I2RS working group
Internet-Draft
Intended status: Informational
Expires: July 23, 2017

S. Hares
Huawei

January 19, 2017

I2RS Revision to Yang Module Security Considerations Section
draft-hares-i2rs-yang-sec-consider-00

Abstract

This document suggests changes to the yang security considerations section for yang module draft supporting the I2RS protocol security requirements.

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 23, 2017.

Table of Contents

1. Introduction

This document proposes language for the the security consideration section for Yang modules from the I2RS Working group which utilize the I2RS protocol enhancements to the NETCONF/RESTCONF. The I2RS protocol enhancement to the NETCONF/RESTCONF protocol must meet the protocol security requirements established in [I-D.ietf-i2rs-protocol-security-requirements], and the environment requirements set in [I-D.ietf-i2rs-security-environment-reqs].

[I-D.ietf-netmod-revised-datastores] desribes a revised network management datastore structure for management configuration data stores used for configuration and operational state. Within this

context, the I2RS protocol is a control plane protocol which creates a control-plane datastore separate from the NETCONF/RESTCONF configuration datastores which are write-able (candidate, running, and startup datstores) or expanded uninstalled configuration (intended datastores). The I2RS protocol creates the I2RS ephemeral datastore which is one of the control plane datastores. Any I2RS protocol implementation merges the control plane datastore with the processed intended datastore (removing missing resources or delays) to create the applied datastore. The I2RS ephemeral datastore is defined by the YANG data modeling language augmenting to support the I2RS protocol's control plane ephemeral datastore.

The I2RS YANG data models exist in the I2RS ephemeral control plane datastore. Some I2RS Yang Models exist only within the I2RS protocol's ephemeral control plane datastore. Some YANG models which augment configuration datastore and operational state modules. These I2RS YANG data models may augment YANG models for system functions (e.g. interface Yang model), routing information models (RIBS), routing protocol models, or network management protocol. I2RS YANG models MAY import data from the routing system (e.g. OSPF state topology models for L3).

The format of this document is:

- section 2 - compares I2RS protocol security requirements with requirements describe in yang module security considerations found at https://trac.ietf.org/trac/ops/wiki/yang-security-guidelines.

- section 3 - suggests new Explanatory text for Yang module security considerations for I2RS yang modules, and

- section 4 - suggests a new template for Security Considerations section for any I2RS yang module or any module based on an I2RS yang module.

2. Basic Yang Security Considerations versus I2RS Yang Security Considerations

The I2RS mandatory-to-implement protocol security features are different than the basic NETCONF [RFC6241] mandatory-to-implement features or RESTCONF mandatory-to-implement features [I-D.ietf-netconf-restconf] in the following way:

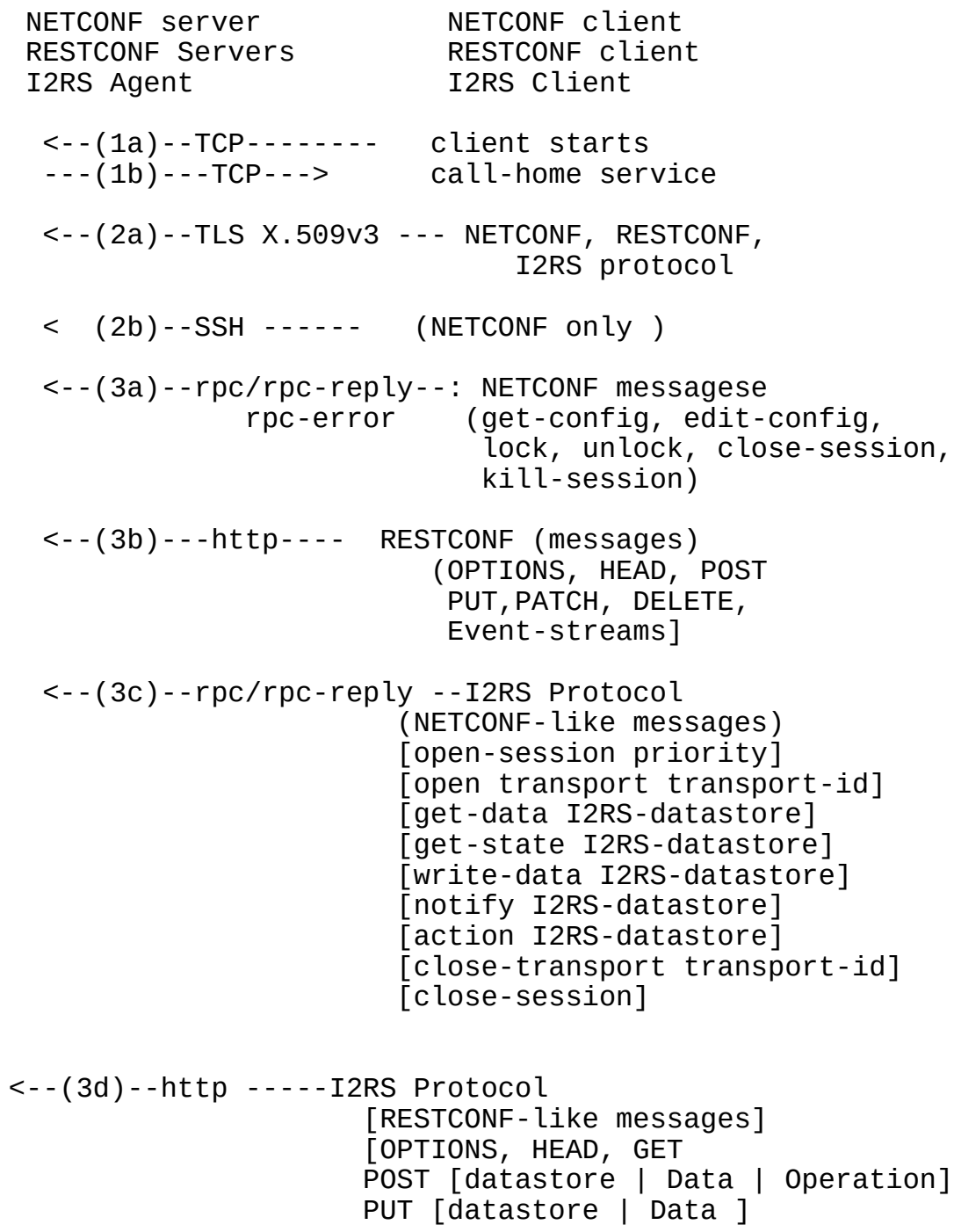
- different mandatory transport features,

