< draft-ietf-i2rs-protocol-security-requirements-11.txt	draft-ietf-i2rs-protocol-security-requirements-12.txt >
I2RS working group S. Hares Internet-Draft Huawei Intended status: Informational D. Migault Expires: March 19, 2017 J. Halpern Ericsson September 15, 2016	I2RS working group S. Hares Internet-Draft Huawei Intended status: Informational D. Migault Expires: March 30, 2017 J. Halpern Ericsson September 26, 2016
I2RS Security Related Requirements draft-ietf-i2rs-protocol-security-requirements-11	I2RS Security Related Requirements draft-ietf-i2rs-protocol-security-requirements-12
Abstract	Abstract
This presents security-related requirements for the I2RS protocol which provides a new interface to the routing system described in the I2RS architecture document (RFC7921). The I2RS protocol is a re-use protocol implemented by re-using portions of existing IETF protocols and adding new features to these protocols. The I2RS protocol re-uses security features of a secure transport (E.g. TLS, SSH, DTLS) such as encryption, message integrity, mutual peer authentication,	This presents security-related requirements for the I2RS protocol which provides a new interface to the routing system described in the I2RS architecture document (RFC7921). The I2RS protocol is a re-use protocol implemented by re-using portions of existing IETF protocols and adding new features to these protocols. The I2RS protocol re-uses security features of a secure transport (E.g. TLS, SSH, DTLS) such as encryption, message integrity, mutual peer authentication,
skipping to change at *page 1, line 44*	**skipping to change at *page 1, line 44***
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 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."	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 March 19, 2017.	This Internet-Draft will expire on March 30, 2017.
Copyright Notice	Copyright Notice
Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.	Copyright (c) 2016 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	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
skipping to change at *page 2, line 34*	**skipping to change at *page 2, line 34***
2.1. Requirements Language . . . . 4 2.2. Security Definitions . . . . 5 2.3. I2RS Specific Definitions . . . . 5 3. Security Features and Protocols: Re-used and New . . . . . . 7 3.1. Security Protocols Re-Used by the I2RS Protocol . . . . . 7 3.2. New Features Related to Security . . . . 8 3.3. I2RS Protocol Security Requirements vs. IETF Management Protocols . . . . 9 4. Security-Related Requirements . . . . 10 4.1. I2RS Peers(agent and client) Identity Authentication . . 11 4.2. Identity Validation Before Role-Based Message Actions . . 12 4.3. Peer Identity, Priority, and Client Redundancy . . . . . 12 4.4. Multi-Channel Transport: Secure Transport and Insecure Transport . . . . 14 4.5. Management Protocol Security . . . . 16 4.6. Role-Based Data Model Security . . . . 17 4.7. Security of the environment . . . . 18 5. Security Considerations . . . . 18 6. IANA Considerations . . . . 18 7. Acknowledgement . . . . 18 8. References . . . . 18 8.1. Normative References . . . . 18 8.2. Informative References . . . . 19 Authors' Addresses 21	2.1. Requirements Language . . . . 4 2.2. Security Definitions . . . . 5 2.3. I2RS Specific Definitions . . . . 5 3. Security Features and Protocols: Re-used and New . . . . . . 7 3.1. Security Protocols Re-Used by the I2RS Protocol . . . . . 7 3.2. New Features Related to Security . . . . 8 3.3. I2RS Protocol Security Requirements vs. IETF Management Protocols . . . . 9 4. Security-Related Requirements . . . . 10 4.1. I2RS Peers(agent and client) Identity Authentication . . 11 4.2. Identity Validation Before Role-Based Message Actions . . 11 4.3. Peer Identity, Priority, and Client Redundancy . . . . . 12 4.4. Multi-Channel Transport: Secure Transport and Insecure Transport . . . . 13 4.5. Management Protocol Security . . . . 15 4.6. Role-Based Data Model Security . . . . 16 4.7. Security of the environment . . . . 17 5. Security Considerations . . . . 17 6. IANA Considerations . . . . 17 7. Acknowledgement . . . . 17 8. References . . . . 18 8.1. Normative References . . . . 18 8.2. Informative References . . . . 19 Authors' Addresses 20
1. Introduction	1. Introduction
The Interface to the Routing System (I2RS) provides read and write access to information and state within the routing process. An I2RS client interacts with one or more I2RS agents to collect information from network routing systems. [RFC7921] describes the architecture of this interface, and this documents assumes the reader is familiar with this architecture and its definitions. Section 2 highlights some of the references the reader is required to be familiar with.	The Interface to the Routing System (I2RS) provides read and write access to information and state within the routing process. An I2RS client interacts with one or more I2RS agents to collect information from network routing systems. [RFC7921] describes the architecture of this interface, and this documents assumes the reader is familiar with this architecture and its definitions. Section 2 highlights some of the references the reader is required to be familiar with.
skipping to change at *page 4, line 12*	**skipping to change at *page 4, line 12***
protocols (Radius over TLS or Diameter over TLS) to securely distribute identity information.	protocols (Radius over TLS or Diameter over TLS) to securely distribute identity information.
Section 3 provides an overview of security features and protocols being re-used (section 3.1) and the new security features being required (section 3.2). Section 3 also explores how existing and new security features and protocols would be paired with existing IETF management protocols (section 3.3).	Section 3 provides an overview of security features and protocols being re-used (section 3.1) and the new security features being required (section 3.2). Section 3 also explores how existing and new security features and protocols would be paired with existing IETF management protocols (section 3.3).

