

TRAM Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 21, 2016

A. Johnston
Avaya
J. Uberti
Google
J. Yoakum
K. Singh
Avaya
October 19, 2015

An Origin Attribute for the STUN Protocol
draft-ietf-tram-stun-origin-06

Abstract

STUN, or Session Traversal Utilities for NAT, is a protocol used to assist other protocols traverse Network Address Translators or NATs. This specification defines an ORIGIN attribute for STUN that can be used in similar ways to the HTTP header field of the same name. WebRTC browsers utilizing STUN and TURN would include this attribute which would provide servers with additional information about the STUN and TURN requests they receive. This specification defines the usage of the STUN ORIGIN attribute for web, SIP, and XMPP contexts.

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 April 21, 2016.

Copyright Notice

Copyright (c) 2015 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	2
1.1. Requirements Language	4
2. STUN ORIGIN attribute	4
2.1. Origin Matching Rules	5
2.2. STUN Usage	6
2.3. TURN Usage	6
2.4. NAT Behavior Discovery Usage	6
2.5. ICE Usage	6
2.6. Media Keep-Alive Usage	6
2.7. SIP Keep-Alive Usage	6
2.8. Multiple Origins	7
3. IANA Considerations	7
4. Security Considerations	7
5. Implementation Status	8
6. Acknowledgements	10
7. References	10
7.1. Normative References	10
7.2. Informative References	11
Authors' Addresses	12

1. Introduction

STUN, or Session Traversal Utilities for NAT [RFC5389], is a protocol used to assist other protocols traverse Network Address Translators or NATs. TURN, or Traversal Using Relays around NAT [RFC5766], is a STUN extension that allows endpoints to acquire a relayed address for media flows. It is most commonly used in conjunction with ICE, Interactive Connectivity Establishment [RFC5245], which is used to establish peer-to-peer flows between endpoints through NATs and firewalls.

STUN defines three authentication modes, depending on the STUN usage. For STUN binding requests sent between peers, such as for ICE connectivity checks, a short term authentication method is recommended. Each peer contributes random strings which are exchanged over signaling and used to authenticate the connectivity checks. For TURN, a usage of STUN used to acquire and refresh relay addresses, a long term authentication method is recommended. This

authentication is similar to SIP Digest [RFC3261], which involves an authentication challenge for each request. A server, upon receipt of a TURN request, generates an authentication challenge that includes a realm and nonce. The client resends the TURN request supplying a user name and password based on the realm indicated by the server. For a STUN binding request sent to a STUN server, no authentication is recommended, as generating the response is less work for a server than the server utilizing the short term or long term authentication approach. The server responds statelessly, so the only resources used are those to process each request, which are minimal.

WebRTC, Web Real-Time Communications, adds peer-to-peer real-time, interactive voice and video media capabilities and data channels to browsers [I-D.ietf-rtcweb-overview] without a plugin or download, and allows web developers to access this functionality using JavaScript API calls [WebRTC-API]. WebRTC includes STUN, TURN, and ICE client functionality built into browsers. For a session established between two browsers, if either browser is behind a NAT, a STUN server is necessary. Public STUN servers are currently available and a web application can suggest a particular STUN server be used. In cases where a particular combination of NAT mapping and filtering and/or firewalling is present, a TURN server is needed to establish a peer connection. In this case, TURN credentials need to be available to the browser for the long term authentication approach. A TURN server for WebRTC might serve a number of different domains and realms.

From the perspective of the web application provider, providing service for a number of different domains and realms, it is useful to know something about the source of the STUN request when processing the request. For a web application provider STUN or TURN server, the server will have no idea which web pages or sites are sending binding requests to the service. In conventional applications, the SOFTWARE attribute would provide some identifying information to the service, but that no longer works when the browser is the application. For a web application provider TURN server, the TURN server does not know which realm to include in an authentication challenge.