- I2RS Protocol supports a priority and secondary opaque associated with each Peer Identity,

- o I2RS Yang Models exist in control plane data stores rather than in the configuration data stores,
- o Different validation processes,
- o different NACM policies,
- o optional non-secure transport can be used for a restricted set of non-confidential data that does not have privacy issues.

2.1. Mandatory to implement transport layer

NETCONF [RFC6241] and RESTCONF [I-D.ietf-netconf-restconf] utilize secure transports to establish a session between a server on a network node and a client (often on a end-system). The secure transport layer in these two protocol is a lower layer than the application layer exchange between the server and client. Figure 1 provides shows how NETCONF, RESTCONF, and I2RS start their transport connections (1a or 1b), establish secure connections (2a or 2b), and send messges between a client and an NETCONF/RESCONF or I2RS agent.



Note, in the drawing above, the I2RS agent features MAY utilize the NETCONF server methodology with different protocol commands (get-data, get-state, write-data, notify, action) which can be directed at a particular datastore.

Similarily, the RESTCONF methodology can be augmented with different commands to reference the I2RS datastore.

This section reviews the manadatory to implement secure transport layer for NETCONF, RESTCONF, and I2RS protocol. For NETCONF, the I2RS agent features utilizes the NETCONF server functions, but allows multiple trasnports between the I2RS Client and I2RS Agent. For RESTCONF, the I2RS agent features utilize the RESTCONF server functions. Based on this review, it suggest I2RS Yang modules must utilize a TLS connection with X.509v3.

2.1.1. Mandatory to implement NETCONF Transport Layer

NETCONF's [RFC6241] mandatory-to-implement transport (SSH) [RFC6242] augmented by NETCONF's access control module [RFC6536] provides security for Data passed via NETCONF. NETCONF allows user to run NETCONF over TLS using X.509 authentication [RFC7589] which mandates support for of TLS 1.2 [RFC5246] with its mandatory-to-implement Cipher suite ("TLS_RSA_WITH_AES_CBC_SHA"), and suggests implementers abide by recommendations in [RFC7525].

2.1.2. Mandatory to implement RESTCONF Transport Layer

RESTCONF [I-D.ietf-netconf-restconf] MUST operate over HTTP over the TLS using TLS [RFC7230] [RFC5246] with the https URI scheme with port 443. RESTCONF server MUST present an X.509v3 based certificate when establishing a connection with an RESTCONF Client. The RESTCONF use of X.509v3 certifications is consistent with NTECONF use of X.509 ceritifications.

2.1.3. Mandatory to implement I2RS Transport Layer

The I2RS protocol security requirements [I-D.ietf-i2rs-protocol-security-requirements] require I2RS Yang modules to be accessed peer [identity] authentication, confidentiality, data integrity, and [practical] replay protection for I2RS messages" and support "mechanism that mitigate DoS attacks" and "DDos prevention" SEC-REQ-01 to SEC-REQ-05, SEC-REQ-09 to SEQ-REQ-11). The I2RS client and I2RS Agent MUST use mutual peer authentication based on unique identifier (see SEC-REQ-01, SEC-REQ-02, SEC-REQ-03).

