I2RS working group                                           S. Hares
Internet-Draft                                                 Huawei
Intended status: Standards Track                              S. Brim
Expires: August 10, 2015                                  Consultant
                                                       N. Cam-Winget
                                                               Cisco
                                                          J. Halpern
                                                            Ericcson
                                                            D. Zhang
                                                               Q. Wu
                                                              Huawei
                                                             A. Abro
                                                        S. Asadullah
                                                               Cisco
                                                          J. Halpern
                                                            Ericcson
                                                               E. Yu
                                                               Cisco
                                                    February 6, 2015

                   I2RS Security Considerations
                    draft-hares-i2rs-security-03

Abstract

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

Status of This Memo

Copyright Notice

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 and
   configuration process (as illustrated in the diagram in the
   architecture document within routing elements.  The I2RS client
   [I-D.ietf-i2rs-architecture] interacts with one or more I2RS agents
   to collect information from network routing systems.  This security
   architecture expands on the security issues involved in the I2RS
   protocol's message exchange between the I2RS client and the I2RS
   agent which are described in [I-D.ietf-i2rs-architecture]

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.  This document discusses I2RS use of
Roles as Scope+Access where scope is the portion of the routing
tree, and access is permissions to read or write (or both).
Figure 1 replicates [RFC4949] diagram on RBAC roles and
assignments (page 254).

Role hierarchy or Permissions inheritance

[RFC4949] describes the hierarchy of roles and identities in role-
based access control shown in Figure 1 and described above.  I2RS
will used role-based access control as defined above, and shown in
Figure 2.

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] (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.  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 without detection.

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.

```
          (c) Permission Inheritance Assignments (i.e., Role Hierarchy)
                              [Constraints]
                                 +=====+
                                 |     |
               (a) Identity      v     v   (b) Permission
   +----------+  Assignments  +-------+  Assignments  +----------+
   |Identities|<=============>| Roles |<=============>|Permissions|
   +----------+ [Constraints] +-------+ [Constraints] +----------+
        |  |                     ^   ^
        |  |   +-----------+     |   |     +--------------------+
        |  |   | +-------+ |     |   |     |       Legend       |
        |  +===>|Session|=====+  |   |     |                    |
        |      | +-------+ |     |   |     |     One-to-One      |
        |      |   ...     |     |   |     | ================== |
        |      | +-------+ |     |   |     |                    |
        +======>|Session|=========+  |     |     One-to-Many     |
   (d) Identity | +-------+ |  (e) Role    | =================> |
      Selections |          |  Selections  |                    |
   [Constraints]|   Access  |[Constraints] |     Many-to-Many    |
                |  Sessions |              | <================> |
                +----------+              +--------------------+
```
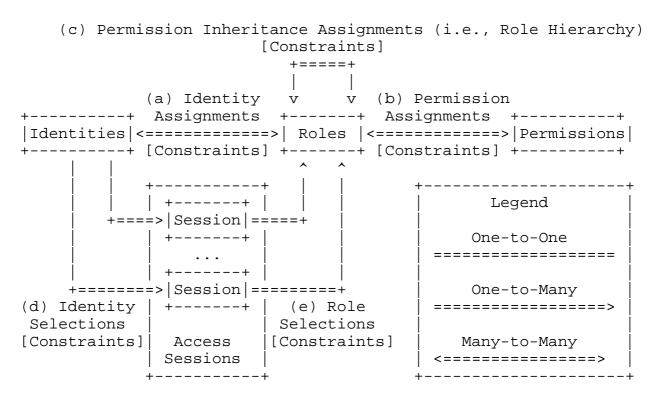
               Figure 1 - Security definition of Role inheritance

3.  Security Issues

   The security for the I2RS protocol utilizes the role based access
   security for the I2RS client's access to the I2RS agent's data (read/
   write).  The I2RS [I-D.ietf-i2rs-architecture]  treats the agent's

notification stream or publication stream as a pre-authorized read.
This security consideration document examines the major points:

I2RS roles and identities

   This section looks at how I2RS roles and identities created by
   [I-D.ietf-i2rs-architecture], how I2RS model derived from the
   security model of role-based access control matches the
   [I-D.ietf-i2rs-architecture], and how Identities and roles get
   distributed.

