BEHAVE
Internet-Draft
Intended status: Standards Track
Expires: March 31, 2014

M. Petit-Huguenin
Impedance Mismatch
S. Nandakumar
G. Salgueiro
P. Jones
Cisco Systems
September 27, 2013

Traversal Using Relays around NAT (TURN) Uniform Resource Identifiers
draft-petithuguenin-behave-turn-uris-08

Abstract

This document specifies the syntax of Uniform Resource Identifier (URI) schemes for the Traversal Using Relays around NAT (TURN) protocol. It defines two URI schemes to provision the TURN Resolution Mechanism [RFC5928].

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 March 31, 2014.

Table of Contents

1. Introduction

This document specifies the syntax and semantics of the Uniform Resource Identifier (URI) scheme for the Traversal Using Relays around NAT (TURN) protocol.

The TURN protocol is a specification allowing hosts behind NAT to control the operation of a relay server. The relay server allows hosts to exchange packets with its peers. The peers themselves may also be behind NATs. RFC 5766 [RFC5766] defines the specifics of the TURN protocol.

The "turn" and "turns" URI schemes are used to designate a TURN server (also known as a relay) on Internet hosts accessible using the TURN protocol. With the advent of standards such as [WEBRTC], we anticipate a plethora of endpoints and web applications to be able to identify and communicate with such a TURN server to carry out the TURN protocol. This also implies those endpoints and/or applications to be provisioned with appropriate configuration required to identify

the TURN server. Having an inconsistent syntax has its drawbacks and can result in non-interoperable solutions. It can result in solutions that are ambiguous and have implementation limitations on the different aspects of the syntax and alike. The "turn/turns" URI scheme helps alleviate most of these issues by providing a consistent way to describe, configure and exchange the information identifying a TURN server. This would also prevent the shortcomings inherent with encoding similar information in non-uniform syntaxes such as the ones proposed in [WEBRTC], for example.

[RFC5928] defines a resolution mechanism to convert a secure flag, a host name or IP address, a potentially empty port, and a potentially empty transport to a list of IP address, port, and TURN transport tuples.

To simplify the provisioning of TURN clients, this document defines a TURN and a TURNS URI scheme that can carry the four components needed for the resolution mechanism.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] when they appear in ALL CAPS. When these words are not in ALL CAPS (such as "should" or "Should"), they have their usual English meanings, and are not to be interpreted as RFC 2119 key words.

3. Definitions of the TURN and TURNS URI

3.1. URI Scheme Syntax

A TURN/TURNS URI has the following formal ABNF syntax [RFC5234]:

```
turnURI       = scheme ":" host [ ":" port ]
                [ "?transport=" transport ]
scheme        = "turn" / "turns"
transport     = "udp" / "tcp" / transport-ext
transport-ext = 1*unreserved
```

<host>, and <port> are specified in [RFC3986]. While these two ABNF productions are defined in [RFC3986] as components of the generic hierarchical URI, this does not imply that that the turn and turns schemes are hierarchical URIs. Developers MUST NOT use a generic hierarchical URI parser to parse a turn or turns URI.

The <host>, <port> and <transport> components are passed without modification to the [RFC5928] algorithm. <secure> is set to false if

<scheme> is equal to "turn" and set to true if <scheme> is equal to "turns" and passed to the [RFC5928] algorithm with the other components.

3.2. URI Scheme Semantics

The "turn" and "turns" URI schemes are used to designate a TURN server (also known as a relay) on Internet hosts accessible using the TURN protocol. The TURN protocol supports sending messages over UDP, TCP or TLS-over-TCP. The "turns" URI scheme MUST be used when TURN is run over TLS-over-TCP (or in the future DTLS-over-UDP) and the "turn" scheme MUST be used otherwise.

The required <host> part of the "turn" URI denotes the TURN server host.

As specified in [RFC5766] and [RFC5928], the <port> part, if present, denotes the port on which the TURN server is awaiting connection requests. If it is absent, the default port is 3478 for both UDP and TCP. The default port for TURN over TLS is 5349.

4. Implementation Status

Note to RFC Editor: Please remove this section and the reference to [RFC6982] before publication.

