

I2RS working group
Internet-Draft
Intended status: Standards Track
Expires: July 3, 2016

S. Hares
Huawei
D. Migault
J. Halpern
Ericsson
December 31, 2015

I2RS Security Related Requirements
draft-ietf-i2rs-protocol-security-requirements-02

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 July 3, 2016.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
1.1.	Requirements Language	2
1.2.	Definitions	3
2.	Security-Related Requirements	5
2.1.	Mutual authentication of I2RS client and I2RS Agent . . .	5
2.2.	Transport Requirements Based on Mutual Authentication . .	6
2.3.	Data Confidentiality Requirements	7
2.4.	Data Integrity Requirements	7
2.5.	Role-Based Data Model Security	8
3.	Acknowledgement	8
4.	IANA Considerations	9
5.	Security Considerations	9
6.	References	9
6.1.	Normative References	9
6.2.	Informative References	9
	Authors' Addresses	10

[1.](#) Introduction

The Interface to the Routing System (I2RS) provides read and write access to information and state within the routing process. The 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.haas-i2rs-ephemeral-state-reqs](#)] discusses I2RS roles-based 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](#)].

1.2. Definitions

This document utilizes the definitions found in the following drafts: [\[RFC4949\]](#), 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 use;
- 2)(I)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;
- 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.";
- 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, 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
2. (O) "The property that information has not been modified or destroyed in an unauthorized manner."

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.

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 mutually authenticated 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. (See: role-based access control. Compare: duty, billet, principal, user.)
- 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

[RFC4949] describes role-based access control as: (I) 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] (page 254) 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. The draft [[I-D.ietf-i2rs-traceability](#)] describes traceability for I2RS interface and protocol. Traceability is not equivalent to a security audit trail.

I2RS the following phrase that incorporates an [[RFC4949](#)] definition:

I2RS protocol data integrity

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

2. 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 non-secure transport. The I2RS protocol MUST BE able to provide atomicity of a 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 these details of these security requirements.

2.1. Mutual authentication of I2RS client and I2RS Agent

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

- o SEC-REQ-01: All I2RS clients and I2RS agents MUST have at least one unique identifier that uniquely identifies each party.
- o SEC-REQ-02: The I2RS protocol MUST utilize these identifiers for mutual identification of the I2RS client and I2RS agent.
- o 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.
- o SEC-REQ-04: The I2RS client, upon receiving an I2RS message from an I2RS agent, MUST confirm the I2RS agent has a valid identifier

- o SEC-REQ-05: Identifier distribution and the loading of these identifiers into I2RS agent and I2RS Client SHOULD occur outside the I2RS protocol.
- o 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.
- o SEC-REQ-07: Each Identifier MUST be linked to one priority
- o 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.

2.2. 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.

Note: The non-secure transport can be used for publishing telemetry data that was specifically indicated to non-confidential in the data model. 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. Data models SHOULD clearly annotate what data nodes can be passed over an insecure connection. The default transport is a secure transport.

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 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.

Most I2RS environments (I2RS Client - I2S 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

2.3. Data Confidentiality Requirements

SEC-REQ-13: In a critical infrastructure, certain data within routing elements is sensitive and read/write operations on such data MUST 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.

2.4. 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 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. 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

2.5. Role-Based Data Model Security

The [[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 several 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.

3. Acknowledgement

The author 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.

4. IANA Considerations

This draft includes no request to IANA.

5. Security Considerations

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

6. References

6.1. 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-12](#) (work in progress), December 2015.
- [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>>.

6.2. Informative References

- [I-D.haas-i2rs-ephemeral-state-reqs]
Haas, J., "I2RS Ephemeral State Requirements", [draft-haas-i2rs-ephemeral-state-reqs-00](#) (work in progress), May 2015.
- [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-08](#) (work in progress), December 2015.
- [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-03](#) (work in progress), October 2015.

[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-05](#) (work in progress), December 2015.

[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