Data Security

   The data security section looks at incidents when the I2RS data
   stream will need confidentiality and message integrity, transport
   security, how role-based access control of I2RS data impacts the
   I2RS Information Model and Data Model design, and light weight
   clients who work without confidentiality.

4.  Security roles and Identities for the I2RS client and I2RS Agent

   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
   client and 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 (via internal policy) to one role.  The
   context of the I2RS client-agent communication is based on a role
   which may/may not require message confidentiality, message integrity
   protection, or replay attack protection.

   The rigorous definition of a role in RBAC-based security is role is
   function associated with an activity (set of actions).  The set of
   actions in I2RS performs is limited are read or write actions on a
   specific set of data in the data model.  Therefore, we can express:

      Role = routing tree + Read/Write/Read-Write

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 exists even if 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 I2RS client software could arrange to store multiple secure identities, and use a specific identity that only associates roles which only have Read access. This administrative design of identities and roles could insure a "status-only" application did gain write access.  This administrative design is possible within I2RS architecture but not mandated.

Multiple identities provide some secondary level support for the application-client, but may grow the number of identities.  The multiple identities per client could also be used for multiple levels of security for the data passed between an I2RS client and agent as either: a) confidential, b) authorized with message integrity protection, c) authorized without message integrity protection, and or d) no protection.

5.  I2RS Data Security

I2RS data security involves determining of the I2RS client to I2RS agent data transfer needs to be confidential, or have message integrity, or support an end-to-end integrity (in the case of stacked clients).  This section discuss the consideration of I2RS data security.

It is assumed that all 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 to help 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 monkeys.

## 5.1.  Data Confidentiality Requirements

In a critical infrastructure, certain data within routing elements is
sensitive and R/W 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.

## 5.2.  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 t 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.

6.  Open Issues

   The following are open issues for the I2RS WG to discuss:

   Unencrypted Message Exchanges

      The I2RS Security discussion group believes that encrypting all
      the data messages is the best approach for security.  Some I2RS WG
      discussion has indicated a desire for the the I2RS client-agent
      message exchanges to be unencrypted.  The discussion group needs
      the I2RS WG members to provide more detail since a mixture of
      encrypted and unencrypted data will require more complexity in the
      Information Model (IM) and Data Model (DM).

   Transport requirements

      The architecture provides the ability to have multiple transport
      sessions providing protocol and data communication between the
      I2RS Agent and the I2RS client.  The discussion group proposed on
      mandatory secure transport.  Should there be one mandatory secure
      transport protocol or multiple allowable protocols?

   Auditable Data Streams

      Auditable data streams does not have a security consideration
      because I2RS is not inventing a new audit protocol as many
      protocols (syslog) are available to be used.  Verifying audit
      stream data is outside the I2RS protocol, but those designing the
      IM and DMs with audit stream capability need to provide the
      appropriate hooks such as: on/off action, data selection, and
      protocol (for example syslog) that the I2RS Agent (or I2RS routing
      system) sends the audit data upon.

7.  Acknowledgement

   The authors would like to thank Wes George, Ahmed Abro, Qin Wu, Eric
   Yu, Alia Atlas, and Jeff Haas for their wonderful contributions to
   our discussion discussion.

8.  IANA Considerations

   This draft includes no request to IANA.

9.  Security Considerations

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

10.  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-02
            (work in progress), June 2014.

   [I-D.hares-i2rs-info-model-policy]
            Hares, S. and W. Wu, "An Information Model for Basic
            Network Policy", draft-hares-i2rs-info-model-policy-03
            (work in progress), July 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-08 (work in
            progress), January 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-rib-info-model]
            Bahadur, N., Folkes, R., Kini, S., and J. Medved, "Routing
            Information Base Info Model", draft-ietf-i2rs-rib-info-
            model-05 (work in progress), January 2015.

   [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-02 (work in progress), July 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-04 (work in
            progress), July 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-06 (work in progress), July 2014.

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

   [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.

Authors' Addresses

   Susan Hares
   Huawei
   7453 Hickory Hill
   Saline, MI  48176
   USA


   Email: shares@ndzh.com


   Scott Brim
   Consultant

   Email: scott.brim@gmail.com


   Nancy Cam-Winget
   Cisco

   Email: ncamwing@cisco.com


   Joel Halpern
   Ericcson

   Email: joel.halpern@ericsson.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