I2RS working group
Internet-Draft
Intended status: Standards Track
Expires: November 6, 2016

S. Hares
Huawei
D. Migault
J. Halpern
Ericsson
May 5, 2016

I2RS Security Related Requirements
draft-ietf-i2rs-protocol-security-requirements-04

Abstract

This presents security-related requirements for the I2RS protocol for mutual authentication, transport protocols, data transfer and transactions.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on November 6, 2016.

Copyright Notice

Table of Contents

1. Introduction 2
1.1. Requirements Language 3
2. Definitions 3
2.1. Security Definitions 3
2.2. I2RS Specific Definitions 6
3. Security-Related Requirements 7
3.1. Mutual authentication of an I2RS client and an I2RS Agent 8
3.2. Transport Requirements Based on Mutual Authentication . . 8
3.3. Data Confidentiality Requirements 10
3.4. Data Integrity Requirements 10
3.5. Role-Based Data Model Security 11
3.6. Security of the environment 11
4. Acknowledgement 12
5. IANA Considerations 12
6. Security Considerations 12
7. References 12
7.1. Normative References 12
7.2. Informative References 12
Authors' Addresses 13

1. Introduction

The Interface to the Routing System (I2RS) provides read and write access to information and state within the routing process. An I2RS client interacts with one or more I2RS agents to collect information from network routing systems.

This document describes the requirements for the I2RS protocol in the security-related areas of mutual authentication of the I2RS client and agent, the transport protocol carrying the I2RS protocol messages, and the atomicity of the transactions. These requirements align with the description of the I2RS architecture found in [I-D.ietf-i2rs-architecture] document which solves the problem described in [I-D.ietf-i2rs-problem-statement].

[I-D.ietf-i2rs-ephemeral-state] discusses I2RS role-based access control that provides write conflict resolution in the ephemeral data store using the I2RS Client Identity, I2RS Secondary Identity and priority. The draft [I-D.ietf-i2rs-traceability] describes the traceability framework and its requirements for I2RS. The draft [I-D.ietf-i2rs-pub-sub-requirements] describes the requirements for I2RS to be able to publish information or have a remote client subscribe to an information data stream.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Definitions

2.1. Security Definitions

This document utilizes the definitions found in the following documents: [RFC4949] and [I-D.ietf-i2rs-architecture]

Specifically, this document utilizes the following definitions:

access control

[RFC4949] defines access control as the following:

1. (I) Protection of system resources against unauthorized access.

2. (I) A process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy. (See: access, access control service, computer security, discretionary access control, mandatory access control, role-based access control.)

3. (I) /formal model/ Limitations on interactions between subjects and objects in an information system.

4. (O) "The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner." [I7498-2]

5. (O) /U.S. Government/ A system using physical, electronic, or human controls to identify or admit personnel with properly authorized access to a SCIF.

Authentication

[RFC4949] describes authentication as the process of verifying (i.e., establishing the truth of) an attribute value claimed by or for a system entity or system resource. Authentication has two steps: identify and verify.

Data Confidentiality

[RFC4949] describes data confidentiality as having two properties:

> a) Data is not disclosed to system entities unless they have been authorized to know the data, and
>
> b) Data is not disclosed to unauthorized individuals, entities or processes.

The key point is that confidentiality implies that the originator has the ability to authorize where the information goes. Confidentiality is important for both read and write scope of the data.

Data Integrity

[RFC4949] states data integrity includes:

> 1. (I) The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. [...]
>
> 2. (O) "The property that information has not been modified or destroyed in an unauthorized manner." [I7498-2]

Data Privacy

[RFC4949] describes data privacy as a synonym for data confidentiality. This I2RS document will utilize data privacy as a synonym for data confidentiality.

Identity

[RFC4949] (I) The collective aspect of a set of attribute values (i.e., a set of characteristics) by which a system user or other system entity is recognizable or known. (See: authenticate, registration. Compare: identifier.)

Identifier

[RFC4949] (I) A data object -- often, a printable, non-blank character string -- that definitively represents a specific identity of a system entity, distinguishing that identity from all others. (Compare: identity.)

