference to MRPP or to other designated notifying organizations.
      - 4.3.2 - Interference Reporting Training
        - [SSPO 6] Projects/Spectrum Managers/Operations Centers shall conduct proficiency training for reporting unexplained interference.

- CCSDS Cryptographic Algorithms
  - CCSDS 352.0-B-2, Blue Book August 2019
    - "A single, symmetric encryption algorithm is recommended for use by all CCSDS missions. In addition, a specific mode of operation for the algorithm is also recommended"
    - 3.1 Algorithm and Mode
      - In order to achieve a minimum baseline all CCSDS missions shall use the Advanced Encryption Standard algorithm (reference [1]) for encryption.
    - 3.2 Cryptographic Key Size
      - Future CCSDS implementations (for missions whose planning begins after the publication of issue 2 of this specification) shall use a 256-bit key.
    - 3.3 Algorithm Mode of Operation
      - CCSDS implementations shall use Counter Mode (references [2], [3], and [4]). Other modes of operation are allowed but should be carefully considered before use.
    - 3.4 Authenticated Encryption
      - If encryption in combination with data integrity and origin authentication is required, implementations shall use Galois/Counter Mode (GCM) as specified in references [4] and [5] and [11].
      - The MAC 't' size shall be 128 bits.
    - 4.2.2 HMAC Hash Algorithm
      - CCSDS HMAC implementations shall use SHA as specified in FIPS 180-4 (reference [10]).
      - CCSDS HMAC implementations shall *normally* use the SHA-256 variant (reference [10]) as illustrated in RFC 6234 (reference [B20]).
      - CCSDS implementations *may use* alternative hash algorithms such as SHA-224 (reference [10]), SHA-384 (reference [10]), SHA-512 (reference [10]), or RIPEMD-160 (reference [B14]), among others, with the HMAC algorithm.
      - SHA-1 shall not be used.
      - CCSDS implementations should not truncate the length of the MAC resulting from HMAC.
    - 4.3 Cipher-Based Authentication
      - Except as noted in 4.3.2, the Cipher Based Message Authentication Code (CMAC— reference [9]) shall be used if a cipher-based MAC is employed.
        - The Galois Message Authentication Code (GMAC—reference [4]) may be used in place of CMAC when an authenticated encryption implementation is used for authentication only.
      - For future CCSDS implementations (for missions whose planning begins after the publication of issue 2 of this specification), CMAC shall use the AES algorithm using a 256- bit key size.
      - For existing CCSDS implementations, CMAC may use the AES algorithm using any of the following key sizes: 128-bit, 192-bit, or 256-bit.
    - 4.4 Digital Signature Based Authentication
      - Digital Signature Standard (DSS—reference [8]) shall be used when using digital signature technology.
      - The Rivest-Shamir-Adleman (RSA) Digital Signature Algorithm (PKCS #1 version 2.1 as referred to in reference [8]) should be used.
      - For future CCSDS implementations (for missions whose planning begins after the publication of issue 2 of this specification), the RSA Digital Signature Algorithm key length shall be 4096 bits.
      - For existing CCSDS implementations, the RSA Digital Signature Algorithm key length may be 2048 bits.
      - For spacecraft without the ability to contact a key server to obtain public keys, a public key cache can be pre-loaded prior to launch, or public keys may be uploaded after launch or when additional keys or updated keys need to be loaded. This is probably not an issue for ground systems which are assumed to have robust network communications and access to a Public Key Infrastructure (PKI) or Certificate Authority (CA) (reference [B22]).
  - CCSDS 352.9-G-2, Green Book July 2023
    - AES is the sole symmetric encryption algorithm that is recommended for use by all CCSDS missions and ground systems. Regarding the AES mode of operation, while other modes are allowed, the

Recommended Standard recommends that the AES Counter Mode be used. Legacy implementations may use 128-bit keys, but for future missions, a key length of 256 bits is recommended.