In the web world, HTTP requests have the concept of origin. The origin of a web page, as defined in [RFC6454], is defined by the URI's scheme, host or IP address, and port portions. The HTTP Origin header field inserted by the web browser carries this information and is useful information for servers that receive HTTP requests generated via JavaScript. For example, Cross Origin Resource Sharing, CORS, allows an HTTP server to serve HTTP requests from multiple origins.

This specification proposes extending the origin concept to STUN requests. STUN requests generated by a web browser would include the

origin of the HTTP page that is initiating the Peer Connection. Using this extra information, a STUN server could use the origin to determine which STUN binding requests to respond to, reducing the load on a STUN server. Using this information, a TURN server could use the origin to determine which realm to include in the authentication challenge. A TURN server can also use the origin information for logging and analytics, and also as additional information after authentication for providing service. This specification also defines an origin for SIP and XMPP users of STUN and TURN.

An important use case that the STUN Origin helps solve is the operation of a multi-tenanted TURN server (i.e. a TURN server that serves multiple, perhaps tens of thousands of different domains). The problem associated with this use case is described in paragraph 6 of Section 4 of [RFC7376]. While it is possible for a TURN server to use the same authentication credentials across many domains, a more likely (and more manageable) scenario is to have separate credentials for each domain, and hence a different realm for each domain. With the TURN server configured with a mapping between a domain (conveyed in the Origin) and the realm string (to be used in the authentication challenge), a single TURN URI could be used across all domains, and the resulting JavaScript code would be portable.

Note that the origin information is most useful as a hint in initial STUN and TURN requests as received by a server. However, origin information still has value throughout the session even after authentication for logging and other purposes.

The following sections of this document define the STUN ORIGIN attribute and define its usage.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. STUN ORIGIN attribute

This specification defines how to apply the web origin concept and syntax of [RFC6454] to the STUN protocol.

This specification defines a new Attribute to the STUN protocol [RFC5389]. The attribute is called ORIGIN and uses the syntax defined in Section 15 of [RFC5389]. The number used for this in the type field is 0x802F, chosen in the comprehension optional range.

The value of ORIGIN is a variable-length value. It MUST contain a UTF-8 [RFC3629] encoded sequence of characters. Senders MAY include multiple ORIGIN attributes in a request, and receivers MUST support parsing and receiving multiple ORIGIN attributes. HTTP origins are less than 267 characters (the maximum 253 character domain name plus 8 characters for the URI scheme plus 5 characters for the port number).

For a web browser (HTTP User Agent), the contents of the ORIGIN attribute is the unicode-serialization of an origin defined in Section 6.1 of [RFC6454]. The origin value included is the same as the Origin header field for an HTTP request generated from the web page that is creating the Peer Connection. It does not include any string terminating (\x00) character in the serialization.

For a SIP User Agent [RFC3261] using STUN and TURN, the ORIGIN attribute is set to be the URI of the registrar server used by the User Agent (i.e. the Request-URI of a REGISTER method). This is the full Request-URI component of the SIP ABNF defined in [RFC3261]. For example, a SIP user "sip:bob@biloxi.example.com" might register with the Request-URI of "sip:registrar.biloxi.example.com".

For an XMPP client [RFC6120] using STUN and TURN, the ORIGIN attribute is an XMPP URI [RFC5122] representing the full domainpart of the client's Jabber ID (JID) as defined in the ABNF of [RFC6122]; for example, if the client's JID is "juliet@im.example.com/balcony" then the ORIGIN attribute would be "xmpp:im.example.com".

Other contexts can define a usage of the ORIGIN attribute to use an appropriate URI or URL.

If an ORIGIN attribute is not present in a request, it is up to the server how to handle the request. For example, it could assume a default Origin.

2.1. Origin Matching Rules

For any usage of ORIGIN, the following rules MUST be followed to ensure privacy. An ORIGIN attribute MUST NOT be included in a STUN or TURN request if the fully qualified domain name (FQDN) of the Origin does not match the FQDN of the STUN or TURN URI which was used to reach the STUN or TURN server. That is, only if the domain of the Origin is the same as the origin of the STUN or TURN server is the Origin information sent. The FQDN comparison does not include ports or URI schemes. For example, a web origin from `http://foo.example.com:8080` would match a TURN URI of `turn:foo.example.com`. A SIP origin of `sips:bar.example.org:5061` would match a STUN URI of `stun:bar.example.org:999`.