The new features I2RS extends to these protocols are a priority mechanism to handle multi-headed reads, an opaque secondary identifier to allow traceability of an application utilizing a specific I2RS client to communicate with an I2RS agent, and insecure transport constrained to be utilized only for read-only data which publically available data (e.g. public BGP Events, public telemetry information, web service available) and some legacy data.	The new features I2RS extends to these protocols are a priority mechanism to handle multi-headed writes, an opaque secondary identifier to allow traceability of an application utilizing a specific I2RS client to communicate with an I2RS agent, and insecure transport constrained to be utilized only for read-only data which publically available data (e.g. public BGP Events, public telemetry information, web service available) and some legacy data.
Section 4 provides the I2RS protocol security requirements by the following security features:	Section 4 provides the I2RS protocol security requirements by the following security features:
o peer identity authentication (section 4.1),	o peer identity authentication (section 4.1),
skipping to change at *page 7, line 24*	**skipping to change at *page 7, line 24***
The I2RS AAA protocols supporting the I2RS higher-layer protocol.	The I2RS AAA protocols supporting the I2RS higher-layer protocol.
The I2RS higher-layer protocol requires implementation of a I2RS secure-transport component protocol and the I2RS management component protocol. The I2RS AAA component protocol is optional.	The I2RS higher-layer protocol requires implementation of a I2RS secure-transport component protocol and the I2RS management component protocol. The I2RS AAA component protocol is optional.
3. Security Features and Protocols: Re-used and New	3. Security Features and Protocols: Re-used and New
3.1. Security Protocols Re-Used by the I2RS Protocol	3.1. Security Protocols Re-Used by the I2RS Protocol
I2RS also requires a secure transport protocol and key distribution protocols. The secure transport features required by I2RS are peer authentication, confidentiality, data integrity, and replay protection for I2RS messages. According to [I-D.ietf-taps-transports], the secure transport protocols which support peer authentication, confidentiality, data integrity, and replay protection are the following:	I2RS requires a secure transport protocol and key distribution protocols. The secure transport features required by I2RS are peer authentication, confidentiality, data integrity, and replay protection for I2RS messages. 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,	1. TLS [RFC5246] over TCP or SCTP,
2. DTLS over UDP with replay detection and anti-DoS stateless cookie	2. DTLS over UDP with replay detection and anti-DoS stateless cookie
skipping to change at *page 7, line 46*	**skipping to change at *page 7, line 46***
allow DTLS options of record size negotiation and and conveyance of "don't" fragment bits to be optional in deployments.	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	3. HTTP over TLS (over TCP or SCTP), and
4. HTTP over DTLS (with the requirements and optional features specified above in item 2).	4. HTTP over DTLS (with the requirements and optional features specified above in item 2).
The following protocols will need to be extended to provide confidentiality, data integrity, peer authentication, and key distribution protocols: SSH, SCTP, or the ForCES TML layer over SCTP.	The following protocols will need to be extended to provide confidentiality, data integrity, peer authentication, and key distribution protocols: IPFIX (over SCTP, TCP or UDP) and ForCES TML layer (over SCTP). These protocols will need extensions to run over a secure transport (TLS or DTLS) (see section 3.3 for details).