The I2RS transport layer transport protocol "MUST be associated with a key management system that guarantees that only the entities having sufficient privileges can get the keys to encrypt/decrypt the sensitive data" (see SEC-REQ-12). The transport protocol the I2RS messages are passed over MUST be able to support multiple transport between the I2RS client and I2RS Agent, but a single connection

between I2RS client and I2RS Agent MAY elect to use one transport (SEC-REQ-14).

The security association between an I2RS Agent and I2RS client continues even when a secure transport connections (TLS over TCP) exists. Therefore, all I2RS clients receiving a message over a secure connection to an I2RS agent MUST confirm that the I2RS agent has a valid identifier (SEC-REQ-05) and all I2RS agents recieving a messages over a secure connection from an I2RS client MUST confirm that the I2RS client has a valid identity (SEC-REQ-04).

According to [I-D.ietf-taps-transports], the secure transport protocols which support peer authentication, confidentiality, data integrity, and replay protection are the following:

1. TLS [RFC5246] over TCP or SCTP,

2. DTLS over UDP with replay detection and anti-DoS stateless cookie mechanism required for the I2RS protocol, and the I2RS protocol allow DTLS options of record size negotiation and and conveyance of "don't" fragment bits to be optional in deployments.

3. HTTP over TLS (over TCP or SCTP), and

4. HTTP over DTLS (with the requirements and optional features specified above in item 2).

2.1.4. Change to Security Considerations for Mandatory Transport Layer

Based on these additional requirements, the mandatory-to-implement NETCONF transport for I2RS Yang modules is NETCONF over TLS with Mutual X.509 authentication [RFC7589] augmented by NETCONF's access control module. The mandatory-to-implement RESTCONF transport for I2RS YANG Modules is HTTP over TLS with mutual X.509 authentication.

This requirement should replace the existing requirement for the NETCONF transport of SSH [RFC6242] in the Yang modules.

2.2. Priority and Opaque Secondary Identity

The I2RS protocol security requirements require that a priority and a secondary opaque identifier be associated with the primary I2RS identifier (client or agent) (see SEC-REQ-07 and SEC-REQ-08). In NETCONF the X.509v3 identity which is used for mutual authentication, becomes a NETCONF user name. NETCONF links a NTECONF user name to a NETCONF group. Network access control policy [I-D.ietf-netconf-rfc6536bis] is associated with this user name for the configuration datastore. In RESTCONF, the X.509v3 identity used

for mutual authentication, becomes a RESTCONF user name. Similar to NETCONF the RESTCONF user name links to a RESTCONF user name. RESTCONF network access policy MAY link the RESTCONF user name to group identifier to apply NACM policy.

I2RS protocol links the X.509v3 identity which is used for X.509v3 mutual identification to a I2RS user identity (user-id) on the I2RS agent. Associated with the I2RS user-id is one priority per security session, one secondary identifier per protocol transaction (NETCONF or RESTCONF), and multiple transport sessions. The I2RS user-id links to a policy-id that can be utilized to set NAMCs on transports sessions or secondary identifiers, or other constraints.

This section describes the format of these user identifiers in X.509v3 use, and how I2RS uses the priority associated with the I2RS user-id.

2.2.1. TLS User-Id Formats

NETCONF over TLS with Mutual X.509 authentication [RFC7589] requires that the NETCONF server keep a order list of mapping of certificates to that the X.509v3 certification is mapped to a NETCONF user name. The mapping requires keeping ordered list of these mappings with each list entry containing the following:

- certificate fingerprint,
- map type (specified, san-rfc822-name, san-dns-name, san-ip-adderss, san-any, common-nam), and
- optional auxillary data.

The map type "specified" indicates the NETCONF username is specified in the auxilary data. The map types begining with "san-..." indicate the user name is found in the subjectAltName and take a particular form (rfc822-name, dns-name, ip-address) or anyone of these forms (san-any). The common-nam map type indicates CommonName is mapped to the user name after being converted to UTF-8.

In a similar fashion, the I2RS will utilize user name found in the formats as an I2RS identity.