Mutual Authentication

[RFC4949] implies that mutual authentication exists between two interacting system entities.

Mutual authentication in I2RS implies that both sides move from a state of mutual suspicion to to mutual authentication to trusted mutual communication after each system has been identified and validated by its peer system.

role

[RFC4949] describes role as:

1. (I) A job function or employment position to which people or other system entities may be assigned in a system. [...]

2. (O) /Common Criteria/ A pre-defined set of rules establishing the allowed interactions between a user and the TOE.

The I2RS uses the common criteria definition.

role-based access control

[RFC4949] describes role-based access control as: "A form of identity-based access control wherein the system entities that are identified and controlled are functional positions in an organization or process."

security audit trail

[RFC4949] describes a security audit trail as "A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results."

Requirements to support a security audit is not covered in this document.

[I-D.ietf-i2rs-traceability] describes traceability for I2RS interface and the I2RS protocol. Traceability is not equivalent to a security audit trail.

Trust

[RFC4949]

1. (I) /information system/ A feeling of certainty (sometimes based on inconclusive evidence) either (a) that the system will not fail or (b) that the system meets its specifications

(i.e., the system does what it claims to do and does not perform unwanted functions). (See: trust level, trusted system, trustworthy system. Compare: assurance.)

2. . (I) /PKI/ A relationship between a certificate user and a CA in which the user acts according to the assumption that the CA creates only valid digital certificates. (Also referred as "trusted" in [RFC4949].)

2.2. I2RS Specific Definitions

I2RS protocol data integrity

The transfer of data via the I2RS protocol has the property of data integrity described in [RFC4949].

I2RS component protocols

Protocols which are combined to create the I2RS protocol.

I2RS Higher-level protocol

The I2RS protocol exists as a higher-level protocol which may combine other protocols (NETCONF, RESTCONF, IPFIX and others) within a specific I2RS client-agent relationship with a specific trust for ephemeral configurations, event, tracing, actions, and data flow interactions. The protocols included in the I2RS protocol protocol are defined as I2RS component protocols. (Note: Version 1 of the I2RS protocol will combine only NETCONF and RESTCONF. Experiments with other protocols such as IPFIX have shown these are useful to combine with NETCONF and RESTCONF features.)

I2RS message

is a complete data message of one of the I2RS component protocols. The I2RS component protocols may require multiple IP-packets to send one protocol message.

I2RS multi-message atomicity

An I2RS operation (read, write, event, action) must be contained within one I2RS message. Each I2RS operation must be atomic. While it is possible to have an I2RS operation which is contained in multiple I2RS (E.g. write in multiple messages), this is not supported in order to simply the first version of I2RS. Multiple-message atomicity of I2RS operations would be used in a roll-back of a grouping of commands (e.g. multiple writes).

I2RS transaction

is a unit of I2RS functionality. Some examples of I2RS transactions are:

* The I2RS client issues a read request to a I2RS agent, and the I2RS Agent responding to the read request

* The I2RS client issues a write of ephemeral configuration values into an I2RS agent’sbr data model, followed by the I2RS agent response to the write.

* An I2RS client may issue an action request, the I2RS agent responds to the action-request, and then responds when action is complete. Actions can be single step processes or multiple step process.

* An I2RS client requests to receive an event notification, and the I2RS Agent sets up to send the events.

* An I2RS agent sends events to an I2RS Client on an existing connection.

An I2RS action may require multiple I2RS messages in order to complete a transation.

I2RS secondary identifier

The I2RS architecture document [I-D.ietf-i2rs-architecture] defines a secondary identity as the entity of some non-I2RS entity (e.g. application) which has requested a particular I2RS client perform an operation. The I2RS secondary identifier represents this identity so it may be distinguished from all others.

