draft-hares-i2rs-auth-trans
draft-ietf-i2rs-security-requirements

Susan Hares

Identity + Secondary Identity (3)

- **SEC-REQ-06:** The I2RS protocol SHOULD assume some mechanism (IETF or private) will distribute or load identities so that the I2RS client/agent has these identifiers prior to the I2RS protocol establishing a connection between I2RS client and I2RS agent.
- **SEC-REQ-07:** Each identifier MUST be linked to one priority
- **SEC-REQ-08:** Each identifier is associated with one secondary identifier during a particular read/write sequence, but the secondary identifier may vary during the time a connection between the I2RS client and I2RS agent is active. The variance of the secondary identifier allows the I2rs client to be associated with multiple applications and pass along an identifier for these applications in the secondary identifier.

Transport Requirements (1)

- **SEC-REQ-09:** The data security of the I2RS protocol
  - MUST be able to support transfer of the data over a secure transport and
  - optionally MAY be able to support a non-security transport. A secure transport MUST provide data confidentiality, data integrity, and replay prevention.

  - Note: The non-secure transport protocol can be used for publishing telemetry data that is non-confidential.
  - Data models must clearly state what goes over secure transports, and what data may go over insecure transports.

Keys for Secure Transport (1)

- **SEC-REQ-10:** A secure transport MUST be associated with a key management solution that can guarantee that only the entities having sufficient privileges can get the keys to encrypt/decrypt the sensitive data.

  Per RFC4107/BCP107 this key management system SHOULD be automatic, but MAY BE manual if the following constraints from BCP107:

  - a)environment has limited bandwidth or high round-trip times,
  - b)the information being protected has a low value and
  - c)the total volume over the entire lifetime of the long-term session key will be very low,
  - d)the scale of the deployment is limited.

- Few I2RS will qualify for the manual key system, but data models should indicate which data models are eligible to be served by manual key systems

Transport Requirements

- **SEC-REQ-11:** The I2RS protocol MUST be able to support multiple secure transport sessions providing protocol and data communication between an I2RS Agent and an I2RS client.
  - However, a single I2RS Agent to I2RS client connection MAY elect to use a single secure transport session or a single non-secure transport session.
- **SEC-REQ-12:** The I2RS Client and I2RS Agent protocol SHOULD implement mechanisms that mitigate DoS attacks

Data Confidentiality

- SEC-REQ-13: In a critical infrastructure, certain data within routing elements is sensitive and read/write operations on such data MUST be controlled in order to protect its confidentiality.
  - While carriers may share peering information, most carriers do not share configuration and traffic statistics.
  - To achieve this, access control to sensitive data needs to be provided, and the confidentiality protection on such data during transportation needs to be enforced.

Data Message Integrity

- SEC-REQ-14: An integrity protection mechanism for I2RS SHOULD be able to ensure the following:
  - 1) the data being protected is not modified without detection during its transportation and
  - 2) the data is actually from where it is expected to come from
  - 3) the data is not repeated from some earlier interaction of the protocol.

Data Message Integrity

- SEC-REQ-15: The integrity that the message data is not repeated means that I2RS client to I2RS agent transport SHOULD protect against replay attack

- SEC-REQ-16: The I2RS message traceability and notification requirements found in [I-D.ietf-i2rs-traceability] and [I-D.ietf-i2rs-pub-sub-requirements]
  - SHOULD be supported in communication channel that is non-secure to trace or notify about potential security issues

Roles and data access

- SEC-REQ-17: The rules around what role is permitted to access and manipulate what information plus a secure transport (which protects the data in transit) SHOULD ensure that data of any level of sensitivity is reasonably protected from being observed by those without permission to view it, so that privacy requirements are met.

Role-Based Data Model

- SEC-REQ-18: Role security MUST work when multiple transport connections are being used between the I2RS client and I2RS agent as the I2RS architecture [I-D.ietf-i2rs-architecture] states.
  - TCP has one stream, SCTP has multiple streams
- SEC-REQ-19: I2RS clients MAY be used by multiple applications to configure routing via I2RS agents, receive status reports, turn on the I2RS audit stream, or turn on I2RS traceability.

QUESTIONS?