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [RFC6982]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to [RFC6982], "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

4.1. turnuri

Organization: Impedance Mismatch

Name: turnuri 0.3.4 http://debian.implementers.org/stable/source/turnuri.tar.gz

Description: A reference implementation of this document and of RFC 5928 [RFC5928].

Level of maturity: Beta.

Coverage: Fully implements this specification and RFC 5928.

Licensing: AGPL3

Contact: Marc Petit-Huguenin <marc@petit-huguenin.org>.

4.2. libjingle

Organization: Google Inc.

Name: libjingle revision 4831 https://code.google.com/p/chromium/codesearch#chromium/src/third_party/libjingle/source/talk/app/webrtc/peerconnection.cc

Description: Libjingle is a set of components provided by Google to implement Jingle protocols XEP-166 (http://xmpp.org/extensions/xep-0166.html) and XEP-167 (http://xmpp.org/extensions/xep-0167.html).

Level of maturity: Beta.

Coverage: Implements draft-petithuguenin-behave-turn-uris-07 without IPv6. The turn and turns schemes are parsed, and TLS is used when the secure bit is set. The libjingle library does not use the SRV and NAPTR RR from the RFC 5928 resolution mechanism.

Licensing: BSD 3-clauses license.

Contact: https://code.google.com/p/chromium/

4.3. Firefox

Organization: Mozilla

Name: Firefox Aurora 21 http://hg.mozilla.org/mozilla-central/rev/6b5016ab9ebb

Description: Mozilla Firefox is a free and open source web browser.

Level of maturity: Beta.

Coverage: Implements draft-petithuguenin-behave-turn-uri-03 without RFC 5928. The mozilla code parses the turn and turns schemes but does not seems to use TLS.

Licensing: Mozilla Public License, v2.0.

Contact: http://www.mozilla.org/en-US/firefox/channel/

5. Security Considerations

Security considerations for the resolution mechanism are discussed in Section 5 of [RFC5928]. Note that this section contains normative text defining authentication procedures to be followed by turn clients when TLS is used.

The "turn" and "turns" URI schemes do not introduce any specific security issues beyond the security considerations discussed in [RFC3986].

While the turn and turns URIs do not themselves include the username or password that will be used to authenticate the TURN client, in certain environments, such as WebRTC, the username and password will almost certainly be provisioned remotely by an external agent at the same time as a turns URI is sent to that client. Thus, in such situations, if the username and password were received in clear there would be little or no benefit to using a turns URI. For this reason a TURN client MUST ensure that the username, password, and turns URI and any other security-relevant parameters are received with equivalent security before using the turns URI. Receiving those parameters over another TLS session can provide the appropriate level of security, if both TLS sessions are similarly parameterised, e.g. with commensurate strength ciphersuites.

6. IANA Considerations

This section contains the registration information for the "turn" and "turns" URI Schemes (in accordance with [RFC4395]).

6.1. TURN URI Registration

URI scheme name: turn

Status: permanent

URI scheme syntax: See Section 3.1.

URI scheme semantics: See Section 3.2.

Encoding considerations: There are no encoding considerations beyond those in [RFC3986].

Applications/protocols that use this URI scheme name:

> The "turn" URI scheme is intended to be used by applications with a need to identify a TURN server to be used for NAT traversal.

Interoperability considerations: N/A

Security considerations: See Section 5.

Contact: Marc Petit-Huguenin <petithug@acm.org>

Author/Change controller: The IESG

References: RFCXXXX

[[NOTE TO RFC EDITOR: Please change XXXX to the number assigned to this specification, and remove this paragraph on publication.]]

6.2. TURNS URI Registration

URI scheme name: turns

Status: permanent

URI scheme syntax: See Section 3.1.

URI scheme semantics: See Section 3.2.

Encoding considerations: There are no encoding considerations beyond those in [RFC3986].

Applications/protocols that use this URI scheme name:

> The "turns" URI scheme is intended to be used by applications with a need to identify a TURN server to be used for NAT traversal over a secure connection.

Interoperability considerations: N/A

Security considerations: See Section 5.

Contact: Marc Petit-Huguenin <petithug@acm.org>

Author/Change controller: The IESG

References: RFCXXXX

[[NOTE TO RFC EDITOR: Please change XXXX to the number assigned to this specification, and remove this paragraph on publication.]]

