

Behavior Engineering for Hindrance	R. Denis-Courmont	
Avoidance	Nokia	
Internet-Draft	November 18, 2008	
Intended status: Informational		
Expires: May 22, 2009		

[TOC](#)

Test vectors for STUN

draft-ietf-behave-stun-test-vectors-04

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/lid-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 May 22, 2009.

Abstract

The Session Traversal Utilities for NAT (STUN) protocol defines several STUN attributes. The content of some of these -- FINGERPRINT, MESSAGE-INTEGRITY and XOR-MAPPED-ADDRESS -- involve binary-logical operations (hashing, xor). This document provides test vectors for those attributes.

Table of Contents

- [1.](#) Introduction
- [2.](#) Test vectors
 - [2.1.](#) Sample request

- [2.2.](#) Sample IPv4 response
- [2.3.](#) Sample IPv6 response
- [2.4.](#) Sample request with long-term authentication
- [3.](#) Security Considerations
- [4.](#) IANA Considerations
- [5.](#) Acknowledgements
- [6.](#) References
 - [6.1.](#) Normative References
 - [6.2.](#) Informative References
- [Appendix A.](#) Source code for test vectors

1. Introduction

[TOC](#)

The Session Traversal Utilities for NAT (STUN)[\[RFC5389\]](#) ([Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT \(STUN\)," October 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[\[RFC2104\]](#) ([Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," February 1997.](#)) authentication code.

This document provides samples of 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.](#))). These messages include FINGERPRINT, MESSAGE-INTEGRITY and XOR-MAPPED-ADDRESS STUN attributes. These attributes are considered to be most prone to implementation errors. An additional message is provided to test STUN authentication with long-term credentials (which is not used by ICE).

In the following sample messages, two types of plain UTF-8 text attributes are included. The values of certain of these attributes were purposely sized to require padding. Non-ASCII characters are represented as <U+xxxx> where xxxx is the hexadecimal number of their Unicode code point.

In this document, ASCII white spaces (U+0020) are used for padding within the first three messages - this is arbitrary. Similarly, the last message uses nul bytes for padding. As per [\[RFC5389\] \(Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT \(STUN\)," October 2008.\)](#), padding bytes may take any value.

2.1. Sample request

[TOC](#)

This request uses the following parameters:

Software name: "STUN test client" (without quotes)

Username: "evtj:h6vY" (without quotes)

Password: "V0kJxbRl1RmTxUk/WvJxBt" (without quotes)

00 01 00 58	Request type and message length
21 12 a4 42	Magic cookie
b7 e7 a7 01 }	
bc 34 d6 86 }	Transaction ID
fa 87 df ae }	
80 22 00 10	SOFTWARE attribute header
53 54 55 4e }	
20 74 65 73 }	User-agent...
74 20 63 6c }	...name
69 65 6e 74 }	
00 24 00 04	PRIORITY attribute header
6e 00 01 ff	ICE priority value
80 29 00 08	ICE-CONTROLLED attribute header
93 2f f9 b1 }	Pseudo-random tie breaker...
51 26 3b 36 }	...for ICE control
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
9a ea a7 0c }	
bf d8 cb 56 }	
78 1e f2 b5 }	HMAC-SHA1 fingerprint
b2 d3 f2 49 }	
c1 b5 71 a2 }	
80 28 00 04	FINGERPRINT attribute header
e5 7a 3b cf	CRC32 fingerprint

2.2. Sample IPv4 response

[TOC](#)

This response used the following parameter:

Password: "V0kJxbRl1RmTxUk/WvJxBt" (without quotes)

Software name: "test vector" (without quotes)

Mapped address: 192.0.2.1 port 32853

01 01 00 3c	Response type and message length
21 12 a4 42	Magic cookie
b7 e7 a7 01 }	
bc 34 d6 86 }	Transaction ID
fa 87 df ae }	
80 22 00 0b	SOFTWARE attribute header
74 65 73 74 }	
20 76 65 63 }	UTF-8 server name
74 6f 72 20 }	
00 20 00 08	XOR-MAPPED-ADDRESS attribute header
00 01 a1 47	Address family (IPv4) and xor'd mapped port number
e1 12 a6 43	Xor'd mapped IPv4 address
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)

Software name: "test vector" (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	Magic cookie
b7 e7 a7 01 }	
bc 34 d6 86 }	Transaction ID
fa 87 df ae }	
80 22 00 0b	SOFTWARE attribute header
74 65 73 74 }	
20 76 65 63 }	UTF-8 server name
74 6f 72 20 }	
00 20 00 14	XOR-MAPPED-ADDRESS attribute header
00 02 a1 47	Address family (IPv6) and xor'd mapped port number
01 13 a9 fa }	
a5 d3 f1 79 }	Xor'd mapped IPv6 address
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