2.2. STUN Usage

For STUN requests sent without authentication to a STUN server (i.e. STUN binding requests sent to a STUN server), the STUN client **MUST** include the ORIGIN attribute if it matches per the rules of Section 2.1. Otherwise, the ORIGIN attribute is omitted.

A STUN server can derive additional information for logging and analytics about the request through the ORIGIN attribute, such as the source of the request. For example, an enterprise STUN server might only reply to STUN binding requests from certain domains.

2.3. TURN Usage

TURN [RFC5766] Allocate requests **MUST** include ORIGIN if it matches per the rules of Section 2.1. Otherwise, the ORIGIN attribute is omitted. For all other TURN requests, including the Send method, the use of the ORIGIN attribute is **NOT RECOMMENDED** as it provides no value.

A TURN server can use the ORIGIN attribute to determine which REALM to include in the authentication challenge. A TURN server can also use the ORIGIN attribute after authentication to provide appropriate service.

2.4. NAT Behavior Discovery Usage

For the NAT Behavior Discovery Usage in [RFC5780], the rules for STUN usage apply.

2.5. ICE Usage

ICE [RFC5245] connectivity checks **MUST NOT** include the ORIGIN attribute. Including the ORIGIN attribute leaks information about the site used by one peer to the other peer in the session.

2.6. Media Keep-Alive Usage

For media keep-alive STUN requests described in Section 20 of [RFC5245], the rules for ICE usage apply.

2.7. SIP Keep-Alive Usage

For SIP keep-alive STUN requests described in [RFC5626], the ORIGIN attribute **MUST NOT** be included. No valid use cases for the ORIGIN attribute have been identified to date, and as a result the ORIGIN attribute will be ignored.

2.8. Multiple Origins

Multiple Origins for HTTP Requests are described in Section 7.2 of [RFC6454]. Multiple origins can occur when the same resource is fetched by multiple origins at the same time (e.g. multiple tabs, windows, frames, etc.). In the context of WebRTC, it doesn't make sense for a STUN binding or TURN allocation to be shared across origins (e.g. Peer Connections). Based on their definitions, multiple SIP and XMPP origins also do not apply here. Therefore, if a STUN request contains multiple origins, the first origin **MUST** be used and the remaining origins ignored.

3. IANA Considerations

This specification, if approved, adds a new value to the IANA "STUN Attributes Registry" created by [RFC5389]. The ORIGIN attribute value is 0x802F.

4. Security Considerations

The security considerations of [RFC6454] apply to this extension. Servers using the information present in the STUN ORIGIN attribute need to realize that this attribute could be set arbitrarily by a non-browser client or modified by an intermediary. The method proposed in this document is not meant to replace existing STUN authentication mechanisms but to provide additional information to the server for logging and analytics and how to handle the request after authentication.

Just as browsers do not allow a web application to set the HTTP Origin header field via JavaScript, web browsers (HTTP User Agents) **MUST NOT** allow a web application to set the STUN ORIGIN attribute through JavaScript.

While the STUN MESSAGE-INTEGRITY attribute can provide integrity protection for all attributes present in a STUN request, MESSAGE-INTEGRITY is not present in the initial STUN message sent. As a result, an ORIGIN attribute could be modified or removed from a STUN request without the server knowing. DTLS or TLS transport **SHOULD** be used when integrity protection for the ORIGIN attribute is important.

