BEHAVE
Internet-Draft
Intended status: Standards Track
Expires: August 5, 2012

M. Petit-Huguenin
Unaffiliated
S. Nandakumar
G. Salgueiro
P. Jones
Cisco Systems
February 2, 2012

Traversal Using Relays around NAT (TURN) Uniform Resource Identifiers
draft-petithuguenin-behave-turn-uris-00

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 that can be used to provision the configuration values needed by the resolution mechanism defined in [RFC5928].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79. This document may not be modified, and derivative works of it may not be created, except to format it for publication as an RFC or to translate it into languages other than English.

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 August 5, 2012.

Copyright Notice

Copyright (c) 2012 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 carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

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/turns" URI scheme is 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, an eventually empty port, and an eventually 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.

A reference implementation [REF-IMPL] is available.

2. Terminology

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].

"SHOULD", "SHOULD NOT", "RECOMMENDED", and "NOT RECOMMENDED" are

appropriate when valid exceptions to a general requirement are known to exist or appear to exist, and it is infeasible or impractical to enumerate all of them. However, they should not be interpreted as permitting implementors to fail to implement the general requirement when such failure would result in interoperability failure.

3. Syntax of a TURN or TURNS URI

3.1. URI Scheme Syntax

The "turn" URI takes the following form (the syntax below is non-normative):

```
turn:<userinfo>@<host>:<port>
turns:<userinfo>@<host>:<port>
```

Note that <userinfo> with the "@" (at) sign character, as well as the <port> part and the preceding ":" (colon) character, is OPTIONAL.

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

```
   turnURI       = scheme ":" [ userinfo "@" ] turn-host
                   [ ":" turn-port ] [ "?transport=" transport ]
   scheme        = "turn" / "turns"
   userinfo      = user [ ":" password ]
   user          = 1*(%x21-24 / %x26-39 / %x3B-3F / %x41-7F
                   / escaped)
                       ; The symbols "%", ":", "@", and symbols
                       ; with a character value below 0x21 may
                       ; be represented as escaped sequences.
   password      = 1*(%x21-24 / %x26-3F / %x41-7F / escaped)
                       ; The symbols "%", "@", and symbols with
                       ; a character value below 0x21 may be
                       ; represented as escaped sequences.
   transport     = "udp" / "tcp" / transport-ext
   transport-ext = 1*unreserved
   turn-host     = IP-literal / IPv4address / reg-name
   turn-port     = *DIGIT
   IP-literal    = "[" ( IPv6address / IPvFuture  ) "]"
   IPvFuture     = "v" 1*HEXDIG "." 1*( unreserved / sub-delims / ":" )
   IPv6address   =                            6( h16 ":" ) ls32
                   /                       "::" 5( h16 ":" ) ls32
                   / [               h16 ] "::" 4( h16 ":" ) ls32
                   / [ *1( h16 ":" ) h16 ] "::" 3( h16 ":" ) ls32
                   / [ *2( h16 ":" ) h16 ] "::" 2( h16 ":" ) ls32
                   / [ *3( h16 ":" ) h16 ] "::"    h16 ":"   ls32
                   / [ *4( h16 ":" ) h16 ] "::"              ls32
                   / [ *5( h16 ":" ) h16 ] "::"              h16
                   / [ *6( h16 ":" ) h16 ] "::"
   h16           = 1*4HEXDIG
   ls32          = ( h16 ":" h16 ) / IPv4address
   IPv4address   = dec-octet "." dec-octet "." dec-octet "." dec-octet
   dec-octet     = DIGIT                 ; 0-9
                   / %x31-39 DIGIT       ; 10-99
                   / "1" 2DIGIT          ; 100-199
                   / "2" %x30-34 DIGIT   ; 200-249
                   / "25" %x30-35        ; 250-255
   reg-name      = *( unreserved / pct-encoded / sub-delims )
   escaped       = "%" HEXDIG HEXDIG
```

<unreserved>, <sub-delims>, and <pct-encoded> are specified in [RFC3986].

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. The core rules <ALPHA>, <DIGIT> and <HEXDIGIT> are used as described in Appendix B of RFC 5234 [RFC5234].

The eventual <user> and <password> components are used as input for the TURN [RFC5766] protocol itself.

3.2. URI Scheme Semantics

The TURN protocol supports sending messages over UDP, TCP or TLS-over-TCP. The "turns" URI scheme SHALL be used when TURN is run over TLS-over-TCP (or in the future DTLS-over-UDP) and the "turn" scheme SHALL be used otherwise.

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

The <userinfo> part identifies the credentials required for the long-term credential mechanism as described in the section 10.2 of RFC 5389 [RFC5389].

The <port> part, if present, denotes the port on which the TURN server is awaiting connection requests. If it is absent, the default port SHALL be 3478 for both UDP and TCP. The default port for TURN over TLS SHALL be 5349.

The <userinfo> part specifies the username and password. Both the <user> and <password> values are UTF-8 encoded and escaped as per section 2.5 of RFC 3986 [RFC3986].

4. Security Considerations

Security considerations for the resolution mechanism are discussed in [RFC5928].

As described in Section 3.2.1 of STD 66 [RFC3986], having authentication information (specifically passwords) in a URI means that the URI must be handled carefully:

> The passing of authentication information in clear text has proven to be a security risk in almost every case where it has been used.

