TRAM
Internet-Draft
Intended status: Informational
Expires: February 19, 2015

T. Reddy
R. Ravindranath
Cisco
M. Perumal
Ericsson
A. Yegin
Samsung

August 18, 2014

Problems with STUN long-term Authentication for TURN draft-ietf-tram-auth-problems-05

Abstract

This document discusses some of the security and practical problems with the current Session Traversal Utilities for NAT (STUN) authentication for Traversal Using Relays around NAT (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 February 19, 2015.

Copyright Notice

Copyright (c) 2014 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

Traversal Using Relays around NAT (TURN) [RFC5766] is a protocol that is often used to improve the connectivity of Peer-to-Peer (P2P) applications (as defined in section 2.7 of [RFC5128]). TURN allows a connection to be established when one or both sides is incapable of a direct P2P connection. The TURN server is also a building block to support interactive, real-time communication using audio, video, collaboration, games, etc., between two peer web browsers using the Web Real-Time communication (WebRTC) [I-D.ietf-rtcweb-overview] framework.

TURN server is also used in the following scenarios:

- Users of WebRTC based web application may use TURN server to hide host candidate addresses from the remote peer for privacy.

- Enterprise networks deploy firewalls which typically 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 DeMilitarized Zone (DMZ) might be used to traverse firewalls.

- The use-case explained in "Simple Video Communication Service, enterprise aspects" (Section 3.2.5 of [I-D.ietf-rtcweb-use-cases-and-requirements]) refers to deploying a TURN server in the DMZ to audit all media sessions from inside an Enterprise premises to any external peer.

- TURN server could also be deployed for RTP Mobility [I-D.wing-tram-turn-mobility] etc.

- TURN Server may be used for IPv4-to-IPv6, IPv6-to-IPv6, and IPv6 - to-IPv4 relaying [RFC6156].

- Interactive Connectivity Establishment (ICE) [RFC5245] connectivity checks using server reflexive candidates could fail when the endpoint is behind NAT [RFC3235] that performs Address-dependent mapping as described in section 4.1 of [RFC4787]. In such cases relayed candidate allocated from the TURN server is used for media.

STUN [RFC5389] specifies an authentication mechanism called the long-term credential mechanism. TURN [RFC5766] in section 4 specifies that TURN servers and clients must implement this mechanism and the TURN server must demand 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 applications would use ICE protocol 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, client authentication is essential to prevent un-authorized users from accessing the TURN server and misuse of credentials could impose significant cost on the victim TURN server.

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

An Allocate request is more likely than a Binding request 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

This note uses terminology defined in [RFC5389], [RFC5766].

3. Scope

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

4. Problems with STUN long-term Authentication for TURN

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.

2. When TURN server is deployed in the 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. This results in management overhead on the TURN server. Long-term credentials (username, realm, and password) need to be stored on the server-side using MD5 hash over the credentials, which is not considered best current practice. [RFC6151] discusses security vulnerabilities of MD5 and encourages not to use it. It is not possible to use STUN long-term credentials in US FIPS 140-2 [FIPS-140-2] compliant implementations, since MD5 isn't an approved algorithm.

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. If TURN usernames are linked to real usernames then it will result in privacy leakage, but 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. STUN authentication relies on HMAC-SHA1 [RFC2104]. There is no mechanism for hash agility in the protocol itself, although Section 16.3 of [RFC5389] does discuss a plan for migrating to a

more secure algorithm in case HMAC-SHA1 is found to be compromised.

5. A man-in-the middle attacker posing as a TURN server challenges the client to authenticate, learns the USERNAME of the client and later snoops the traffic from the client identifying the user activity resulting in privacy leakage.

6. 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 in the response, except the source transport address of the TURN request. Note this is a problem with multi-tenant scenarios only. This may not be a problem when TURN server is located in enterprise premises.

7. In WebRTC the Javascript code needs to 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. The malicious java script could misuse or leak the credentials. If the credentials happen to be used for accessing services other than TURN then the security implications are much larger.

5. Security Considerations

This document lists problems with current STUN authentication for TURN so that it can serve as the basis for stronger authentication mechanisms.

6. IANA Considerations

This document does not require any action from IANA.

7. Acknowledgments

Authors would like to thank Dan Wing, Harald Alvestrand, Sandeep Rao, Prashanth Patil, Pal Martinsen, Marc Petit-Huguenin, Gonzalo Camarillo, Brian E Carpenter, Spencer Dawkins, Adrian Farrel and Simon Perreault for their comments and review.

8. References

8.1. Normative References

[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

[FIPS-140-2] NIST, , "NIST, "Security Requirements for Cryptographic Modules"", June 2005, <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

[I-D.ietf-rtcweb-overview] Alvestrand, H., "Overview: Real Time Protocols for Browser-based Applications", draft-ietf-rtcweb-overview-10 (work in progress), June 2014.

[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-14 (work in progress), February 2014.

[I-D.wing-tram-turn-mobility] Wing, D., Patil, P., Reddy, T., and P. Martinsen, "Mobility with TURN", draft-wing-tram-turn-mobility-00 (work in progress), June 2014.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[RFC3235] Senie, D., "Network Address Translator (NAT)-Friendly Application Design Guidelines", RFC 3235, January 2002.

[RFC4787] Audet, F. and C. Jennings, "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP", BCP 127, RFC 4787, January 2007.

[RFC5128] Srisuresh, P., Ford, B., and D. Kegel, "State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs)", RFC 5128, March 2008.

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

[RFC6151] Turner, S. and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, March 2011.

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
Ericsson
Ferns Icon
Doddanekundi, Mahadevapura
Bangalore, Karnataka 560037
India

Email: muthu.arul@gmail.com

Alper Yegin
Samsung
Istanbul
Turkey

Email: alper.yegin@yegin.org