

I2RS Security Related Requirements

draft-hares-i2rs-auth-trans-03

Susan Hares

Intent of this document

- To attempt to provide requirements for the security of the I2RS protocol
- Provide examples of the security behavior
- To drive discussion about potential implementations of that behavior and their representations in netconf/restconf and yang.

Security topics

- Mutual authentication
- Transport requirements
- Data Confidentiality
- Message integrity
- Role-Based Data Model Security

Mutual authentication (1)

- All I2RS clients and I2RS agents MUST have at least one unique identifier that uniquely identifies each party.
- The I2RS protocol MUST utilize these identifiers for mutual identification of the I2RS client and I2RS agent.
- An I2RS agent, upon receiving an I2RS message from a client, MUST confirm that the client has a valid identity.
- The client, upon receiving an I2RS message from an agent, MUST confirm the I2RS identity.

Mutual Authentication (2)

- Identity distribution and the loading of these identities into I2RS agent and I2RS Client occur outside the I2RS protocol.
- 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.
- Each Identity will be linked to one priority
- 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.

Secure Transport Requirements

- I2RS protocol must support secure transport
 - Confidentiality, message integrity, and end-to-end integrity within the protocol session,
 - Must be able to allow non-secure sessions
 - Key rotation
 - Multiple secure transports
- Support for stacked clients is not in the protocol

Confidentiality & integrity

- Data confidentiality
 - Some data will be sensitive, and so protocol must be able to protect against unauthorized read/writes during transportation
- Message integrity
- 1) the data being protected are not modified without detection during its transportation
- 2) the data is actually from where it is expected to come from (no MITM attacks)
- 3) the data is not repeated from some earlier interaction of the protocol (no replay)

No Multi-message atomicity & rollback

Multiple Message Handling

I2RS architecture does not include multi-message atomicity and rollback mechanisms, but suggests an I2RS client may indicate one of the following error handling techniques for a given message sent to the I2RS client:

1. Perform all or none: All operations succeed or none of them will be applied. This useful when there are mutual dependencies.
2. Perform until error: Operations are applied in order, and when error occurs the processing stops. This is useful when dependencies exist between multiple-message operations, and order is important.
3. Perform all storing errors: Perform all actions storing error indications for errors. This method can be used when there are no dependencies between operations, and the client wants to sort it out.

Role Based Data Model Security

- Must work with multiple transport sessions
 - Transport session start/stop
 - Example: TCP versus SCTP
- One client-agent connection will use 1 priority
- Multiple applications may talk to 1 client but that application-client interchange is out of scope