The STUN ORIGIN attribute has privacy implications. As a result, TLS or DTLS transport **SHOULD** be used. If STUN requests containing the origin attribute are not encrypted with TLS or DTLS, an on-path attacker could determine this information by inspecting STUN messages between the STUN client and STUN server. This information is often available in other messages sent by the browser, such as DNS or HTTP requests. However, in cases where secure HTTP is used, including the

ORIGIN attribute over an unencrypted transport could leak this information. In cases where privacy is paramount, but TLS or DTLS transport is not available, the ORIGIN attribute MAY be omitted.

The STUN ORIGIN attribute also has privacy implications in that the origin information is shared with a STUN or TURN server which otherwise might not know this information. This information could be used to track usage of real-time communication services. A STUN or TURN server will always know the public IP address of each user, but the ORIGIN attribute provides more information about which service or provider is being used. The particular STUN and TURN servers used are usually selected by the real-time communications service provider (i.e. the web provider for WebRTC or the SIP or XMPP service provider). In addition, they are usually also run by the same provider, or by a trusted partner, especially for TURN. However, a service or provider using an untrusted third party STUN or TURN server needs to recognize that the operator of the third party STUN or TURN server will learn the identity of the service or provider through this extension. In order to prevent the leakage of usage of information, the Origin and STUN or TURN URI matching rules defined in Section 2.1 MUST be used. These rules ensure that the inclusion of the ORIGIN attribute does not provide any new information to the operator of the STUN or TURN server than they already know.

5. Implementation Status

Note to RFC Editor: Please remove this entire section prior to publication, including the reference to RFC 6982.

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".

Two proof-of-concept implementations have been created in support of this proposed standard. One provides a WebRTC enabled browser that includes the appropriate STUN ORIGIN Attribute with the Origin insight known to the browser in STUN/TURN messages sent to servers. The other provides an example of a multiple realms capable TURN server that takes advantage of Origin insight provided in the STUN ORIGIN Attribute.

A Chrome browser implementation has been created by Graham Yoakum and Ryan Yoakum (Skobalt LLC) and is freely licensed under the standard terms of the open source Chromium and WebRTC projects. This proof-of-concept version of the Google Chrome browser (nicknamed 'Chromeo') sends Origin insight in STUN and TURN messages using the proposed new STUN ORIGIN attribute with a value of 0x802F (as initially proposed, however that value is easily changed in a single line of code). 'Chromeo' includes a Chrome flag to enable and disable this unique feature (and is by default disabled to prevent any non-intentional use of this feature until the standard is finalized). This implementation is based on is draft-johnston-tram-stun-origin-02.

Coordinated changes to both the WebRTC and Chromium open source projects have been formally submitted for consideration. The two submitted change lists together implement the complete browser proof-of-concept. 'Chromeo' has been built for Linux and STUN protocol behavior has been verified using WireShark traces illustrating that proper STUN Origin attributes are being included in STUN/TURN messages sent by the browser to servers (screen captures of STUN messages illustrating the Origin attribute and content are available).

The WebRTC and Chromium open source projects can be found at:
<http://www.webrtc.org/> and <http://www.chromium.org/>

Google can choose to accept or modify the changes proposed for Chrome and other browser vendors can access and take advantage of the publicly available WebRTC and Chromium open source submissions as desired. Hopefully this will enable browsers to quickly implement STUN Origin enhancements.

A multiple realms capable advanced open source Origin enabled TURN server (named 'Coturn') has been created by Oleg Moskalenko and is freely licensed under the New BSD license. This reference implementation and proof-of-concept provides a clone (a spin-off) of the rfc5766-turn-server project adding Origin-based multiple realms support.

'Coturn' is backward-compatible with rfc5766-turn-server project but the code is more complex and it uses a different (also more complex)

database structure. It is the intent to add all IETF TRAM TURN server related capabilities to this project as they mature. 'Coturn' is publicly available and can be found at: <https://github.com/coturn/coturn/>

6. Acknowledgements

Thanks to John Selbie, Tirumaleswar Reddy, Simon Perreault, Marc Petit-Huguenin, Andy Hutton, and Oleg Moskalkenko for their feedback and reviews. Special thanks to Graham Yoakum and Ryan Yoakum of Skobalt LLC and Oleg Moskalkenko of rfc5766-turn-server project for contributing open source proof-of-concept implementations for a Chrome web browser and a multiple realms capable TURN server, quickly demonstrating feasibility.

