I2RS working group
Internet-Draft
Intended status: Standards Track
Expires: September 5, 2014

S. Hares
Hickory Hill Consulting
W. George
Time-Warner Cable
S. Brim
Consultant
N. Cam-Winget
Cisco
D. Zhang
Q. Wu
Huawei
A. Abro
S. Asadullah
Cisco
J. Halpern
Ericcson
E. Yu
Cisco

March 4, 2014

I2RS Security Architecture
draft-hares-i2rs-security-00

Abstract

This presents an expansion of the security architecture found in the i2rs architecture.

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 September 5, 2014.

Table of Contents

1. Introduction

The Interface to the Routing System (I2RS) [[I-D.ietf-i2rs-architecture]] provides read and write access to the information and state within the routing process within routing elements. The I2RS client interacts with one or more I2RS agents to collect information from network routing systems. This security architecture expands on the the security issues involved in the i2rs client - i2rs agent exchange described in [I-D.ietf-i2rs-architecture].

2. Definitions

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

Specifically, this document utilize the following definitions:

Access control

[RFC4949] describes access control as: a) protection of system resources against unauthorized access, b) process controlled by a security policy that permits access only by authorized entities (users, programs, process, or others) according to that policy, c) preventing unauthorized use of resource, d) using human controls to identify or admit properly authorized people to a SCIF, and e) limitations on between subjects and objections in a system. I2RS focuses on role-based access control (RBAC).

Authentication

[RFC4949] describes authentication as the process of verifying (i.e., establish 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 has 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 a user can designated that the 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 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 having identified and validated.

Mutual Suspicion

[RFC4949] defines mutual suspicion as a state that exist 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 exercises a particular agent role. The negotiation is over the client ability to exercise the agents role as a resource. Please refere to diagram below. Existing work includes IETF work in ABFAB and HTTP related SAML work.

Role-based Access control

[RFC4949] describes role-based access control as an identity-based access control herein the system entities that are identified and controlled are functional positions in an organization or process. This document discusses the roles and identities that allow read, write or read-write access to I2RS agent functions.

Role-based Access control

[RFC4949] describes role-based access control as an identity-based access control herein the system entities that are identified and controlled are functional positions in an organization or process. This document discusses the roles and identities that allow read, write or read-write access to I2RS agent functions.

Role certificate

[RFC4949] describes a role certificate as an organizational certificate that is issued to a system entity that is a member of the set of users that have identities that are assigned to the same role.

Security audit trail

[RFC4949] describes a security audit trail as a chronological record of system activity 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. To apply this to the I2RS system, this implies that the processes on the I2RS client-I2RS Agent protocol and related actions on the I2RS-Agent can record a set of activity that will allow the reconstruction and examination of the sequence of environments and activities around actions caused by the I2RS protocol data streams.

I2RS integrity

The data transfer as it is transmitted between client and agent cannot be modified by unauthorized parties.

3. Security Issues

The following diagram is a variation of the [RFC4949] diagram on role-based security, and provides the context for the assumptions of security on the role-based work.