2.2.2. I2RS use of priority

The I2RS data models define some data models which MUST exist within the I2RS protocol’s ephemeral datastore (e.g. I2RS Ephemeral Data Store, I2RS Protocol), and some which MAY exist (e.g. protocol independents models or modules which augment routing protocol

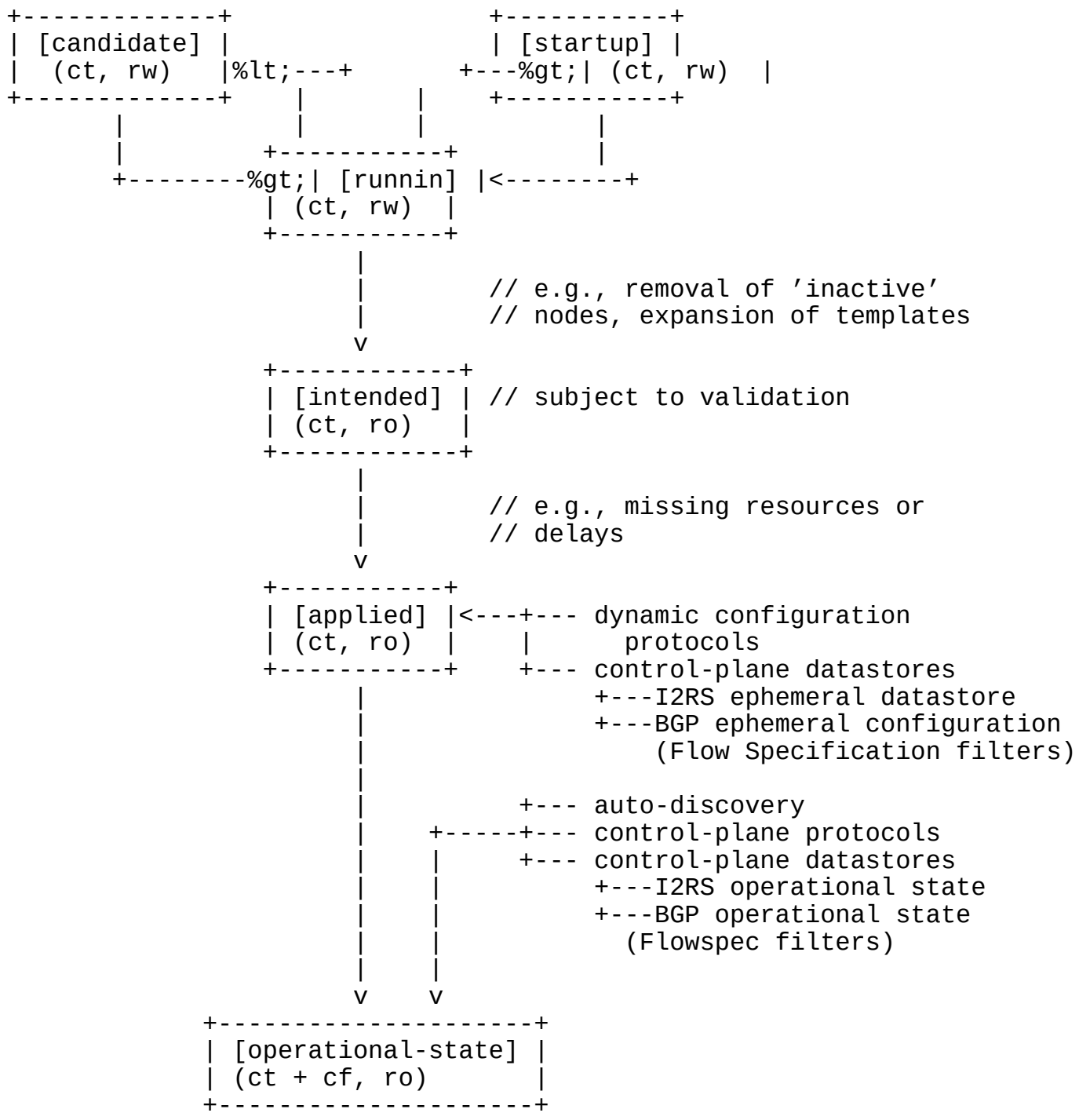
modules). The YANG Modules which define state in the I2RS Control plane data store may have both configuration state and operational state. The I2RS Data Models installed in an I2RS ephemeral state data MUST be able to be read by multiple I2RS Clients (if security network access policies allow it) and written by one I2RS Client at a time. If multiple I2RS client attempt to write the same I2RS data, it is considered an operational error situation (which causes I2RS agent to notify both client's about if security policies allow). To resolve these contentions, a priority scheme is used. The link between the I2RS client identity and the priority must be established before the I2RS Client makes write changes to the I2RS Agent. The client identity's link to a priority controls multiple write access rather than mutual identification.

How does the I2RS security requirement for a single to user to have only one priority (SEC-REQ-07) and one secondary opaque identifier (SEC-REQ-08) impact the security of I2RS Yang Data Models?