3. Security-Related Requirements

The security for the I2RS protocol requires mutually authenticated I2RS clients and I2RS agents. The I2RS client and I2RS agent using the I2RS protocol MUST be able to exchange data over a secure transport, but some functions may operate on a non-secure transport. The I2RS protocol MUST be able to provide atomicity of an I2RS transaction, but it is not required to have multi-message atomicity and roll-back mechanism transactions. Multiple messages transactions may be impacted by the interdependency of data. This section discusses the details of these security requirements.

3.1. Mutual authentication of an I2RS client and an I2RS Agent

The I2RS architecture [I-D.ietf-i2rs-architecture] sets the following requirements:

- SEC-REQ-01: All I2RS clients and I2RS agents MUST have an identity, and at least one unique identifier that uniquely identifies each party in the I2RS protocol context.

- 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 I2RS client, MUST confirm that the I2RS client has a valid identifier.

- SEC-REQ-04: The I2RS client, upon receiving an I2RS message from an I2RS agent, MUST confirm the I2RS agent has a valid identifier.

- SEC-REQ-05: Identifier distribution and the loading of these identifiers into I2RS agent and I2RS Client SHOULD occur outside the I2RS protocol.

- SEC-REQ-06: The I2RS protocol SHOULD assume some mechanism (IETF or private) will distribute or load identifiers 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 have just one priority.

- SEC-REQ-08: Each Identifier is associated with one secondary identifier during a particular I2RS transaction (e.g. read/write sequence), but the secondary identifier may vary during the time a connection between the I2RS client and I2RS agent is active. Since a single I2RS client may be use by multiple applications, the secondary identifier may vary as the I2RS client is utilize by different application each of whom have a unique secondary identity and identifier.

3.2. Transport Requirements Based on Mutual Authentication

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

The default I2RS transport is a secure transport.

A non-secure transport can be can be used for publishing telemetry data or other operational state that was specifically indicated to non-confidential in the data model in the Yang syntax.

The configuration of ephemeral data in the I2RS Agent by the I2RS client SHOULD be done over a secure transport. It is anticipated that the passing of most I2RS ephemeral state operational status SHOULD be done over a secure transport. As [I-D.ietf-i2rs-ephemeral-state] notes data model MUST indicate whether the transport exchanging the data between I2RS client and I2RS agent is secure or insecure. The default mode of transport is secure so data models SHOULD clearly annotate what data nodes can be passed over an insecure connection.

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 BCP107 [RFC4107] this key management system SHOULD be automatic, but MAY be manual in the following scenarios:

a) The environment has limited bandwidth or high round-trip times.

b) The information being protected has low value.

c) The total volume of traffic over the entire lifetime of the long-term session key will be very low.

d) The scale of the deployment is limited.

Most I2RS environments (Clients and Agents) will not have the environment described by BCP107 [RFC4107] but a few I2RS use cases required limited non-secure light-weight telemetry messages that have these requirements. An I2RS data model must indicate which portions can be served by manual key management.

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.

3.3. Data Confidentiality Requirements

SEC-REQ-13: In a critical infrastructure, certain data within routing elements is sensitive and read/write operations on such data SHOULD be controlled in order to protect its confidentiality. For example, most carriers do not want a router's configuration and data flow statistics known by hackers or their competitors. 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.

3.4. Data Integrity Requirements

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,

2) the data is actually from where it is expected to come from, and

3) the data is not repeated from some earlier interaction of the protocol. (That is, when both confidentiality and integrity of data is properly protected, it is possible to ensure that encrypted data is not modified or replayed without detection.)

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

Requirements SEC-REQ-13 and SEC-REQ-14 are SHOULD requirements only because it is recognized that some I2RS Client to I2RS agent communication occurs over a non-secure channel. The I2RS client to I2RS agent over a secure channel would implement these features. In order to provide some traceability or notification for the non-secure protocol, SEC-REQ-16 suggests traceability and notification are important to include for any non-secure protocol.

SEC-REQ-16: The I2RS message traceability and notification requirements 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.

3.5. Role-Based Data Model Security

The I2RS Architecture [I-D.ietf-i2rs-architecture] defines a role or security role as specifying read, write, or notification access by a I2RS client to data within an agent's data model.

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.

