Internet Engineering Task Force (IETF)
Request for Comments: 6546
Obsoletes: 6046
Category: Standards Track
ISSN: 2070-1721

B. Trammell
ETH Zurich

April 2012

Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS

Abstract

The Incident Object Description Exchange Format (IODEF) defines a common XML format for document exchange, and Real-time Inter-network Defense (RID) defines extensions to IODEF intended for the cooperative handling of security incidents within consortia of network operators and enterprises. This document specifies an application-layer protocol for RID based upon the passing of RID messages over HTTP/TLS.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6546.

1. Introduction

The Incident Object Description Exchange Format (IODEF) [RFC5070] describes an XML document format for the purpose of exchanging data between Computer Security Incident Response Teams (CSIRTs) or those responsible for security incident handling for service providers (SPs). The defined document format provides a simple way for CSIRTs to exchange data in a way which can be easily parsed.

IODEF defines a message format, not a protocol, as the sharing of messages is assumed to be out of scope in order to allow CSIRTs to exchange and store messages in a way most suited to their established incident-handling processes. However, Real-time Inter-network Defense (RID) [RFC6545] does require a specification of a protocol to ensure interoperability among members in a RID consortium. This document specifies the transport of RID messages within HTTP [RFC2616] Request and Response messages over TLS [RFC5246] (herein, HTTP/TLS). Note that any IODEF message may also be transported using this mechanism, by sending it as a RID Report message.

1.1. Changes from RFC 6046

This document contains the following changes with respect to its predecessor [RFC6046]:

- The status of the document is Standards Track.
- The document is updated to refer to the updated RID specification, [RFC6545], where appropriate.
- Language regarding the use of HTTP/1.1 and TCP ports for RID transport is clarified.
- The RID-Callback-Token entity header field is added to allow matching of RID replies during callback, independent of the content of the underlying RID message.
- The minimum required version of TLS is upgraded to 1.1, and the minimum recommended version to 1.2.
- Language regarding PKI for RID over HTTPS is clarified, and updated to refer to [RFC6125].

This document obsoletes [RFC6046] and moves it to Historic status.

2. Terminology and Normative Sections

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

RID systems participating in a consortium are required to fully implement the protocol in Section 3 in order to interoperate within the consortium; the remainder of this document is informative and provides helpful background or explanatory information.

3. Transmission of RID Messages over HTTP/TLS

This section specifies the details of the transport of RID messages [RFC6545] over HTTP/TLS. In this arrangement, each RID server is both an HTTP/TLS server and an HTTP/TLS client. When a RID message is sent, the sending RID system connects to the receiving RID system and sends the message, optionally receiving a message in reply. Each RID system MUST be prepared to accept HTTP/TLS connections from any RID peer with which it communicates, in order to support callback for delayed replies (see below).

BCP 56 [RFC3205] contains a number of important considerations when using HTTP for application protocols. These include the size of the payload for the application, whether the application will use a web browser, whether the protocol should be defined on a port other than 80, and if the security provided through HTTP/TLS suits the needs of the new application.

It is acknowledged within the scope of these concerns that HTTP/TLS is not ideally suited for RID transport, as the former is a client-server protocol and the latter a message-exchange protocol; however, the ease of implementation of RID systems over HTTP/TLS outweighs these concerns. Consistent with BCP 56, RID systems listen for TCP connections on port 4590 (see Section 5). Every RID system participating in a consortium SHOULD listen for HTTP/TLS connections on the assigned port. RID systems MAY be configurable to listen on ports other than the well-known port; this configuration is out of scope for this specification. RID systems SHOULD NOT use TCP port 443 (the standard port for HTTP over TLS) for RID messages in order to avoid confusing standard HTTP/TLS servers for RID systems.

RID systems MUST implement all REQUIRED functionality for HTTP/1.1 [RFC2616]. All RID messages sent in HTTP Requests MUST be sent using the POST method with a Request-URI of '/'. As RID documents are XML, the RID media type is 'text/xml'; i.e., the 'Content-type' Request and Response headers MUST be 'text/xml'. As RID messages MUST be sent using the POST method, the GET and HEAD methods have no

particular meaning on a RID system; a RID system SHOULD answer 'GET /' or 'HEAD /' with 204 No Content. Other Request-URIs are reserved for future use; any access to Request-URIs other than '/' by any method on a RID system SHOULD return the appropriate HTTP error (404 Not Found).

Since the content of RID messages is essentially declarative, a RID system interrupted during transport MAY simply repeat the transaction; the sending of a RID message is idempotent.

As the queries and replies in a RID message exchange may be significantly separated in time, RID over HTTP/TLS supports a callback mechanism. In this mechanism, the receiving RID system MAY return a 202 Accepted response, called a RID callback, instead of a RID message. The RID callback MUST contain a zero-length entity body and a 'RID-Callback-Token' entity header field, itself containing a unique token generated by the receiving RID system.

The RID-Callback-Token is an opaque, whitespace-free string of up to 255 printable ASCII characters that MUST uniquely identify the callback among all callbacks from the receiving RID system to the sending RID system. Due to the amount of time that may be required to generate a RID Result or Report response, there is no upper bound on the time period for this uniqueness requirement. The RID-Callback-Token in ABNF [RFC5234] form is shown below:

```
callback-token = 1*255(VCHAR)
```

When performing RID callback, a responding system MUST connect to the host at the network-layer address from which the original request was sent; there is no mechanism in RID for redirected callback. This callback SHOULD use TCP port 4590 unless configured to use a different port.

While a RID system SHOULD return the reply in an HTTP Response if it is available immediately or within a generally accepted HTTP client timeout (about thirty seconds), this is not mandatory, and as such RID systems MUST be prepared for a query to be met with a 202 Accepted, an empty Response body, a connection termination, and a callback. Note that all RID messages require a response from the receiving RID system, so a sending RID system can expect either an immediate response or a callback.