The client priority allows the I2RS agent to select which I2RS client has priority when multiple I2RS clients try to write the same data node in an I2RS ephemeral control plane datastore. This priority resolution of multiple writes occurs after both I2RS clients are allowed to have network access (policy set by NACM [I-D.ietf-netconf-rfc6536bis]) to a data model. Therefore, the security considerations of the I2RS YANG Data models do not have to consider priority contention. The secondary opaque associated for the period of a I2RS protocol operation only provides tracing capability to determine what happened.

2.3. I2RS Yang Models Exist in I2RS Ephemeral DataStores

The I2RS protocol is a higher layer protocol encourages which reuses other IETF protocols (NETCONF/RESTCONF) and modeling language (YANG), but modifies these protocols (NETCONF/RESTCONF) and the modeling language to support the required features. Figure 2 provides a diagram of how I2RS ephemeral configuration state ("config=true" nodes), and I2RS operational state nodes ("config=false" nodes) which are part of the I2RS Control Plane Ephemeral datastore interact with datastores in the updated IETF management datastore model [I-D.ietf-netmod-revised-datastores], and not a part of the configuration datastore. The I2RS protocol implementation merges the I2RS ephemeral datastore with currently appplied datastore.



ct = config true; cf = config false
rw = read-write; ro = read-only
boxes denote datastores

Figure 2 - modified from NETMOD Revised datastores (draft-ietf-netmod-revised-datastores-00.txt)

The I2RS ephemeral datastore is a control plane datastore which contains configuration data ("config=true") which does not persist over a reboot. The I2RS datastore may only be one of the ephemeral configuration datastores. The I2RS protocol creates, reads, writes, updates, deletes, notifies, signals events, performs actions,and traces (CRUD-NEAT) the data in the I2RS ephemeral datastore. The I2RS protocol mechanisms validate the I2RS ephemeral datastore values. If a routing system reboots, the information in an I2RS ephemeral datastore does not persist across the reboot.

2.3.1. Security Considerations for Datastore Interactions

An I2RS protocol implementation applies this configuration to a routing system which will also have basic IP routing functions (e.g. interfaces, IP address, routing), system management functions (e.g. syslog), and security functions (e.g. keystore, keychain, Network Access Control Management (NACM)). The I2RS implementation is required to have configuration knobs that will specify how the intended configuration is validated, checked, and merged with the I2RS ephemeral configuration state. If a system with I2RS protocol implementation also has dynamic configuration protocols (e.g. dhcp) or other control plane configuraton protocols (e.g. BGP Flow Specification filters passed in the BGP protocol, but defined to be installed as ephemeral state in the routing system), then the implementation must have configuration knobs and policy to merge the configuration (that is "config=true") data modules in a known manner. The applied configuration state stored by system must be able to identify which datastore (intended, dynamic configuration protocol datastore, I2RS ephemeral control-plane datastore) installed each piece of configuration in the running system.

Similar to NETCONF or RESTCONF configuration data stores (candidate, running, start-up, intended, and applied), some writable data nodes in a Yang Data Model that could be especially disruptive if abused. These data nodes MUST Be explicitly listed by name and the associated security risks MUST be spelled out. In addition, some writable data nodes in an I2RS ephemeral configuration could cause problems with nodes if: data models have write or read/write scoped data which can cause security threats by:

- I2RS ephemeral data read by the user could cause a security threats
- overwriting NETCONF/RESTCONF configuration with I2RS ephemeral control plane configurations could cause network security risks or Denial of Service (DoS),

- o fluctuating between I2RS ephemeral configuration datastore data and other control plane datastores could cause security risks or denial of service (DoS),

- o I2RS ephemeral configuration overwriting dynamic configuration protocol configuration (e.g. dhcp leases) could cause security risks or denial of service attacks (DoS), or fluctuation between I2RS ephemeral control plane confguration and dynamic configuration control plane could cause problems.

I2RS data models containing I2RS ephemeral configuration which might cause these problems should provide this information in the security considerations section.

Operational state contains all configured data used by the system ("config=true" nodes) and applied configuration and operational state as read-only data. Operational state data does not persist across a reboot of the routing system, but is regenerated. This requirement to regenerate data requires the I2RS protocol to reload any operational state it regenerates.

The I2RS protocol implementations MUST support I2RS Yang models which define operational state. System-wide operational state may come from auto-discovery, control plane protocols (e.g. BFD, BGP), or control plane datastores such as the I2RS Ephemeral Control Plane Datastore. The I2RS protocol implementation must extend the read of operational state so that the operational data may get all operational data, or data specific to the I2RS operational data.

I2RS ephemeral data store, similar to NETCONF/RESTCONF operational state, may have read-only data in the each ephemeral configuration datastore or the ephemeral operational datastores that contains especially sensitive information or that raise significant privacy concerns. It is important that the security section MUST be explicitly listed this data by name and the reasons for the sensitivity/privacy concerns MUST be explained.