7. Acknowledgements

Thanks to Margaret Wasserman, Magnus Westerlund, Juergen Schoenwaelder, Sean Turner, Ted Hardie, Dave Thaler, Alfred E. Heggestad, Eilon Yardeni, Dan Wing, Alfred Hoenes, and Jim Kleck for the comments, suggestions and questions that helped improve the draft-petithuguenin-behave-turn-uri-bis document.

Many thanks to Cullen Jennings for his detailed review and thoughtful comments on the draft-nandakumar-rtcweb-turn-uri document.

Thanks to Bjoern Hoehrmann, Dan Wing, Russ Housley, S. Moonesamy, Graham Klyne, Harald Alvestrand, Hadriel Kaplan, Tina Tsou, Spencer Dawkins, Ted Lemon, Barry Leiba, Pete Resnick, and Stephen Farrell for the comments, suggestions and questions that helped improve this document.

The authors would also like to express their gratitude to Dan Wing for his assistance in shepherding this document. We also want to thank Gonzalo Camarillo, the Real-time Applications and Infrastructure Director, for sponsoring this document as well his careful reviews.

8. References

8.1. Normative References

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

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

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

[RFC5766] Mahy, R., Matthews, P., and J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", RFC 5766, April 2010.

[RFC5928] Petit-Huguenin, M., "Traversal Using Relays around NAT (TURN) Resolution Mechanism", RFC 5928, August 2010.

8.2. Informative References

[RFC4395] Hansen, T., Hardie, T., and L. Masinter, "Guidelines and Registration Procedures for New URI Schemes", BCP 35, RFC 4395, February 2006.

[WEBRTC] Bergkvist, A., Burnett, D., Jennings, C., and A. Narayanan, "WebRTC 1.0: Real-time Communication Between Browsers", World Wide Web Consortium WD WD-webrtc-20120821, August 2012, <http://www.w3.org/TR/2012/WD-webrtc-20120821>.

[RFC6982] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", RFC 6982, July 2013.

Appendix A. Examples

Table 1 shows how the <secure>, <port> and <transport> components are populated from various URIs. For all these examples, the <host> component is populated with "example.org".

URI	<secure>	<port>	<transport>
turn:example.org	false		
turns:example.org	true		
turn:example.org:8000	false	8000	
turn:example.org?transport=udp	false		UDP
turn:example.org?transport=tcp	false		TCP
turns:example.org?transport=tcp	true		TLS

Table 1

Appendix B. Design Notes

- One recurring comment was to stop using the suffix "s" on URI scheme, and to move the secure option to a parameter (e.g. ";proto=tls"). We decided against this idea because the STUN URI does not have a ";proto=" parameter and we would have lost the symmetry between the TURN and STUN URIs. A more detailed account of the reasoning behind this is available at <http://blog.marc.petit-huguenin.org/2012/09/on-design-of-stun-and-turn-uri-formats.html>

- Following the advice of RFC 4395 section 2.2., and because the TURN URI does not describe a hierarchical structure, the TURN URIs are opaque URIs.

- <password> is not used in the URIs because it is deprecated [RFC3986]. <username> and <auth> are not used in the URIs because they do not guide the resolution mechanism.

- As discussed at IETF 72 in Dublin, there is no generic parameters in the URI to prevent compatibility issues.

Appendix C. Release notes

This section must be removed before publication as an RFC.

C.1. Modifications between petithuguenin-behave-turn-uris-08 and petithuguenin-behave-turn-uris-07

- s/eventually/potentially/

- Changed the ABNF to use references from RFC 3986 instead of copying them.

- Converted the design note about hierarchical parsers into a MUST NOT statement.

- Updated the RFC 6982 forms for Chrome and Firefox.

- Added text in security section about verifying that username, password and uris are received over a secure connection.

Authors' Addresses

Marc Petit-Huguenin
Impedance Mismatch

Email: petithug@acm.org

Suhas Nandakumar
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134
US

Email: snandaku@cisco.com

Gonzalo Salgueiro
Cisco Systems
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
US

Email: gsalguei@cisco.com

Paul E. Jones
Cisco Systems
7025 Kit Creek Road
Research Triangle Park, NC 27709
US

Email: paulej@packetizer.com