Table 1 lists the allowable RID message types in an HTTP Response for a given RID message type in the Request. A RID system MUST be prepared to handle an HTTP Response of the given type(s) when sending

the corresponding HTTP Request. A RID system MUST NOT send an HTTP Response containing any RID message other than the one corresponding to the one sent in the HTTP Request.

Request RID type	Callback	Result	Response RID type
InvestigationRequest		200	Acknowledgement
InvestigationRequest		200	Result
InvestigationRequest		200	Report
InvestigationRequest		202	[empty]
TraceRequest		200	Acknowledgement
TraceRequest		200	Result
TraceRequest		200	Report
TraceRequest		202	[empty]
Query		200	Acknowledgement
Query		200	Report
Query		202	[empty]
Acknowledgement	X	200	[empty]
Result	X	200	[empty]
Report		200	Acknowledgement
Report		200	[empty]
Report	X	200	[empty]

Table 1

The use of stable DNS names to address RID systems is RECOMMENDED; in addition to facilitating connection to RID systems within a consortium, these are to be used as reference identifiers for a RID system's peers. For security purposes, RID systems SHOULD NOT return 3xx Redirection response codes, and SHOULD NOT follow any 3xx Redirection. The protocol provides no in-band method for handling a change of address of a RID system.

If a RID system receives an improper RID message in an HTTP Request, it MUST return an appropriate 4xx Client Error result code to the requesting RID system. If a RID system cannot process a RID message received in an HTTP Request due to an error on its own side, it MUST return an appropriate 5xx Server Error result code to the requesting RID system.

Note that HTTP provides no mechanism for signaling to a server that a response body is not a valid RID message. If a RID system receives an improper RID message in an HTTP Response, or cannot process a RID message received in an HTTP Response due to an error on its own side,

it MUST log the error and present it to the RID system administrator for handling; the error logging format is an implementation detail and is considered out of scope for this specification.

RID systems MUST support and SHOULD use HTTP/1.1 persistent connections as described in [RFC2616]. RID systems MUST support chunked transfer encoding on the HTTP server side to allow the implementation of clients that do not need to pre-calculate message sizes before constructing HTTP headers.

RID systems MUST use TLS version 1.1 [RFC4346] or higher for confidentiality, identification, and authentication, when sending RID messages over HTTPS. HTTPS is specified in Section 2 of [RFC2818]. RID systems MUST use mutual authentication; that is, both RID systems acting as HTTPS clients and RID systems acting as HTTPS servers MUST be identified by an X.509 certificate [RFC5280]. Mutual authentication requires full path validation on each certificate, as defined in [RFC5280].

The TLS session MUST use non-NULL ciphersuites for authentication, integrity, and confidentiality. Sessions MAY be renegotiated within these constraints.

All RID systems SHOULD be identified by a certificate containing DNS-ID identifier as in Section 6.4 of [RFC6125]; the inclusion of Common Names (CN-IDs) in certificates identifying RID systems is NOT RECOMMENDED. RID systems MUST verify the reference identifiers of their peers against those stored in the certificates presented using one of the methods in the following paragraph. Wildcards MUST NOT appear in the DNS-ID or CN-ID of a certificate identifying a RID system.

RID systems MUST support the verification of certificates against an explicit whitelist of peer certificates. RID systems SHOULD support the verification of reference identifiers by matching the DNS-ID or CN-ID with a reverse DNS lookup of the connecting RID peer; this support SHOULD allow the lookup to be cached and/or done in advance in order to ensure verifiability during instability or compromise of DNS itself.

Additional general information on the use of PKI with RID systems is detailed in Section 9.3 of [RFC6545].

RID systems MUST support TLS version 1.1 and SHOULD support TLS version 1.2 [RFC5246]; RID systems MUST NOT request, offer, or use any version of SSL, or any version of TLS prior to 1.1, due to known security vulnerabilities in prior versions of the protocol; see Appendix E of [RFC5246] for more information.

4. Security Considerations

In addition to the final paragraphs in Section 3 on the use of TLS to secure RID message transport, all security considerations of related documents apply, especially the Incident Object Description Exchange Format (IODEF) [RFC5070] and Real-time Inter-network Defense (RID) [RFC6545]. The protocol described herein is built on the foundation of those documents; the security considerations contained therein are incorporated by reference.

5. IANA Considerations

Consistent with BCP 56 [RFC3205], since RID over HTTP/TLS is a substantially new service, and should be controlled at the consortium member network's border differently than HTTP/TLS, it requires a new port number. IANA has assigned port 4590/tcp to RID with service name "RID over HTTP/TLS".

6. Acknowledgements

The author would like to thank David Black for the review, and Kathleen Moriarty for work on earlier revisions of this specification. This work was partially supported by the European Union Seventh Framework Program under grant agreement 257315 (DEMONS).

7. References

7.1. Normative References

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

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[RFC5070] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident Object Description Exchange Format", RFC 5070, December 2007.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, March 2011.

[RFC6545] Moriarty, K., "Real-time Inter-network Defense (RID)", RFC 6545, April 2012.

7.2. Informative References

[RFC3205] Moore, K., "On the use of HTTP as a Substrate", BCP 56, RFC 3205, February 2002.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[RFC6046] Moriarty, K. and B. Trammell, "Transport of Real-time Inter-network Defense (RID) Messages", RFC 6046, November 2010.

Author’s Address

Brian Trammell
Swiss Federal Institute of Technology Zurich
Gloriastrasse 35
8092 Zurich
Switzerland

Phone: +41 44 632 70 13
EMail: trammell@tik.ee.ethz.ch