I2RS ephemeral datastores may overwrite with ephemeral data sensitive information stored in NETCONF/RESTCONF configuration datastores or operational datastores. This overwriting may decrease the concerns for sensitivity/privacy of the information or increase it. The ovewriting and the policy that controls it must be explained in the I2RS Yang Data Model.

2.4. Different Validations

The I2RS protocol is to designed to operate on top of the operates on top of the TLS connection using modified network management protocols (NETCONF, RESTCONF, and others) to:

- create, read, update, delete ephemeral configuration data within the I2RS ephemeral data store (CRUD)
- to notify the I2RS client when an event occurs in the I2RS Agent, or the I2RS agent when an event occurs as part of a subscription servic,
- signal the occurrence of individual events (I2RS agent to I2RS client or I2RS client to I2RS agent),
- act if a action is request (e.g. rpc),
- trace information

(These can be summarizes as CRUD-NEAT operations).

The validation for these processes is specific to the I2RS protocol so the validations will be different, but defined in the I2RS protocol. Therefore, the security considerations will need to consider any differences in I2RS protocol features.

2.5. Different NACM Policy

The expanded NETCONF NACM [I-D.ietf-netconf-rfc6536bis] proposes changes to the NACM procedure so that it focuses on:

- Permission to invoke specific protocol operations,
- Permission to read and/or alter specific data nodes within any datastore,
- Permission to receive specific notification event types.

The NETCONF NACM is based on a netconf group’s permissions where each netconf user identifier is linked to 1 or more group permissions. NETCONF which runs over TLS with X.509v3 services [RFC7589] passes a name which becomes the netconf user name. As described above the I2RS protocol also a user name which becomes the I2RS usser identifier (user-id) The I2RS user-id may be mapped to different NACM policy based on a I@RS protocol implementation and the I2RS protocol features.

An I2RS protocol implementation also interacts with the following systems to import/export data: to the following:

routing system (defined as Routing Access Control Management (RACM)),

host system functions (defined as System Access control Management (SACM),

NACM policy for I2RS protocol will need to be augment by this RACM and SACM policy. A security consideration section should discuss these issues.

2.6. Optional Insecure Protocol

The I2RS protocol allow an implementation of I2RS protocol (NETCONF or RESTCONF) to optionally support of an insecure transport as well as a secure transport if a set of mandatory constraints are met. of the following constraints are met:

- the content that is suitable for insecure transport (see SEC-REQ-06),
- Yang models with non-confidential data must provide an indication that non-confidential data exists within the model in a machine readable form. A non-secure transport may be used to publish only read scope data or notification scope data if the associated data model indicates the data is non-confidential (see SEC-REQ-13),
- The I2RS protocol makes use of both secure and insecure transports, but this use MUST NOT be done in any way that weakens the secure transport protocol used in the I2RS protocol or other contexts that do not have this requirement for mixing secure and insecure modes of operation (SEC-REQ-16)
- The I2RS higher-layer protocol MUST provide a mechanism for message traceability (requirements in [RFC7922]) that supports the tracking higher-layer functions run across secure connection or a non-secure transport (SEC-REQ-19).

Any I2RS Data model proposing to transmit a portion of the data over an insecure transport MUST provide a section of security considerations that explains how these constraints are net.

3. I2RS YANG Model Security Explanation

Any security consideration section for an I2RS YANG data model must contain the following sections:

- Basic Yang Module Data considerations - relating to sensitive writeable nodes, sensitive read-able nodes, sensitive rpc operations),

- I2RS related Yang Model considerations - relating to mandatory transport, I2RS use of priority and opaque secondary identity, validation of I2RS protocol operations, NACM interactions in a multiple datastore (config + I2RS control plane datastore), and use of optional insecure data.

This section provide an overview of what goes in each of these two sections. Section 4 provides abbrev template for this information.

3.1. Basic YANG Model Security Considerations

Each specification that defines one or more YANG modules MUST contain a section that discusses security considerations relevant to those modules. The following data usage must be explained in the security consideratinon section:

1. If any writable data nodes that could be especially disruptive if abused, then these nodes MUST be explicitly listed by name and the associated security risks MUST be spelled out.

2. If any readable data nodes that contain especially sensitive information or that raise significant privacy concerns, then these data nodes MUST be explicitly listed by name and the reasons for the sensitivity/privacy concerns MUST be explained.

3. If any new RPC operations have been defined, then the security considerations of each new RPC operation MUST be explained.