The specific type of key management protocols an I2RS secure transport uses depends on the transport. Key management protocols utilized for the I2RS protocols SHOULD support automatic rotation.	The specific type of key management protocols an I2RS secure transport uses depends on the transport. Key management protocols utilized for the I2RS protocols SHOULD support automatic rotation.
An I2RS implementer may use AAA protocols over secure transport to distribute the identities for I2RS client and I2RS agent and role authorization information. Two AAA protocols are: Diameter [RFC6733] and Radius [RFC2865]. To provide the best security I2RS peer identities, the AAA protocols MUST be run over a secure transport	An I2RS implementer may use AAA protocols over secure transport to distribute the identities for I2RS client and I2RS agent and role authorization information. Two AAA protocols are: Diameter [RFC6733] and Radius [RFC2865]. To provide the best security I2RS peer identities, the AAA protocols MUST be run over a secure transport
skipping to change at *page 8, line 35*	**skipping to change at *page 8, line 39***
The I2RS client with the highest priority will have its write succeed. This document specifies requirements for this new concept of priority.	The I2RS client with the highest priority will have its write succeed. This document specifies requirements for this new concept of priority.
The opaque secondary identifier identifies an application which is using the I2RS client to I2RS agent communication to manage the routing system. The secondary identifier is opaque to the I2RS protocol. In order to protect personal privacy, the secondary identifier should not contain personal identifiable information.	The opaque secondary identifier identifies an application which is using the I2RS client to I2RS agent communication to manage the routing system. The secondary identifier is opaque to the I2RS protocol. In order to protect personal privacy, the secondary identifier should not contain personal identifiable information.
The last new security feature is the ability to allow non-confidential data to be transfered over a non-secure transport. It is expected that most I2RS data models will describe information that will be transferred with confidentiality. Therefore, any model which transfers data over a non-secure transport is marked. The use of a non-secure transport is optional, and an implementer SHOULD create knobs that allow data marked as non-confidential to be sent over a secure transport.	The last new feature related to I2RS security is the ability to allow non-confidential data to be transferred over a non-secure transport. It is expected that most I2RS data models will describe information that will be transferred with confidentiality. Therefore, any model which transfers data over a non-secure transport is marked. The use of a non-secure transport is optional, and an implementer SHOULD create knobs that allow data marked as non-confidential to be sent over a secure transport.
Non-confidential data can only be read or notification scope transmission of events. Non-confidential data cannot be write scope or notification scope configuration. An example of non-confidential data is the telemetry information that is publically known (e.g. BGP route-views data or web site status data) or some legacy data (e.g. interface) which cannot be transported in secure transport. The IETF I2RS Data models MUST indicate in the data model the specific data which is non-confidential.	Non-confidential data can only be read or notification scope transmission of events. Non-confidential data cannot be write scope or notification scope configuration. An example of non-confidential data is the telemetry information that is publically known (e.g. BGP route-views data or web site status data) or some legacy data (e.g. interface) which cannot be transported in secure transport. The IETF I2RS Data models MUST indicate in the data model the specific data which is non-confidential.
Most I2RS data models will expect that the information described in	Most I2RS data models will expect that the information described in