7. References

7.1. Normative References

- [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>>.
- [RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <<http://www.rfc-editor.org/info/rfc3261>>.
- [RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <<http://www.rfc-editor.org/info/rfc3629>>.
- [RFC5122] Saint-Andre, P., "Internationalized Resource Identifiers (IRIs) and Uniform Resource Identifiers (URIs) for the Extensible Messaging and Presence Protocol (XMPP)", RFC 5122, DOI 10.17487/RFC5122, February 2008, <<http://www.rfc-editor.org/info/rfc5122>>.
- [RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, DOI 10.17487/RFC5245, April 2010, <<http://www.rfc-editor.org/info/rfc5245>>.

- [RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, DOI 10.17487/RFC5389, October 2008, <<http://www.rfc-editor.org/info/rfc5389>>.
- [RFC5626] Jennings, C., Ed., Mahy, R., Ed., and F. Audet, Ed., "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)", RFC 5626, DOI 10.17487/RFC5626, October 2009, <<http://www.rfc-editor.org/info/rfc5626>>.
- [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, DOI 10.17487/RFC5766, April 2010, <<http://www.rfc-editor.org/info/rfc5766>>.
- [RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, DOI 10.17487/RFC6120, March 2011, <<http://www.rfc-editor.org/info/rfc6120>>.
- [RFC6122] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Address Format", RFC 6122, DOI 10.17487/RFC6122, March 2011, <<http://www.rfc-editor.org/info/rfc6122>>.
- [RFC6454] Barth, A., "The Web Origin Concept", RFC 6454, DOI 10.17487/RFC6454, December 2011, <<http://www.rfc-editor.org/info/rfc6454>>.
- [RFC7350] Petit-Huguenin, M. and G. Salgueiro, "Datagram Transport Layer Security (DTLS) as Transport for Session Traversal Utilities for NAT (STUN)", RFC 7350, DOI 10.17487/RFC7350, August 2014, <<http://www.rfc-editor.org/info/rfc7350>>.

7.2. Informative References

- [I-D.ietf-rtcweb-overview] Alvestrand, H., "Overview: Real Time Protocols for Browser-based Applications", draft-ietf-rtcweb-overview-14 (work in progress), June 2015.
- [RFC5780] MacDonald, D. and B. Lowekamp, "NAT Behavior Discovery Using Session Traversal Utilities for NAT (STUN)", RFC 5780, DOI 10.17487/RFC5780, May 2010, <<http://www.rfc-editor.org/info/rfc5780>>.

- [RFC6982] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", RFC 6982, DOI 10.17487/RFC6982, July 2013, <<http://www.rfc-editor.org/info/rfc6982>>.
- [RFC7376] Reddy, T., Ravindranath, R., Perumal, M., and A. Yegin, "Problems with Session Traversal Utilities for NAT (STUN) Long-Term Authentication for Traversal Using Relays around NAT (TURN)", RFC 7376, DOI 10.17487/RFC7376, September 2014, <<http://www.rfc-editor.org/info/rfc7376>>.
- [WebRTC-API] Bergkvist, A., Burnett, D., Jennings, C., and A. Narayanan, "WebRTC 1.0: Real-time Communication Between Browsers", W3C Working Draft <http://www.w3.org/TR/webrtc/>, 2013, <<http://www.w3.org/TR/2013/WD-webrtc-20130910/>>.

Authors' Addresses

Alan Johnston
Avaya
St. Louis, MO
USA

Email: alan.b.johnston@gmail.com

Justin Uberti
Google
Kirkland, WA
USA

Email: justin@uberti.name

John Yoakum
Avaya
Cary, NC
USA

Email: yoakum@avaya.com

Kundan Singh
Avaya
San Francisco, CA
USA

Email: kundan10@gmail.com