draft-hares-i2rs-auth-trans

Susan Hares

NETCONF (Juergen) Review

- Requirements 1, 02, 5, 6, 7, 9, 11, 13, 14, 15, 16, 18, 19, 20 – no problem noted

Editorial

- Editorial: Req. 3 /4 – need clarification on words,
- Req. 8 – not a security requirement
- Req 10 – is ambiguous

Concerns:

- Req. 8 – not a security requirement
- REQ 12 – Why is DDoS a protocol functions?
- Multiple message sequences – Why is this a security issue?
- Why support an insecure protocol?

Protocol Requirements (1)

- Basic 101 on I2RS Clients and I2RS agent mutual authentication
  - SEC-REQ-01: All I2RS clients and I2RS agents MUST have at least one unique identifier that uniquely identifies each party.
  - SEC-REQ-02: The I2RS protocol MUST utilize these identifiers for mutual identification of the I2RS client and I2RS agent.
  - SEC-REQ-03:An I2RS agent, upon receiving an I2RS message from a client, MUST confirm that the client has a valid identity.
  - SEC-REQ-04: The client, upon receiving an I2RS message from an agent, MUST confirm the I2RS agent's identity.
  - SEC-REQ-05: Identity distribution and the loading of these identities into I2RS agent and I2RS Client SHOULD occur outside the I2RS protocol.

Identity + Secondary Identity

- **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 identities prior to the I2RS protocol establishing a connection between I2RS client and I2RS agent.
- **SEC-REQ-07:** Each Identity MUST be linked to one priority
- **SEC-REQ-08:** Each Identity is associated with one secondary identity during a particular read/write sequence, but the secondary identity may vary during the time a connection between the I2RS client and I2RS agent is active. The variance of the secondary identity allows the I2rs client to be associated with multiple applications and pass along an identifier for these applications in the secondary identifier.

Transport Requirements

- **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 be able to support a non-security transport.
  - A security transport is defined to have the qualities of confidentiality, has message integrity, prevents replay attack, and supports end-to-end integrity of the I2RS client-agent session.

- **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.
  - (pre-shared keys OK)

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

Multiple Message

- REQ-17 – was deprecated
  - Perform all or none
  - Perform until error
  - Perform all storing errors

Role-Based Data Model

- SEC-REQ-18 – Man in the Middle attacks
- SEC-REQ-19: 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.
- SEC-REQ-20: 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?