I2RS working group
Internet-Draft
Intended status: Standards Track
Expires: December 12, 2015

S. Hares
Huawei

June 10, 2015

I2RS Security Related Requirements
draft-hares-i2rs-auth-trans-00

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 12, 2015.

Table of Contents

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 associated with a data model's 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.

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 confidentiality service

[RFC4949] also describes data confidentiality service as a security service that protects data against unauthorized disclosure. Please note that an operator can designate all people are authorized to view a piece of data which would mean a data confidentiality service would be essentially a null function.

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 afte each system has been identified and validated by its peer system

Mutual Suspicion

[RFC4949] defines mutual suspicion as a state that exists between two interacting system entities in which neither entity can trust the other to function correctly with regard to some security requirement.

Role

[RFC4949] describes role as a job function or employment position to which people or other system entities may be assigned in a system. In the I2RS interface, the I2RS agent roles relate to the roles that the I2RS client is utilizing. In the I2RS interface, the I2RS client negotiation is over the client's ability to access resources made available through the agent's particular role.

Role-based Access control

[RFC4949] describes role-based access control as an identity-based access control wherein the system entities that are identified and controlled are functional positions in an organization or process. Within [RFC4949] five relationships are discussed: 1) administrators to assign identities to roles, 2) administrators to assign permissions to roles, 3) administrators to assign roles to roles, 4) users to select identities in sessions, and 5) users to select roles in sessions.

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.

I2RS integrity

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

3. Security-Related Requirements

The security for the I2RS protocol requires mutually authenticated I2RS client and I2RS agent MUST be able to exchange data over a secure transport, and MUST use role-based security to store data in I2RS data models in ephemeral state, and MUST provide atomicity of a transaction. This section describes the requirements for the mutual authentication of the I2RS agent and client, and the secure transport. The issues relating to role-based security to store data in I2RS data models in ephemeral state is covered in [I-D.haas-i2rs-ephemeral-state-reqs].

3.1. Mutual authentication of I2RS client and I2RS Agent

The I2RS architecture [I-D.ietf-i2rs-architecture]document states:

> "Mutual authentication between the I2RS Client and I2RS Agent is required. An I2RS Client must be able to trust that the I2RS Agent is attached to the relevant Routing Element so that write/ modify operations are correctly applied and so that information received from the I2RS Agent can be trusted by the I2RS Client."

This architecture set the following requirements:

- 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.
- 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) in order to distribute or load identities and that the I2RS client/agent will load the 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 will be linked to one secondary identity for the period of a connection.

3.2. Transport Requirements Based on Mutual Authentication

I2RS data security MUST be able to support transfer of the data between the I2RS client to I2RS agent in a manner that is confidential, has message integrity, and supports end-to-end integrity (in the case of stacked clients).

The I2RS data security mechanisms used for protecting the I2RS packets needs to be associated with proper key management solutions. A key management solution needs to guarantee that only the entities having sufficient privileges can get the keys to encrypt/decrypt the sensitive data. 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 rules around what role is permitted to access and manipulate what information, combined with encryption to protect the data in transit is intended SHOULD ensure that data of any level of sensitivity is reasonably protected from being observed by those without permission to view it. In that case 'those' can refer to either other roles, sub-agents, or to attackers and assorted MITM (man-in-the-middle)monkeys.

The I2RS protocol MUST support multiple transport sessions providing protocol and data communication between the I2RS Agent and the I2RS client.

3.2.1. NETCONF over SSH

The NETCONF service over SSH is believed to provide the necessary mutual authentication services required by I2RS. Per [RFC6242]: "The identity of the SSH server MUST be verified and authenticated by the SSH client according to local policy before password-based authentication data or any configuration or state data is sent to or received from the SSH server. The identity of the SSH client MUST also be verified and authenticated by the SSH server according to local policy to ensure that the incoming SSH client request is legitimate before any configuration or state data is sent to or received from the SSH client. Neither side should establish a NETCONF over SSH connection with an unknown, unexpected, or incorrect identity on the opposite side.

3.2.2. NETCONF/RESTCONF over TLS

Agent validation of the I2RS client is mandated over TLS in an I2RS context. The client shall also validate the Agent using its server certificate.

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

It is normal to protect the confidentiality of the sensitive data during transportation by encrypting them. Encryption obscures the data transported on the wire and protects them against eavesdropping attacks. Because the encryption itself cannot guarantee the integrity or fresh of data being transported, in practice, confidentiality protection is normally provided with integrity protection.

3.4. Message Integrity Requirements

An integrity protection mechanism for I2RS should be able to ensure 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.

As a part of integrity protection, the replay protection approaches provided for I2RS must consider both online and offline attackers, and have sufficient capability to deal with intra connection and inter-connection attacks. For instance, when using symmetric keys, sequence numbers which increase monotonically could be useful to help in distinguishing the replayed messages, under the assistance of signatures or MACs (dependent on what types of keys are applied). In addition, in the cases where only offline attacker is considered, random nonce could be effective.

3.5. Role-Based Data Model Security

The context of the I2RS client-agent communication may utilize a role which may/may not require message confidentiality, message integrity protection, or replay attack protection. However, the I2RS Protocol MUST be able to support message confidentiality, message integrity protection, and replay attack protection.

Role security for an agent involves pairing the identity to the role. The data store can read information either by write or an event stream.

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 connection is unique.

4. Data Transaction Requirements

Each transaction should be treated as atomic and providing full functionality. If the configuration change is not functionally complete, then the transaction should fail and be rolled back (rollback 0). Example, I2RS agents wants to configure BGP:

```
routing-options {
     autonomous-system autonomous-system;
     }
protocols {
   bgp {
       group group-name {
       peer-as autonomous-system;
      type type;
      neighbor address;
      }
   }
 }
```

If a statement like neighbor address is missing or is mis-formatted, like 300.127.5.23, configuration is not functional, transaction should fail and rollback 0 should be performed by the I2RS agent on the ephemeral config store. If the neighbor address is in the transaction, but the address is not reachable or similar, transaction is accepted, but notification will be sent that BGP peering cannot be established.

5. 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.

6. IANA Considerations

This draft includes no request to IANA.

7. Security Considerations

This is a document about security architecture beyond the consideration for I2RS. Additional security definitions will be added in this section.

8. References

8.1. Normative References

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

8.2. 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