BEHAVE
Internet-Draft
Intended status: Standards Track
Expires: March 07, 2014

T. Reddy
Ram. Ravindranath
Muthu. Perumal
Cisco
A. Yegin
Samsung

September 03, 2013

Problems with STUN Authentication for TURN
draft-reddy-behave-turn-auth-03

Abstract

This document discusses some of the issues with STUN authentication for TURN messages.

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 07, 2014.

Copyright Notice

Table of Contents

1. Introduction

TURN server plays a vital and is a building block to support direct, interactive, real-time communication using audio, video, collaboration, games, etc., between two peers web-browsers in Web Real-Time communication (WebRTC) [I-D.ietf-rtcweb-overview] framework. The use-case explained in Section 4.2.4.1 of [I-D.ietf-rtcweb-use-cases-and-requirements] refers to deploying a TURN[RFC5766] server to audit all media sessions from inside an Enterprise premises to any external peer. TURN server could also be deployed for recording, RTP Mobility [I-D.wing-mmusic-ice-mobility] etc.

TURN server is also used in the following scenarios :

- Users of RTCWEB based web application may choose to use TURN so as to not expose the host candidate addresses to the remote peer for privacy.

- Enterprise networks deploy firewalls typically configured to block UDP traffic. When SIP user agents or WebRTC endpoints are deployed behind such firewalls, media cannot be sent over UDP across the firewall, but must be sent using TCP (which causes a different user experience). In such cases a TURN server deployed in the DMZ MAY be used to traverse Firewalls.

- IPv6 support in TURN includes IPv4-to-IPv6, IPv6-to-IPv6, and IPv6 -to-IPv4 relaying[RFC6156].

- ICE connectivity checks using server-reflexive candidates could fail because endpoint is behind NAT that performs Address-dependent mapping and relayed candidate allocated from the TURN server gets selected for media.

STUN [RFC5389] specifies an authentication mechanism called the long-term credential mechanism. TURN servers and clients are required to implement this mechanism. The server requires that all requests from the client be authenticated using this mechanism, or that a equally strong or stronger mechanism for client authentication be used.

In the above scenarios RTCWEB based web applications would use Interactive Connectivity Establishment (ICE) protocol [RFC5245] for gathering candidates. ICE agent can use TURN to learn server-reflexive and relayed candidates. If the TURN server requires the TURN request to be authenticated then ICE agent will use the long-term credential mechanism explained in section 10 of [RFC5389] for authentication and message integrity. TURN specification [RFC5766] in section 10 explains the importance of long-term credential mechanism to mitigate various attacks. With proposals like[I-D.thomson-mmusic-rtcweb-bw-consent] that defines a STUN BANDWIDTH attribute for requesting bandwidth allocation at a TURN server, STUN authentication becomes further important to prevent un-authorized users from accessing the TURN server.

This note focuses on listing the problems with current STUN authentication for TURN so that it can serve as the basis for stronger authentication mechanisms.

Compared to a Binding request the Allocate request is more likely to be identified by a server administrator as needing client authentication and integrity protection of messages exchanged. Hence, the issues discussed here in STUN authentication are applicable mainly in the context of TURN messages.

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 [RFC5389], [RFC5766].

3. Scope

This document can be used as a tool to design solution(s) to address the problems with the current STUN authentication for TURN messages.

4. Problems with usage of STUN Authentication

1. The long-term credential mechanism in [RFC5389] could use traditional "log-in" username and password given to users which does not change for extended periods of time and uses the key derived from user credentials to generate message integrity for every TURN request/response. An attacker that is capable of eavesdropping on a message exchange between a client and server can determine the password by trying a number of candidate passwords and checking if one of them is correct by calculating the message-integrity of the message using these candidate passwords and comparing with the message integrity value in the MESSAGE-INTEGRITY attribute. The long-term credential mechanism in [RFC5389] is also susceptible to offline dictionary attacks. This attack can be mitigated by using strong passwords with large entropy.

2. When TURN server is deployed in DMZ and requires requests to be authenticated using the long-term credential mechanism in [RFC5389], TURN server needs to be aware of the username and password to validate the message integrity of the requests and to provide message integrity for responses. Thus requiring management overhead to maintain credential database on the TURN server.

3. The long-term credential mechanism in [RFC5389] requires that the TURN client must include username value in the USERNAME STUN attribute. An adversary snooping the TURN messages between the TURN client and server can identify the users involved in the call resulting in privacy leakage. In certain scenarios TURN usernames need not be linked to any real usernames given to users as they are just provisioned on a per company basis.

4. An Attacker posing as a TURN server challenges the client to authenticate, learns the USERNAME of the host and later snoops the traffic from the host identifying the user activity resulting in privacy leakage.

5. Hosting multiple realms on a single IP address is challenging with TURN. When a TURN server needs to send the REALM attribute in response to an unauthenticated request, it has no useful information for determining which realm it should send, except the source transport address of the TURN request. Note this is a problem with multi-tenant scenarios only. This is not a problem when deployed in Enterprise.

6. In WebRTC the Javascript needs be know the username and password to use in W3C RTCPeerConnection API to access the TURN server.

This exposes the user credentials to the Javascript which could be malicious.

5. Security Considerations

This document does not define an architecture nor a protocol; as such it does not raise any security concern.

6. IANA Considerations

This document does not require any action from IANA.

7. Acknowledgments

Authors would like to thank Dan Wing, Sandeep Rao, Prashanth Patil, Pal Martinsen and Simon Perreault for their comments and review.

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.

[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.

[RFC6156] Camarillo, G., Novo, O., and S. Perreault, "Traversal Using Relays around NAT (TURN) Extension for IPv6", RFC 6156, April 2011.

8.2. Informative References

[I-D.ietf-rtcweb-overview]
Alvestrand, H., "Overview: Real Time Protocols for Brower-based Applications", draft-ietf-rtcweb-overview-07 (work in progress), August 2013.

[I-D.ietf-rtcweb-use-cases-and-requirements]
Holmberg, C., Hakansson, S., and G. Eriksson, "Web Real-Time Communication Use-cases and Requirements", draft-ietf-rtcweb-use-cases-and-requirements-11 (work in progress), June 2013.

[I-D.thomson-mmusic-rtcweb-bw-consent]
Thomson, M. and B. Aboba, "Bandwidth Constraints for Session Traversal Utilities for NAT (STUN)", draft-thomson-mmusic-rtcweb-bw-consent-00 (work in progress), October 2012.

[I-D.wing-mmusic-ice-mobility]
Wing, D., Reddy, T., Patil, P., and P. Martinsen, "Mobility with ICE (MICE)", draft-wing-mmusic-ice-mobility-04 (work in progress), June 2013.

[RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, April 2010.

[RFC6544] Rosenberg, J., Keranen, A., Lowekamp, B., and A. Roach, "TCP Candidates with Interactive Connectivity Establishment (ICE)", RFC 6544, March 2012.

Authors' Addresses

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

Email: tireddy@cisco.com

Ram Mohan Ravindranath
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: rmohanr@cisco.com

Muthu Arul Mozhi Perumal
Cisco Systems, Inc.
Cessna Business Park
Sarjapur-Marathahalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: mperumal@cisco.com

Alper Yegin
Samsung
Istanbul
Turkey

Email: alper.yegin@yegin.org