2.4. Sample request with long-term authentication

[TOC](#)

This request uses the following parameters:

Username:

"<U+30DE><U+30C8><U+30EA><U+30C3><U+30AF><U+30B9>" (without quotes) unaffected by SASLprep[\[RFC4013\]](#) (Zeilenga, K., "SASLprep: Stringprep Profile for User Names and Passwords," February 2005.) processing

Password: "The<U+00AD>M<U+00AA>tr<U+2168>" resp "TheMatrIX"

(without quotes) before resp after SASLprep processing

Nonce: "f//499k954d60L34oL9FSTvy64sA" (without quotes)

Realm: "example.org" (without quotes)

00 01 00 60	Request type and message length
21 12 a4 42	Magic cookie
78 ad 34 33 }	
c6 ad 72 c0 }	Transaction ID
29 da 41 2e }	
00 06 00 12	USERNAME attribute header
e3 83 9e e3 }	
83 88 e3 83 }	
aa e3 83 83 }	Username value (18 bytes) and padding (2 bytes)
e3 82 af e3 }	
82 b9 00 00 }	
00 15 00 1c	NONCE attribute header
66 2f 2f 34 }	
39 39 6b 39 }	
35 34 64 36 }	
4f 4c 33 34 }	Nonce value
6f 4c 39 46 }	
53 54 76 79 }	
36 34 73 41 }	
00 14 00 0b	REALM attribute header
65 78 61 6d }	
70 6c 65 2e }	Realm value (11 bytes) and padding (1 byte)
6f 72 67 00 }	
00 08 00 14	MESSAGE-INTEGRITY attribute header
f6 70 24 65 }	
6d d6 4a 3e }	
02 b8 e0 71 }	HMAC-SHA1 fingerprint
2e 85 c9 a2 }	
8c a8 96 66 }	

3. Security Considerations

[TOC](#)

There are no security considerations.

4. IANA Considerations

[TOC](#)

This document raises no IANA considerations.

[TOC](#)

5. Acknowledgements

The author would like to thank Marc Petit-Huguenin, Philip Matthews and Dan Wing for their inputs, and Brian Korver, Alfred E. Heggestad and Gustavo García for their reviews.

6. References

[TOC](#)

6.1. Normative References

[TOC](#)

[RFC5389]	Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, " Session Traversal Utilities for NAT (STUN) ," RFC 5389, October 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).

6.2. Informative References

[TOC](#)

[RFC2104]	Krawczyk, H. , Bellare, M. , and R. Canetti , " HMAC: Keyed-Hashing for Message Authentication ," RFC 2104, February 1997 (TXT).
[RFC4013]	Zeilenga, K. , " SASLprep: Stringprep Profile for User Names and Passwords ," RFC 4013, February 2005 (TXT).

Appendix A. Source code for test vectors

[TOC](#)

```
const unsigned char req[] =
    "\x00\x01\x00\x58"
    "\x21\x12\xa4\x42"
    "\xb7\xe7\xa7\x01\xbc\x34\xd6\x86\xfa\x87\xdf\xae"
    "\x80\x22\x00\x10"
    "STUN test client"
    "\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"
    "\x9a\xea\xa7\x0c\xbf\xd8\xcb\x56\x78\x1e\xf2\xb5"
    "\xb2\xd3\xf2\x49\xc1\xb5\x71\xa2"
    "\x80\x28\x00\x04"
    "\xe5\x7a\x3b\xcf";
```

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

```
const unsigned char req1tc[] =
    "\x00\x01\x00\x60"
    "\x21\x12\xa4\x42"
    "\x78\xad\x34\x33\xc6\xad\x72\xc0\x29\xda\x41\x2e"
    "\x00\x06\x00\x12"
    "\xe3\x83\x9e\xe3\x83\x88\xe3\x83\xaa\xe3\x83\x83"
    "\xe3\x82\xaf\xe3\x82\xb9\x00\x00"
    "\x00\x15\x00\x1c"
    "\x66\x2f\x2f\x34\x39\x39\x6b\x39\x35\x34\x64\x36"
    "\x4f\x4c\x33\x34\x6f\x4c\x39\x46\x53\x54\x76\x79"
    "\x36\x34\x73\x41"
    "\x00\x14\x00\x0b"
    "\x65\x78\x61\x6d\x70\x6c\x65\x2e\x6f\x72\x67\x00"
    "\x00\x08\x00\x14"
    "\xf6\x70\x24\x65\x6d\xd6\x4a\x3e\x02\xb8\xe0\x71"
    "\x2e\x85\xc9\xa2\x8c\xa8\x96\x66";
```

Request with long-term credentials

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 (2008).

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.