- 3.3 AES Modes of Operation
  - AES may be used in several modes of operation, such as Cipher-Block Chaining (CBC), Electronic Codebook (ECB), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR) (reference [5]). Each of these modes accomplishes the same objective, namely transforming plaintext data into ciphertext data.
    - ECB is considered to be extremely weak by the cryptographic community and should not be used
  - To summarize, it was concluded that counter mode would have the best performance for both TM and TC (reference [20]).
    - Counter mode requires the creation of a counter which does not have to be kept secret but must never repeat under the same key. If a counter is repeated, the confidentiality of the blocks encrypted under that counter may be compromised. If a counter overflows a new key must be used. Hence, proper counter management concept and implementation are crucial to counter mode security
- 3.4 Authenticated Encryption
  - Therefore while there is no requirement that the IV be random or unpredictable, the AES/GCM security requires that the counter be a nonce (i.e., each value used at most once under the same key). Additionally, it is also recommended that CCSDS AES/GCM mode implementations restrict the IV size to 96-bits to promote interoperability, efficiency, and simplicity of design.
  - In order to promote interoperability for the 96-bit IV, it is recommended that the deterministic construction be utilized, where the leading (i.e., leftmost) 32-bits of the IV hold a fixed field and the trailing (i.e., rightmost) 64-bits hold the invocation field. In principle, the fixed field should identify the context for the instance of the authenticated encryption function. The invocation field increments upon each invocation of the authenticated encryption function and could be implemented either as an integer counter or a linear feedback shift register driven by a primitive polynomial. To comply with the uniqueness requirement, for any given key, no two distinct devices are allowed to share the same fixed field and no two distinct sets of inputs to any single device are allowed to share the same invocation field.
  - A 96-bit IV is also recommended in Space Data Link Security Protocol—Extended Procedures (reference [21]). Specifically, the IV field length of the OTAR Command PDU, the Key Verification Reply PDU, and the TM, AOS, and USLP Security Associations is 96- bits.
- …

- CCSDS Space Data Link Security Protocol (SDLS)
  - CCSDS 355.0-B-2, Blue Book July 2022
    - Supported protocols
      - Telemetry (TM), CCSDS 132.0-B-3
      - Telecommand (TC), CCSDS 232.0-B-4
      - Advanced Orbiting Systems (AOS), CCSDS 732.0-B-4
      - Unified Space Data Link Protocol (USLP), CCSDS 732.1-B-2
    - Cryptographic Algorithms
      - CCSDS Cryptographic Algorithms, CCSDS 352.0-B-2
    - Security Protocol Entity
      - Apply security function
        - Flow
          - Select data for Transfer Frame Data Field
          - Construct a partial Transfer Frame
          - Call the apply security function for the frame
          - Complete the frame
        - Portion of the TC Transfer Frame contained in the TC_ApplySecurity payload includes an empty security header field

- Process security function
  - Flow - Same as above
- Security association
  - Defines cryptographic communications parameters to be used by both the sending and receiving ends of a communications session, and for maintaining state information for the duration of the session.
  - Defines a simplex (one-way), stateful cryptographic session for providing authentication, data integrity, replay protection, and/or data confidentiality
  - The Security Parameter Index (SPI) is a transmitted value that uniquely identifies the SA applicable to a Transfer Frame
    - The SPI can be considered as a table index key to an SA data base that stores all of the managed information required by each of the SAs on a physical channel
  - Once an SA is created, the lengths of the managed fields in the Security Header and Trailer are fixed for the duration of that SA
  - Both the sender and the receiver must create an SA, associate it with cryptographic key(s), and activate it before the SA may be used to secure Transfer Frames on a channel
- All transfer frames using an SA on a physical channel include a security header and trailer surrounding the frame data area of the transfer frame
  - Security header
    - Security Parameter Index (SPI)
    - Initialization Vector (IV)
    - Anti-Replay Sequence Number (ARSN)
    - Length of any block padding used (when necessary)
  - Security trailer
    - Message Authentication Code (MAC)
- **Annex A - Protocol Implementation Conformance Statement (PICS)**
  - **If it is claimed to conform to this Recommended Standard, the actual PICS proforma to be filled in by a supplier shall be technically equivalent to the text of the PICS proforma in this annex, and shall preserve the numbering/naming and ordering of the PICS proforma items. A PICS that conforms to this Recommended Standard shall be a conforming PICS proforma completed in accordance with the instructions for completion given in A2.**
    - Status Column
      - M = Mandatory (support if required).
      - O = Optional support is permitted for conformance to the standard. If implemented, it must conform to the specifications and restrictions contained in the standard. These restrictions may affect the optionality of other items.
      - O.*n* = The item is optional, but support of at least one of the options labeled with the same number *n* is mandatory. The definitions for the qualification statements used in this annex are written under the tables in which they appear.
      - C.*n* = The item is conditional (where *n* is the number that identified the applicable condition). The definitions for the conditional statements used in this annex are written under the tables in which they appear.
      - n/a = The item is not applicable.
    - Support Column
      - Y = Yes, the feature has been implemented
      - N = No, the feature has not been implemented
      - - = The item is not applicable
  - Created PICS OneNote page