the model will be transferred with confidentiality. Therefore, it is

3.3. I2RS Protocol Security Requirements vs. IETF Management Protocols

Table 1 below provides a partial list of the candidate management protocols and the secure transports each one of the support. One column in the table indicates the transport protocol will need I2RS security extensions.

skipping to change at *page 10, line 20*

Mangement Protocol	Transport Protocol	I2RS Extensions
RESTCONF	HTTP over TLS with X.509v3 certificates, certificate validation, mutual authentication: 1) authenticated server identity, 2) authenticated client identity (*1)	None required (*2)
FORCES	TML overs SCTP (*1)	Needs extension to run TML over TLS over SCTP, or DTLS described above. The IPSEC mechanism is not sufficient for I2RS traveling over multiple hops (router + link) (*2)
IPFIX	SCTP, TCP, UDP TLS or DTLS for secure client (*1)	Needs to extension to support TLS or DTLS with options described above. (*2)

*1 - Key management protocols MUST support appropriate key rotation.

*2 - Identity and Role authorization distributed by Diameter or Radius MUST use Diameter over TLS or Radius over TLS.

4. Security-Related Requirements

skipping to change at *page 11, line 23*

- o role-based security (section 4.6),
- o security environment (section 4.7)

The I2RS Protocol depends upon a secure transport layer for peer authentication, data integrity, confidentiality, and replay protection. The optional insecure transport can only be used restricted set of publically data available (events or information) or a select set of legacy data. Data passed over the insecure transport channel MUST not contain any data which identifies a person or any "write" transactions.

4.1. I2RS Peers(agent and client) Identity Authentication

The following requirements specify the security requirements for Peer Identity Authentication for the I2RS protocol:

- o SEC-REQ-01: All I2RS clients and I2RS agents MUST have an identity, and at least one unique identifier that uniquely identifies each party in the I2RS protocol context.

skipping to change at *page 19, line 36*

[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

the model will be transferred with confidentiality.

3.3. I2RS Protocol Security Requirements vs. IETF Management Protocols

Table 1 below provides a partial list of the candidate management protocols and the secure transports each one of the support. One column in the table indicates the transport protocol will need I2RS security extensions.

skipping to change at *page 9, line 34*

Mangement Protocol	Transport Protocol	I2RS Extensions
RESTCONF	HTTP over TLS with X.509v3 certificates, certificate validation, mutual authentication: 1) authenticated server identity, 2) authenticated client identity (*1)	None required (*2)
FORCES	TML over SCTP (*1)	Needs extension to TML to run TML over TLS over SCTP, or DTLS with options for replay protection and anti-DoS stateless cookie mechanism. (DTLS record size negotiation and conveyance of "don't" fragment bits are optional). The IPSEC mechanism is not sufficient for I2RS traveling over multiple hops (router + link) (*2)
IPFIX	SCTP, TCP, UDP TLS or DTLS for secure client (*1)	Needs to extension to support TLS or DTLS with options for replay protection and anti-DoS stateless cookie mechanism. (DTLS record size negotiation and conveyance of "don't" fragment bits are optional).

*1 - Key management protocols MUST support appropriate key rotation.

*2 - Identity and Role authorization distributed by Diameter or Radius MUST use Diameter over TLS or Radius over TLS.

4. Security-Related Requirements

skipping to change at *page 10, line 46*

- o role-based security (section 4.6),
- o security environment (section 4.7)

The I2RS Protocol depends upon a secure transport layer for peer authentication, data integrity, confidentiality, and replay protection. The optional insecure transport can only be used restricted set of publically data available (events or information) or a select set of legacy data. Data passed over the insecure transport channel MUST NOT contain any data which identifies a person or any "write" transactions.

4.1. I2RS Peers(agent and client) Identity Authentication

The following requirements specify the security requirements for Peer Identity Authentication for the I2RS protocol:

- o SEC-REQ-01: All I2RS clients and I2RS agents MUST have an identity, and at least one unique identifier that uniquely identifies each party in the I2RS protocol context.

skipping to change at *page 19, line 9*

[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-16 (work in progress), August 2016.	[I-D.ietf-i2rs-ephemeral-state] Haas, J. and S. Hares, "I2RS Ephemeral State Requirements", draft-ietf-i2rs-ephemeral-state-18 (work in progress), September 2016.
[I-D.ietf-netconf-restconf] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", draft-ietf-netconf-restconf-16 (work in progress), August 2016.	[I-D.ietf-netconf-restconf] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", draft-ietf-netconf-restconf-16 (work in progress), August 2016.
[I-D.ietf-taps-transports] Fairhurst, G., Trammell, B., and M. K&#258;&#378;hlewind, "Services provided by IETF transport protocols and congestion control mechanisms", draft-ietf-taps- transports-11 (work in progress), July 2016.	[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-11 (work in progress), July 2016.
[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <http://www.rfc-editor.org/info/rfc2865>.	[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <http://www.rfc-editor.org/info/rfc2865>.
[RFC4960] Stewart, R., Ed., "Stream Control Transmission Protocol", RFC 4960, DOI 10.17487/RFC4960, September 2007, <http://www.rfc-editor.org/info/rfc4960>.	[RFC4960] Stewart, R., Ed., "Stream Control Transmission Protocol", RFC 4960, DOI 10.17487/RFC4960, September 2007, <http://www.rfc-editor.org/info/rfc4960>.
End of changes. 18 change blocks.	
47 lines changed or deleted	***61 lines changed or added***

This html diff was produced by rfcdiff 1.41. The latest version is available from http://tools.ietf.org/tools/rfcdiff/