

I2RS working group
Internet-Draft
Intended status: Standards Track
Expires: December 26, 2015

S. Hares
Huawei
June 24, 2015

I2RS Security Related Requirements
draft-hares-i2rs-auth-trans-02

Abstract

This presents an 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 December 26, 2015.

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.	10 I2RS General Requirements	3
1.2.	Definitions	4
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	6
2.4.	Message Integrity Requirements	7
2.4.1.	Handling Multiple Messages	7
2.5.	Role-Based Data Model Security	7
3.	Acknowledgement	8
4.	IANA Considerations	8
5.	Security Considerations	8
6.	References	8
6.1.	Normative References	8
6.2.	Informative References	9
	Author's Address	9

1. Introduction

The Interface to the Routing System (I2RS) provides read and write access to the 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 were initially described in the [I-D.ietf-i2rs-architecture] document. These security requirements are also part of the list of top ten requirements for the I2RS protocol indicated in the section below.

[I-D.haas-i2rs-ephemeral-state-reqs] discusses of 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] describe the requirements for I2RS to be able to publish information or have a remote client subscribe to an information data stream.

1.1. 10 I2RS General Requirements

1. The I2RS protocol SHOULD support highly reliable notifications (but not perfectly reliable notifications) from an I2RS agent to an I2RS client.
2. The I2RS protocol SHOULD support a high bandwidth, asynchronous interface, with real-time guarantees on getting data from an I2RS agent by an I2RS client.
3. The I2RS protocol will operate on data models which may be protocol independent or protocol dependent.
4. I2RS Agent needs to record the client identity when a node is created or modified. The I2RS Agent needs to be able to read the client identity of a node and use the client identity's associated priority to resolve conflicts. The secondary identity is useful for traceability and may also be recorded.
5. Client identity will have only one priority for the client identity. A collision on writes is considered an error, but priority is utilized to compare requests from two different clients in order to modify an existing node entry. Only an entry from a client which is higher priority can modify an existing entry (First entry wins). Priority only has meaning at the time of use.
6. The Agent identity and the Client identity should be passed outside of the I2RS protocol in a authentication and authorization protocol (AAA). Client priority may be passed in the AAA protocol. The values of identities are originally set by operators, and not standardized.
7. An I2RS Client and I2RS Agent mutually authenticate each other based on pre-established authenticated identities.
8. Secondary identity data is read-only meta-data that is recorded by the I2RS agent which associated with a data model's node when the node is written, updated or deleted. Just like the primary identity, the secondary identity is only recorded when the data node is written or updated or deleted.
9. I2RS agent can have a lower priority I2RS client attempting to modify a higher priority client's entry in a data model. The filtering out of lower priority clients attempting to write or modify a higher priority client's entry in a data model SHOULD be effectively handled and not put an undue strain on the I2RS agent. Note: Jeff's suggests that priority is kept at the NACM

at the client level (rather than the path level or the group level) will allow these lower priority clients to be filtered out using an extended NACM approach. This is only a suggestion of a method to provide the requirement

10. The I2RS protocol MUST support the use of a secure transport. However, certain functions such as notifications MAY use a non-secure transport. Each model or service (notification, logging) must define within the model or service the valid uses of a non-secure transport.

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:

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 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.

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 integrity

The data transfer as it is transmitted between client and agent cannot be modified by unauthorized parties without detection.

2. Security-Related Requirements

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

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

2.2. Transport Requirements Based on Mutual Authentication

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, and supports end-to-end integrity (in the case of stacked clients).

A secure transport also 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 is considered for this document to be a key management system. In addition, the key management mechanisms need to be able to update the keys before they have lost sufficient security strengths, without breaking the connection between the agents and clients.

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 connect MAY elect to use a single secure transport session or a single non-secure transport session.

2.3. Data Confidentiality Requirements

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 for this data, and the confidentiality protection on such data during transportation needs to be enforced.

2.4. Message Integrity Requirements

An integrity protection mechanism for I2RS should be able to ensure the following: 1) the data being protected are 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 are not modified or replayed without detection.

2.4.1. Handling Multiple Messages

Section 7.9 of the [I-D.ietf-i2rs-architecture] states the 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.

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 within a data model that a client has to an agent's data model.

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. Observer without

permission can refer to other I2RS clients, attackers, or assorted MITM (man-in-the-middle) monkeys.

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.

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. An application software using I2RS client functions can host several multiple secure identities, but each connection will use only one identity 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 I2RS security requirement 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

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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-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-09 (work in progress), March 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-06 (work in progress), January 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-02 (work in progress), March 2015.
- [I-D.ietf-i2rs-rib-info-model]
Bahadur, N., Folkes, R., Kini, S., and J. Medved, "Routing Information Base Info Model", draft-ietf-i2rs-rib-info-model-06 (work in progress), March 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-03 (work in progress), May 2015.
- [RFC4785] Blumenthal, U. and P. Goel, "Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)", RFC 4785, January 2007.
- [RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.
- [RFC4960] Stewart, R., "Stream Control Transmission Protocol", RFC 4960, September 2007.

Author's Address

Susan Hares
Huawei
7453 Hickory Hill
Saline, MI 48176
USA

Email: shares@ndzh.com