I2RS identity and functions diagram

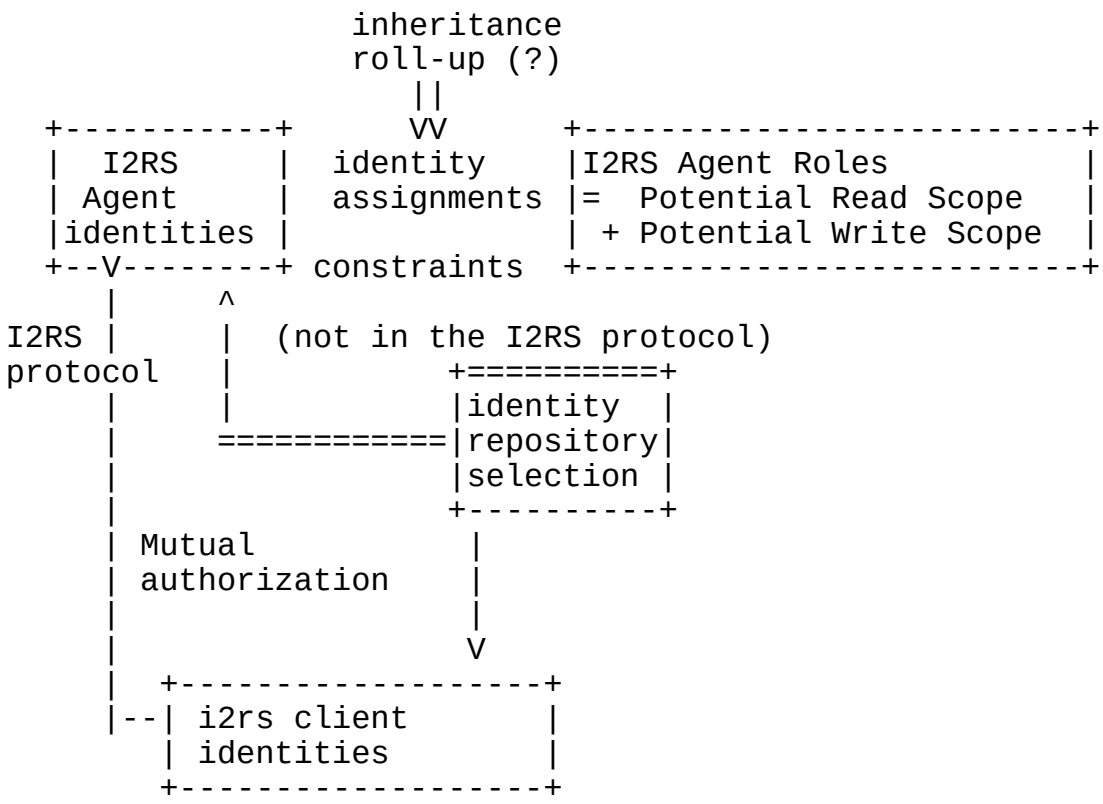
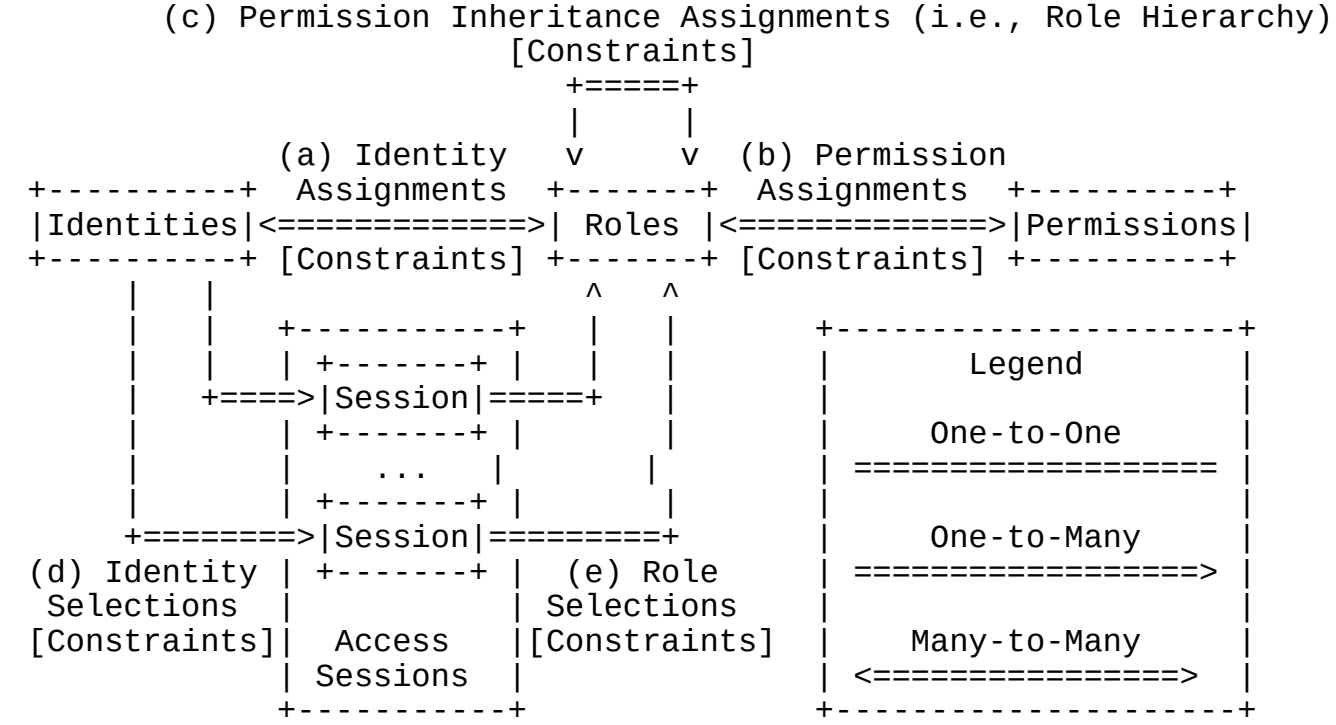


Figure 1 - I2RS Role Based discussion

The I2RS figure is taken from the following Security Definition figure on role hierarchy



3.1. Security roles for the I2RS client-agent

Role is the Agent’s Potential Read Scope plus the Potential write Scope. The potential read scope is the Routing Attributes/variables (for example BGP peer information) that an agent may potential read. A notification or an event stream is a flow that an agent may potential read. A write scope is something the client may write. Examples are is a RIB entry or a PBR entry or protocol variables (BGP, LDP).