3.2. I2RS YANG Model Security Considerations

The I2RS YANG Models is design to exists in the I2RS control plane ephemeral state. Therefore, a security consideration section for an I2RS YANG Data Model must contain the following information:

Mandatory requirement to run I2RS protocol over a TLS sesssion with X.509 mutual authentication whether I2RS protocol uses NETCONF-style messages or RESTCONF-style messages (I2RS protocol MUST not use NETCONF over SSH).

Description of how multiple client write-contentions are resolved via I2RS priority linked to the I2RS user-id and how I2RS secondary identity may trace this. It is important to provide operational insight how how I2RS secondary identity may change and how this will impact tracing.

Validation of I2RS protocol operations may be new. Any concerns with time delays or depth of validation, should be indicated.

NACM policy for network access to an I2RS Ephemeral control plane datastore may be augmented by an access control method for routing protocols (RACM), system information (SACM), and an inter-datastore access (DACM). A discussion how sensitive read information, write information, or I2RS actions are protected in the system.

If a portion of the data model is available via a non-secure transport session, describe how the following restrictions are met

* content of data is suitable for insecure transport,

* YANG modules provide indication of non-confidential data in machine readable form,

* the YANG module’s use of secure and insecure transport does not weaken the secure transport,

* the higher layer protocol MUST provide a mechnisms for message traceability.

4. Revised Security Considerations Template for I2RS Yang Modules

The YANG module defined in this draft is designed to be accessed via the I2RS control plane protocol and reside in the I2RS ephemeral control plane datastore that contains both configuration data and operational state. I2RS ephemeral control plane datastore does not persist (that is does not keep data) across a system reboot.

This consideration section for I2RS Yang Data Models contains three parts: basic YANG model considerations, I2RS ephemeral datstore considerations, and considerations for I2RS Yang Models with non-confidential data sent over an insecure session. The basic model security considerations are common to all YANG modules whether the YANG modules belong to the configuration datastore, or control-plane datastores.

Any I2RS Yang module is required to run the I2RS protocol over a TLS session with X.509v3 mutual authentication whether the I2RS protocol

uses NETCONF-style messages or RESTCONF-style messages. The I2RS protocol implementation uses the name passed as the I2RS user identifier (user-id). Write contention between two clients (with valid write permissions) attempting to write the same data node in a I2RS Yang data model is an operational error, but implementations should use the priority associated with each I2RS user-id to resolve it. Tracing of such content resolution will be done by the system, and will include the opaque secondary identifier which indicates which applications are operationally contending. Only one opaque secondary identifier is linked to a I2RS userid at a time, but the opaque secondary identifier may change multiple times during a security association. The opaque secondary identifier may be passed during transport connection establishment as part of a write-action (write datastore where the datastore is I2RS). All of these features are basic I2RS functionality, and not specific to any I2RS data model.

4.1. Basic YANG Model Security Considerations

What to put in this section: (Instructions to authors)

Each specification that defines one or more YANG modules MUST contain a section that discusses security considerations relevant to those modules. The following data usage must be explained in the security consideration.

1. If there is readable data nodes contain especially sensitive information or that raise significant privacy concerns, these nodes MUST be explicitly listed by name and the reasons for the sensitivity/privacy concerns MUST be explained. One is example is if the data might reveal customer information or violate personal privacy laws (such as those of the European Union) if the data was sent via an unauthorized port.

2. If any writable data nodes that could be especially disruptive if abused, these writeable data nodes MUST be explicitly listed by name and the associated security risks MUST be spelled out.

3. If thre are any new RPC operations have been defined, then the security considerations of each new RPC operation MUST be explained.

4.2. I2RS Yang Models for Secure-Only transports

The I2RS YANG models may utilize new rpc commands for to access the I2RS ephemeral datastore which create, read, update, and delete data nodes; or notify a client of informatio, signal events, perform actions, and perform tracing (CRUD-NEAT) notifies, signals events.

Authors should provide a list of any new rpc commands and any security considerations regarding their use.

NACM policy for network access to an I2RS Ephemeral control plane datastore may be augmented by an access control method for routing protocols (RACM), system information (SACM), and an inter-datastore access (DACM).

Authors should provide a discussion of any data which is retrieved from the routing protocols in the control plane system, system information, or from anyother datastore (configuration, operational state, dynamic configuration protocols, auto-discovery, control-plane protocols). Authors should discuss how fluctuation of the data retrieved from the routing protocols in control plane system, host system, or other datastores could impact data reliability or sensitive data nodes listed in the Basic Yang Module Security considerations. This discussion SHOULD include suggested operational knobs that control the overlay of I2RS configuration data over configuration data or I2RS operation state over other types of operational state.