Section 3.2.1 contains advice on handling URI that contain passwords in the userinfo portion. Implementations of this specification MUST implement that advice.

Specifically if a URI that contains credentials leaks, then it would allow an attacker to use the TURN server which is referenced by the URI. Such an attack has two major impacts. First, it uses up the operator's bandwidth. Second, if the operator bills the user for TURN server usage, then it may expose the user to costs incurred by

the attacker. However, the attacker never obtains the user's private information, nor does this attack allow for traffic amplification.

The expected use environment mitigates to some degree concerns about TURN URIs compared to other URIs, such as HTTPS. First, users do not dereference TURN URIs directly. Instead, they are passed to the TURN stack. Thus, concerns about confusion or leakage due to the URI being displayed to the user are significantly reduced; indeed the URI need never be available to the user at all.

One of the primary use cases for a TURN URI with credentials is WebRTC. In this case, a web server will be offering a calling service and may have an associated TURN server it can use. In this case, the browser will need to use the TURN server and the browser has no long term or preexisting relationship with the TURN server. The web server needs to provide some credential to the client which it can use to access the TURN server. Since TURN authentication is via username and password, this implies that the credential is a username/password pair. While this must be transmitted securely (i.e., over HTTPS), the security properties are the same whether the password is carried separately or is part of the URL. Moreover, because the web server and TURN servers can cooperate, a new password can be issued for every call, making short-term credentials feasible and thus significantly mitigating the risk.

If a TURN URI is transferred between hosts, it MUST be done over a protocol that provides confidentiality such as HTTPS [RFC2818]. It is RECOMMENDED that the credential only be valid for a single call and preferably for no more than one day. That "preferably" is bad.

5. IANA Considerations

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

5.1. TURN URI Registration

URI scheme name: turn

Status: permanent

URI scheme syntax: See Section 3.

URI scheme semantics: See [RFC5928].

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 that might need access to a TURN server.

Interoperability considerations: N/A

Security considerations: See Section 4.

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.]]

5.2. TURNS URI Registration

URI scheme name: turns

Status: permanent

URI scheme syntax: See Section 3.

URI scheme semantics: See [RFC5928].

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 that might need access to a TURN server over a secure connection.

Interoperability considerations: N/A

Security considerations: See Section 4.

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. 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 their comments, suggestions and questions that helped to 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.

The <turn-port> and <turn-host> ABNF productions have been copied from the <port> and <host> ABNF productions from [RFC3986].

This document was written with the xml2rfc tool described in [RFC2629].

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.

[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.

7.2. Informative References

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

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

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, October 2008.

[RFC5769] Denis-Courmont, R., "Test Vectors for Session Traversal Utilities for NAT (STUN)", RFC 5769, April 2010.

[WEBRTC] W3C, "WebRTC 1.0: Real-time Communication Between Browsers".

<http://dev.w3.org/2011/webrtc/editor/webrtc.html>.

[REF-IMPL] Petit-Huguenin, MPH., "Reference Implementation of TURN resolver and TURN URI parser".

<http://debian.implementers.org/stable/source/turnuri.tar.gz>.

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		
turn:user:pwd@example.org	false		
turns:example.org	true		
turns:user:pwd@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

Table 2 shows how the <username>, <password> and <host> components are populated from various URIs. For all the examples, the secure component is populated with false and the port and transport components are empty.

URI	<username>	<password>	<host>
turn:example.org			example.org
turn:192.0.2.1			192.0.2.1
turn:[2001:DB8::1]			2001:DB8::1
turn:user@example.org	user		example.org
turn:user:pwd@example.org	user	pwd	example.org

Table 2

The following example produces the username and password used as example in section 2.4 of [RFC5769]:

turn:%E3%83%9E%E3%83%88%E3%83%AA%E3%83%83%E3%82%AF%E3%82%B9:The%C2%ADM%C2%AAtr%E2%85%A8@example.org

Appendix B. Release notes

This section must be removed before publication as an RFC.

B.1. Merge of draft-nandakumar-rtcweb-turn-uri-00 and draft-petithuguenin-behave-turn-uri-bis-05

- Changed author list.
- Draft is now standard track.
- Merged abstract, introduction, acknowledgement and security sections.
- Added two introductory paragraphs to the beginning iof the introduction.
- Took Section 3 and divided it into Section 3.1 URI Scheme Syntax and Section 3.2 URI Scheme Semantics.
- Explained that most components are passed as is to RFC 5928.
- Added username and password in ABNF.
- Added RFC 5389 as reference.
- Added examples.
- Updated design notes.
- Various minor nits and grammatical issues fixed.

B.2. Modifications between petithuguenin-05 and petithuguenin-04

- Nits.
- Fixed schemes registration.

B.3. Modifications between petithuguenin-04 and petithuguenin-03

- Fixed references code link.

B.4. Modifications between petithuguenin-03 and petithuguenin-02

- Updated RFC references.

B.5. Modifications between petithuguenin-02 and petithuguenin-01

- Nits.

B.6. Modifications between petithuguenin-01 and petithuguenin-00

- Shorten I-D references.

B.7. Design Notes

- As discussed in Dublin, there is no generic parameters in the URI to prevent compatibity issues.

Authors' Addresses

Marc Petit-Huguenin
Unaffiliated

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