Question: Does role by client will lead to proliferation of clients?

3.2. Transport requirements

The architecture provides the ability to have multiple transports sessions providing protocol and data communication between the I2rs Agent and the I2RS client. These transports can be TCP or secure (SCTP) or any form of transport.

The following are questions to address regarding the transport:

- Do we have mandatory-to-implement transport protocols?
- Are there concerns about opening the mandatory-to-implement transport from either the Client or the Server side?

- How would that work with a publication or subscription model?

- Is a publishing broker feasible or does that cause security issues?

3.3. Auditable Data streams

This section discusses how we can get data streams which have a security audit trail (see definitions) for the I2RS Client to I2RS AGent interactions. Agent audit trail could be the logging of what variables written by which client (id of client) on behalf of reported application (ID). Since the reported application id is not valid, all the audit stream states is that the Client told the agent this is the application I'm acting for.

Out of scope for this work is the ability to audit the application to I2RS-Client interfaces, or the I2RS Agent to I2RS routing system.

Questions to be answered:

- I2RS client to I2RS Agent is being able to audit a requirement for all I2RS agents or an option?

- What is scope of audit (full stream, partial stream, specific functions)?

- Does the ability to audit mean the ability to verify?

- How does the filtering of Event data impact the audit process? For example if BGP event changes are only taken from 50 out of 300 BGP peers, does this stop any ability to audit the session? Or if the read filters only watch for key prefixes to be received on a specific set of interfaces, does this stop the ability to audit?

- How do you handle read filtering and auditing? The last section in this document has a read filtering example. Would some conditions such as auditing and read-filtering be not allowed on the policy match?

3.4. Encryption and Integrity

Encryption is used to provide data privacy. The real question is do we need to encrypt the data to retain its data.

- I2RS Client to Agent: Is encryption a recommendation or requirement?

- o I2RS environment: Application to I2RS client: discuss encryption (pro/con)

- o I2RS environment: I2RS client to Routing System: discuss (pro/con)

What is needed for integrity of the data

3.5. stacked I2RS agents

It is possible to have the following hierarchical scenario:

I2RS client---->I2RSAgent=I2RSclient---I2RSAGent(nodes)

Questions:

- o Does this scenario bring unique security issues?

- o Is this scenario outside the I2RS venue

4. IANA Considerations

This draft includes no request to IANA.

5. Security Considerations

This is a document about security architecture beyond the consideration for I2RS

6. Informative References

[I-D.clarke-i2rs-traceability]
Clarke, J., Salgueiro, G., and C. Pignataro, "Interface to the Routing System (I2RS) Traceability: Framework and Information Model", draft-clarke-i2rs-traceability-00 (work in progress), September 2013.

[I-D.hares-i2rs-info-model-policy]
Hares, S. and W. Wu, "An Information Model for Network policy", draft-hares-i2rs-info-model-policy-01 (work in progress), February 2014.

[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-02 (work in progress), February 2014.

[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-02 (work in progress), February 2014.

[I-D.ji-i2rs-usecases-ccne-service]
Ji, X., Zhuang, S., Huang, T., and S. Hares, "I2RS Use Cases for Control of Forwarding Path by Central Control Network Element (CCNE)", draft-ji-i2rs-usecases-ccne-service-01 (work in progress), February 2014.

[I-D.keyupate-i2rs-bgp-usecases]
Patel, K., Fernando, R., Gredler, H., Amante, S., White, R., and S. Hares, "Use Cases for an Interface to BGP Protocol", draft-keyupate-i2rs-bgp-usecases-01 (work in progress), February 2014.

[I-D.white-i2rs-use-case]
White, R., Hares, S., and A. Retana, "Protocol Independent Use Cases for an Interface to the Routing System", draft-white-i2rs-use-case-02 (work in progress), February 2014.

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

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

Authors' Addresses

Susan Hares
Hickory Hill Consulting
7453 Hickory Hill
Saline, MI 48176
USA

Email: shares@ndzh.com

Wesley George
Time-Warner Cable

Email: wesley.george@twcable.com

Scott Brim
Consultant

Email: scott.brim@gmail.com

Nancy Cam-Winget
Cisco

Email: ncamwing@cisco.com

DaCheng Zhang
Huawei

Email: zhangdacheng@huawei.com

Qin Wu
Huawei

Email: bill.wu@huawei.com

Ahmed Abro
Cisco

Email: aabro@cisco.com

Salman Asadullah
Cisco

Email: sasad@cisco.com

Joel Halpern
Ericcson

Email: joel.halpern@ericsson.com

Eric Yu
Cisco

Email: eyu@cisco.com