4.3. I2RS Data Sent Across Insecure Transport

I2RS YANG Modules may contain data which MAY be passed across a non-secure transport session as well as a secure transport. Any I2RS YANG model sending allowing some data to be sent cross an non-secure transport MUST provide adhere to the following requirements:

- content of data model (e.g. nodes or subtrees) which is suitable for insecure transport,
- YANG modules provide indication of non-confidential data in machine readable form,
- how the YANG module’s use of secure and insecure transport does not weaken the secure transport,
- How I2RS protocol provide a mechnisms for message traceability.

Authors provide the following:

- a list of nodes in this YANG data model which MAY be passed across an insecure transport,
- How the YANG Module provides the indication of non-condidential data existing in the data model,

- How access to the data is limited to reads of data nodes, or notifications sent.
- How the use of secure and insecure transport does not weaken the secure transport operationally in a deployment, and
- How traceability supports detecting any security intrusions for this data model.

5. Security Considerations

The document provides an updated YANG security considerations for I2RS data models.

6. IANA Considerations

No IANA considerations for this requirements.

7. Acknowledgments

Authors of the protocol security document, protocol security environment document, ADs (routing, security, OPS)

8. References

8.1. Normative References

[I-D.ietf-i2rs-protocol-security-requirements]
Hares, S., Migault, D., and J. Halpern, "I2RS Security Related Requirements", draft-ietf-i2rs-protocol-security-requirements-17 (work in progress), September 2016.

[I-D.ietf-i2rs-security-environment-reqs]
Migault, D., Halpern, J., and S. Hares, "I2RS Environment Security Requirements", draft-ietf-i2rs-security-environment-reqs-02 (work in progress), November 2016.

[I-D.ietf-netconf-restconf]
Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", draft-ietf-netconf-restconf-18 (work in progress), October 2016.

[I-D.ietf-netmod-revised-datastores]
Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., and R. Wilton, "A Revised Conceptual Model for YANG Datastores", draft-ietf-netmod-revised-datastores-00 (work in progress), December 2016.

[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>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

[RFC5264] Niemi, A., Lonnfors, M., and E. Leppanen, "Publication of Partial Presence Information", RFC 5264, DOI 10.17487/RFC5264, September 2008, <http://www.rfc-editor.org/info/rfc5264>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <http://www.rfc-editor.org/info/rfc6241>.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011, <http://www.rfc-editor.org/info/rfc6242>.

[RFC6536] Bierman, A. and M. Bjorklund, "Network Configuration Protocol (NETCONF) Access Control Model", RFC 6536, DOI 10.17487/RFC6536, March 2012, <http://www.rfc-editor.org/info/rfc6536>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <http://www.rfc-editor.org/info/rfc7230>.

[RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, <http://www.rfc-editor.org/info/rfc7525>.

[RFC7589] Badra, M., Luchuk, A., and J. Schoenwaelder, "Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication", RFC 7589, DOI 10.17487/RFC7589, June 2015, <http://www.rfc-editor.org/info/rfc7589>.

[RFC7920] Atlas, A., Ed., Nadeau, T., Ed., and D. Ward, "Problem Statement for the Interface to the Routing System", RFC 7920, DOI 10.17487/RFC7920, June 2016, <http://www.rfc-editor.org/info/rfc7920>.

[RFC7921] Atlas, A., Halpern, J., Hares, S., Ward, D., and T. Nadeau, "An Architecture for the Interface to the Routing System", RFC 7921, DOI 10.17487/RFC7921, June 2016, <http://www.rfc-editor.org/info/rfc7921>.

[RFC7922] Clarke, J., Salgueiro, G., and C. Pignataro, "Interface to the Routing System (I2RS) Traceability: Framework and Information Model", RFC 7922, DOI 10.17487/RFC7922, June 2016, <http://www.rfc-editor.org/info/rfc7922>.

[RFC7923] Voit, E., Clemm, A., and A. Gonzalez Prieto, "Requirements for Subscription to YANG Datastores", RFC 7923, DOI 10.17487/RFC7923, June 2016, <http://www.rfc-editor.org/info/rfc7923>.

8.2. Informative References

[I-D.ietf-i2rs-ephemeral-state]
Haas, J. and S. Hares, "I2RS Ephemeral State Requirements", draft-ietf-i2rs-ephemeral-state-23 (work in progress), November 2016.

[I-D.ietf-netconf-rfc6536bis]
Bierman, A. and M. Bjorklund, "Network Configuration Protocol (NETCONF) Access Control Model", draft-ietf-netconf-rfc6536bis-00 (work in progress), January 2017.

[I-D.ietf-taps-transports]
Fairhurst, G., Trammell, B., and M. Kuehlewind, "Services provided by IETF transport protocols and congestion control mechanisms", draft-ietf-taps-transports-14 (work in progress), December 2016.

Author’s Address

Susan Hares
Huawei
7453 Hickory Hill
Saline, MI 48176
USA

Email: shares@ndzh.com