

TRAM
Internet-Draft
Intended status: Standards Track
Expires: August 8, 2015

T. Reddy
P. Patil
Cisco
February 4, 2015

IP address privacy by TURN server
draft-reddy-tram-turn-ipaddress-privacy-00

Abstract

A TURN server allocates an IP address for a user. If this address is dis-associated from the user's actual network, the allocated IP address increases the user's privacy. This document describes a means for an client to discover that the TURN server can provide IP address privacy.

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 August 8, 2015.

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.

Internet-Draft IP address privacy by TURN server February 2015

Table of Contents

1.	Introduction	2
2.	Notational Conventions	3
3.	IP address privacy determination procedure	3
3.1.	The ADDRESS-PRIVACY attribute in request	4
3.2.	The ADDRESS-PRIVACY attribute in response	4
4.	IANA Considerations	4
5.	Security Considerations	5
6.	Acknowledgements	5
7.	References	5
7.1.	Normative References	5
7.2.	Informative References	5
	Authors' Addresses	6

[1.](#) Introduction

Disclosing a host's IP address and connected network's IP address can disclose the user's location or network connection point, which is a privacy concern. These addresses are disclosed during normal operation of WebRTC [[I-D.ietf-rtcweb-overview](#)]. To prevent this disclosure, the local address (called "host address" by ICE [[RFC5245](#)]) and the connected network's IP address (called "server reflexive" by ICE) cannot be disclosed to the remote peer. Instead, only the address allocated by a TURN (Traversal Using Relays around NAT) [[RFC5766](#)] server is disclosed to the remote peer. However, if the TURN server is dedicated to a specific network (e.g., it is deployed by a network operator for the sole use of users on that network), that TURN server will similarly leak information about the user's connected network.

Using any of the discovery mechanisms described in [[I-D.ietf-tram-turn-server-discovery](#)], a client may discover multiple Traversal Using Relays around NAT (TURN) servers. The TURN servers discovered could be provided by an enterprise network, an access network, an application service provider or a third party provider. Therefore, the client needs to be able to choose a TURN server that can provide IP address privacy.

The ADDRESS-PRIVACY attribute introduced in this specification can be used by the client to determine if the TURN server can provide IP address privacy from the remote peer.

This technique also solves the following other problems:

- o User may or may not trust the calling service or WebRTC application. [[I-D.ietf-rtcweb-security-arch](#)] discusses users using privacy techniques like Tor so that malicious calling

service does not learn the user's IP address. The Poker example given in section 4 of [[I-D.ietf-rtcweb-security-arch](#)] discusses that the users in the call do not trust the calling service. In this scenario if the user wants IP address privacy then the TURN server provided by the calling service must be avoided and the client must only select a TURN server whose authenticity can be ascertained and can offer IP address privacy.

- o Enterprise Firewall policy typically has a white-list of permitted outside applications/sites and can blacklist HTTP(S) connections via various forms of detections (DNS lookup, ALPN, HTTP URL Filtering, DPI proxy that at least performs HTTPS inspection of SNI in TLS exchange and validates SSL records, HTTP(S) proxy etc.). Firewall in this configuration would block TCP/UDP connection to external peers in the Internet and arbitrary TURN servers. For example firewall would block usage of STUN with external peers and force the clients to use enterprise provided TURN server for all external WebRTC media communications. Enterprise network could leverage firewall and TURN services provided by a third party provider. If the third party offered TURN server can provide IP address privacy then the application can avoid TURN-in-TURN mechanism discussed in [[I-D.schwartz-rtcweb-return](#)] and thus avoid the overhead of using RETURN proxying.

[2.](#) Notational Conventions

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](#)].

This note uses terminology defined in STUN [[RFC5389](#)].

[3.](#) IP address privacy determination procedure

If a client wants IP address privacy, it includes the ADDRESS-PRIVACY

attribute in its TURN Allocate request. If the server can provide IP address privacy then it would echo back ADDRESS-PRIVACY attribute in the Allocate response.

This specification defines a new comprehension-optional STUN attribute ADDRESS-PRIVACY will have a STUN Type TBD-CA. This type is in the comprehension-optional range, which means that TURN servers can safely ignore the attribute if they do not understand it.

[3.1.](#) The ADDRESS-PRIVACY attribute in request

This attribute is used by the client to ask the server if it can provide IP address privacy. This attribute has no value part and thus the attribute length field is 0.

[3.2.](#) The ADDRESS-PRIVACY attribute in response

When a server receives a STUN request that includes a ADDRESS-PRIVACY attribute, it processes the request as per the STUN specification [[RFC5389](#)] plus the specific rules mentioned here. The server checks the following:

- o If the ADDRESS-PRIVACY attribute is not recognized, ignore the attribute because its type indicates that it is comprehension-optional. This should be the existing behavior as explained in [section 3.1 of \[RFC5389\]](#).
- o If the server can provide IP address privacy then it will include ADDRESS-PRIVACY attribute in the response.
- o If the server determines that the relayed address it will allocate and client IP address are in the same geolocation then the server will redirect the client to another server that can provide IP address privacy by replying to the request message with an error response with error code 300 (Try Alternate). (TBD: Is there a need for privacy levels ? (same country different town, same continent different country, different continent etc)).

- o If the server cannot provide IP address privacy or does not want to provide IP address privacy then it will ignore this attribute.

[4.](#) IANA Considerations

[Paragraphs in braces should be removed by the RFC Editor upon publication]

[The ADDRESS-PRIVACY attribute requires that IANA allocate a value in the "STUN attributes Registry" from the comprehension-optional range (0x8000-0xBFFF), to be replaced for TBD-CA throughout this document]

This document defines the ADDRESS-PRIVACY STUN attribute, described in [Section 3](#). IANA has allocated the comprehension-optional codepoint TBD-CA for this attribute.

[5.](#) Security Considerations

It is possible the TURN server provides inadequate IP address privacy to meet the client's needs. For example, the TURN server might be located in the same city as the client, but the client wants to obfuscate its location to the same continent or to a different continent or a different planet. The client should find its geolocation using server-reflexive candidate. The client should also determine the geolocation of the relayed address learned from the TURN server and compare with its geolocation to determine if the TURN server is indeed providing IP address privacy.

Security considerations discussed in [\[RFC5766\]](#) are to be taken into account.

[6.](#) Acknowledgements

Thanks to Dan Wing and Pal Martinsen for the review and comments.

[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.
- [RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", [RFC 5245](#), April 2010.
- [RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", [RFC 5389](#), October 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.

[7.2](#). Informative References

- [I-D.ietf-rtcweb-overview]
Alvestrand, H., "Overview: Real Time Protocols for Browser-based Applications", [draft-ietf-rtcweb-overview-13](#) (work in progress), November 2014.

- [I-D.ietf-rtcweb-security-arch]
Rescorla, E., "WebRTC Security Architecture", [draft-ietf-rtcweb-security-arch-10](#) (work in progress), July 2014.
- [I-D.ietf-tram-turn-server-discovery]
Patil, P., Reddy, T., and D. Wing, "TURN Server Auto Discovery", [draft-ietf-tram-turn-server-discovery-01](#) (work in progress), January 2015.
- [I-D.schwartz-rtcweb-return]
Schwartz, B. and J. Uberti, "Recursively Encapsulated TURN (RETURN) for Connectivity and Privacy in WebRTC", [draft-schwartz-rtcweb-return-04](#) (work in progress), November 2014.

Authors' Addresses

Tirumaleswar Reddy
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: tiredy@cisco.com

Prashanth Patil
Cisco Systems, Inc.
Bangalore
India

Email: praspati@cisco.com