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. These transport message streams may start/stop without affecting the existence of the client/agent data exchange. TCP supports a single stream of data. SCTP [RFC4960] provides security for multiple streams plus end-to-end transport of data.

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. Application software using I2RS client functions may host multiple secure identities, but each connection will use only one identifier with one priority. Therefore, the security of each I2RS Client to I2RS Agent connection is unique.

Please note the security of the application to I2RS client connection is outside of the I2RS protocol or I2RS interface.

Sec-REQ-20: If an I2RS agents or an I2RS client is tightly correlated with a person, then the I2RS protocol and data models should provide additional security that protects the person's privacy. An example of an I2RS agent correlated with a person is a I2RS agent running on someone's phone to control tethering, and an example of a I2RS client might be the client tracking such tethering. This protection MAY require a variety of forms including: "operator-applied knobs", roles that restrict personal access, data-models with specific "privacy roles", and access filters.

3.6. Security of the environment

The security for the implementation of a protocol also considers the protocol environment. The environmental security requirements are found in: [I-D.ietf-i2rs-security-environment-reqs].

4. Acknowledgement

The authors would like to thank Wes George, Ahmed Abro, Qin Wu, Eric Yu, Joel Halpern, Scott Brim, Nancy Cam-Winget, DaCheng Zhang, Alia Atlas, and Jeff Haas for their contributions to the I2RS security requirements discussion and this document. The authors would like to thank Bob Moskowitz for his review of the requirements.

5. IANA Considerations

This draft includes no request to IANA.

6. Security Considerations

This is a document about security requirements for the I2RS protocol and data modules. The whole document is security considerations.

7. References

7.1. Normative References

[I-D.ietf-i2rs-architecture]
Atlas, A., Halpern, J., Hares, S., Ward, D., and T. Nadeau, "An Architecture for the Interface to the Routing System", draft-ietf-i2rs-architecture-15 (work in progress), April 2016.

[I-D.ietf-i2rs-problem-statement]
Atlas, A., Nadeau, T., and D. Ward, "Interface to the Routing System Problem Statement", draft-ietf-i2rs-problem-statement-10 (work in progress), February 2016.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC4107] Bellovin, S. and R. Housley, "Guidelines for Cryptographic Key Management", BCP 107, RFC 4107, DOI 10.17487/RFC4107, June 2005, <http://www.rfc-editor.org/info/rfc4107>.

7.2. Informative References

[I-D.ietf-i2rs-ephemeral-state]
Haas, J. and S. Hares, "I2RS Ephemeral State Requirements", draft-ietf-i2rs-ephemeral-state-05 (work in progress), March 2016.

[I-D.ietf-i2rs-pub-sub-requirements]
Voit, E., Clemm, A., and A. Prieto, "Requirements for Subscription to YANG Datastores", draft-ietf-i2rs-pub-sub-requirements-07 (work in progress), May 2016.

[I-D.ietf-i2rs-security-environment-reqs]
Migault, D., Halpern, J., and S. Hares, "I2RS Environment Security Requirements", draft-ietf-i2rs-security-environment-reqs-01 (work in progress), April 2016.

[I-D.ietf-i2rs-traceability]
Clarke, J., Salgueiro, G., and C. Pignataro, "Interface to the Routing System (I2RS) Traceability: Framework and Information Model", draft-ietf-i2rs-traceability-09 (work in progress), May 2016.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <http://www.rfc-editor.org/info/rfc4949>.

[RFC4960] Stewart, R., Ed., "Stream Control Transmission Protocol", RFC 4960, DOI 10.17487/RFC4960, September 2007, <http://www.rfc-editor.org/info/rfc4960>.

Authors' Addresses

Susan Hares
Huawei
7453 Hickory Hill
Saline, MI 48176
USA

Email: shares@ndzh.com

Daniel Migault
Ericsson
8400 boulevard Decarie
Montreal, QC HAP 2N2
Canada

Email: daniel.migault@ericsson.com

Joel Halpern
Ericsson
US

Email: joel.halpern@ericsson.com