- CCSDS Space Data Link Security Protocol - Extended Procedures (SDLS-EP)
  - CCSDS 355.1-B-1, Blue Book February 2020
    - 4 Interface with SLP & SDLS
      - The SDLS Extended Procedures are interfacing with the Space Link Protocols (SLP) for transport of the procedures Protocol Data Units (PDUs). This Recommended Standard mandates the SLP services be used for transfer of SDLS Extended Procedures PDUs over the space link. A new OCF, the FSR, is also specified to provide real-time reporting of the

Recipient security function to the Initiator. The SDLS Extended Procedures Concept of Operations (reference [C13]) describes various options to implement the interface.
        - Since the SDLS Extended Procedures are meant to provide additional capabilities to the core protocol, they do require interfacing with it. The interfaces are, however, generally on the Initiator and Recipient side, and not directly on SDLS protocol level. However, it is recommended that at least one Security Association be allocated for transporting Extended Procedures PDUs over the space link.
    - **Annex A - Protocol Implementation Conformance Statement (PICS)**
        - **To evaluate conformance of a particular implementation, it is necessary to have a statement of which capabilities and options have been implemented for a given protocol specification. Such a statement is called a Protocol Implementation Conformance Statement. This annex provides the PICS proforma for the Space Data Link Security Extended Procedures in compliance with the relevant requirements, and in accordance with the relevant guidance given in ISO/IEC 9646-7**
- CCSDS Space Data Link Security Protocol - Summary of Concept and Rationale
    - CCSDS 350.5-G-1, Green Book June 2018
- CCSDS Symmetric Key Management
    - CCSDS 354.0-R-2, Red Book February 2022

20230103 - Requirements

Thinking solely about SDLS implementation for now since it's way easier…

An initial "configuration" will be loaded on the ground and on the SC when the SC boots.

What does this "configuration" entail?

- "Managed parameters" for TC / TM / AOS
    - Maximum frame lengths
    - Amount of padding
    - Fill words
    - Etc.
- Cryptographic Library
    - Gcrypt, VeraCrypt, Bouncy Castle, OpenSSL, etc.
- Security Association Database
    - GVCID or virtual channel mappings for use
    - Status for each SA
    - Active SA in use for TC / TM / AOS
- Key Store
    - File directory, encryption type, PKCS#12 keys

Requirements

- Based on initial configuration telemetry should continue to flow down and actual FSW commands should make it through.
- Can send "clear" commands or "encrypted" commands without changing configuration
    - So commanding doesn't have an "active" SA, but access to entire database
- Can change from "clear" telemetry to "encrypted" telemetry
    - Need to maintain an "active" SA for telemetry or maybe provide that when calling the "apply" function
- Can switch between "clear" and "encrypted" modes for command and telemetry
- Report current state of the library
    - Does SDLS-EP handle all this? FECF reports some information I think, but need to ensure this makes it to the user

System Level Unit Tests

- Test each algorithm
    - Change active TM SA
    - Send NOOP EVS Command, Confirm EVS Command Counter Increments

- Test changing configuration, reboot, and still work with new config afterwards