

Behavior Engineering for Hindrance	R. Denis-Courmont	
Avoidance	Nokia	
Internet-Draft	September 21, 2007	
Intended status: Informational		
Expires: March 24, 2008		

[TOC](#)

Test vectors for RFC3489bis draft-denis-behave-rfc3489bis-test-vectors-02

Status of This Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on March 24, 2008.

Abstract

This document includes test vectors for the MESSAGE-INTEGRITY and FINGERPRINT attributes of the STUN protocol.

Table of Contents

- [1.](#) Introduction
- [2.](#) Test vectors
 - [2.1.](#) Sample request
 - [2.2.](#) Sample IPv4 response
 - [2.3.](#) Sample IPv6 response

- [3. Security Considerations](#)
- [4. IANA Considerations](#)
- [5. Acknowledgements](#)
- [6. Normative References](#)
- [Appendix A. Source code for test vectors](#)

1. Introduction

[TOC](#)

The Session Traversal Utilities for NAT (STUN) [\[I-D.ietf-behave-rfc3489bis\]](#) (Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for (NAT) (STUN)," July 2008.) protocol defines two different hashes that may be included in messages exchanged by peers implementing that protocol:

FINGERPRINT attribute: a 32-bits Circular Redundancy Check.

MESSAGE-INTEGRITY attribute: a HMAC-SHA1 authentication code.

This document documents sample properly-formatted STUN messages including these hashes, for the sake of testing implementations of the STUN protocol.

2. Test vectors

[TOC](#)

All included vectors are represented as a series of hexadecimal values in network byte order. Each pair of hexadecimal digits represents one byte.

Messages follow the ICE Connectivity Checks use case of STUN, (see [\[I-D.ietf-mmusic-ice\]](#) (Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols," October 2007.)). They include both FINGERPRINT and MESSAGE-INTEGRITY attributes.

2.1. Sample request

[TOC](#)

This request uses the following parameters:

Username: "evtj:h6vY" (without quotes)

Password: "V0kJxbRl1RmTxUk/WvJxBt" (without quotes)

00 01 00 44	Request type and message length
21 12 a4 42	Message cookie
b7 e7 a7 01 }	
bc 34 d6 86 }	Transaction ID
fa 87 df ae }	
00 24 00 04	
6e 00 01 ff	
80 29 00 08	
93 2f f9 b1	
51 26 3b 36	
00 06 00 09	USERNAME attribute header
65 76 74 6a }	
3a 68 36 76 }	Username (9 bytes) and padding (3 bytes)
59 20 20 20 }	
00 08 00 14	MESSAGE-INTEGRITY attribute header
62 4e eb dc }	
3c c9 2d d8 }	
4b 74 bf 85 }	HMAC-SHA1 fingerprint
d1 c0 f5 de }	
36 87 bd 33 }	
80 28 00 04	FINGERPRINT attribute header
ad 8a 85 ff	CRC32 fingerprint

2.2. Sample IPv4 response

[TOC](#)

This response used the following parameter:

Password: "V0kJxbRl1RmTxUk/WvJxBt" (without quotes)

Mapped address: 192.0.2.1 port 32853

01 01 00 3c	Response type and message length
21 12 a4 42	Message cookie
b7 e7 a7 01 }	
bc 34 d6 86 }	Transaction ID
fa 87 df ae }	
80 22 00 0b	
74 65 73 74	
20 76 65 63	
74 6f 72 20	
00 20 00 08	
00 01 a1 47	
e1 12 a6 43	
00 08 00 14	MESSAGE-INTEGRITY attribute header
2b 91 f5 99 }	
fd 9e 90 c3 }	
8c 74 89 f9 }	HMAC-SHA1 fingerprint
2a f9 ba 53 }	
f0 6b e7 d7 }	
80 28 00 04	FINGERPRINT attribute header
c0 7d 4c 96	CRC32 fingerprint

2.3. Sample IPv6 response

[TOC](#)

This response used the following parameter:

Password: "V0kJxbRl1RmTxUk/WvJxBt" (without quotes)

Mapped address: 2001:db8:1234:5678:11:2233:4455:6677 port 32853

01 01 00 48	Response type and message length
21 12 a4 42	Message cookie
b7 e7 a7 01 }	
bc 34 d6 86 }	Transaction ID
fa 87 df ae }	
80 22 00 0b	
74 65 73 74	
20 76 65 63	
74 6f 72 20	
00 20 00 14	
00 02 a1 47	
01 13 a9 fa	
a5 d3 f1 79	
bc 25 f4 b5	
be d2 b9 d9	
00 08 00 14	MESSAGE-INTEGRITY attribute header
a3 82 95 4e }	
4b e6 7b f1 }	
17 84 c9 7c }	HMAC-SHA1 fingerprint
82 92 c2 75 }	
bf e3 ed 41 }	
80 28 00 04	FINGERPRINT attribute header
c8 fb 0b 4c	CRC32 fingerprint

3. Security Considerations

[TOC](#)

There are no security considerations.

4. IANA Considerations

[TOC](#)

This document raises no IANA considerations.

5. Acknowledgements

[TOC](#)

The author would like to thank Marc Petit-Huguenin for his comments, and Brian Korver, Alfred E. Heggstad and Gustavo García for their review.

6. Normative References

[TOC](#)

[I-D.ietf-behave-rfc3489bis]	Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, " Session Traversal Utilities for (NAT) (STUN) ," draft-ietf-behave-rfc3489bis-18 (work in progress), July 2008 (TXT).
[I-D.ietf-mmusic-ice]	Rosenberg, J., " Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols ," draft-ietf-mmusic-ice-19 (work in progress), October 2007 (TXT).

Appendix A. Source code for test vectors

[TOC](#)

```
const unsigned char req[] =
    "\x00\x01\x00\x44"
    "\x21\x12\xa4\x42"
    "\xb7\xe7\xa7\x01\xbc\x34\xd6\x86\xfa\x87\xdf\xae"
    "\x00\x24\x00\x04"
    "\x6e\x00\x01\xff"
    "\x80\x29\x00\x08"
    "\x93\x2f\xf9\xb1\x51\x26\x3b\x36"
    "\x00\x06\x00\x09"
    "\x65\x76\x74\x6a\x3a\x68\x36\x76\x59\x20\x20\x20"
    "\x00\x08\x00\x14"
    "\x62\x4e\xeb\xdc\x3c\xc9\x2d\xd8\x4b\x74\xbf\x85"
    "\xd1\xc0\xf5\xde\x36\x87\xbd\x33"
    "\x80\x28\x00\x04"
    "\xad\x8a\x85\xff";
```

Request message

```
const unsigned char respv4[] =
    "\x01\x01\x00\x3c"
    "\x21\x12\xa4\x42"
    "\xb7\xe7\xa7\x01\xbc\x34\xd6\x86\xfa\x87\xdf\xae"
    "\x80\x22\x00\x0b"
    "\x74\x65\x73\x74\x20\x76\x65\x63\x74\x6f\x72\x20"
    "\x00\x20\x00\x08"
    "\x00\x01\xa1\x47\xe1\x12\xa6\x43"
    "\x00\x08\x00\x14"
    "\x2b\x91\xf5\x99\xfd\x9e\x90\xc3\x8c\x74\x89\xf9"
    "\x2a\xf9\xba\x53\xf0\x6b\xe7\xd7"
    "\x80\x28\x00\x04"
    "\xc0\x7d\x4c\x96";
```

IPv4 response message

```
const unsigned char respv6[] =
    "\x01\x01\x00\x48"
    "\x21\x12\xa4\x42"
    "\xb7\xe7\xa7\x01\xbc\x34\xd6\x86\xfa\x87\xdf\xae"
    "\x80\x22\x00\x0b"
    "\x74\x65\x73\x74\x20\x76\x65\x63\x74\x6f\x72\x20"
    "\x00\x20\x00\x14"
    "\x00\x02\xa1\x47"
    "\x01\x13\xa9\xfa\xa5\xd3\xf1\x79"
    "\xbc\x25\xf4\xb5\xbe\xd2\xb9\xd9"
    "\x00\x08\x00\x14"
    "\xa3\x82\x95\x4e\x4b\xe6\x7b\xf1\x17\x84\xc9\x7c"
    "\x82\x92\xc2\x75\xbf\xe3\xed\x41"
    "\x80\x28\x00\x04"
    "\xc8\xfb\x0b\x4c";
```

IPv6 response message

Author's Address

[TOC](#)

	Rémi Denis-Courmont
	Nokia Corporation

	P.O. Box 407
	NOKIA GROUP 00045
	FI
Phone:	+358 50 487 6315
EMail:	remi.denis-courmont@nokia.com

Full Copyright Statement

[TOC](#)

Copyright © The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.