

[patch 2/3] tcrypt: Add a self test for the zlib crypto module

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2008-08/msg12672.html>

- *From:* Geert Uytterhoeven <Geert.Uytterhoeven@xxxxxxxxxxx>
 - *Date:* Fri, 29 Aug 2008 15:42:00 +0200
-

From: Geert Uytterhoeven <Geert.Uytterhoeven@xxxxxxxxxxx>

Signed-off-by: Geert Uytterhoeven <Geert.Uytterhoeven@xxxxxxxxxxx>

crypto/tcrypt.c | 9 ++++++
crypto/tcrypt.h | 81 +++
2 files changed, 90 insertions(+)

```
--- a/crypto/tcrypt.c
+++ b/crypto/tcrypt.c
@@ -1400,6 +1400,9 @@ static void do_test(void)
DEFLATE_DECOMP_TEST_VECTORS);
test_comp("lzo", lzo_comp_tv_template, lzo_decomp_tv_template,
LZO_COMP_TEST_VECTORS, LZO_DECOMP_TEST_VECTORS);
+ test_comp("zlib", zlib_comp_tv_template,
+ zlib_decomp_tv_template, ZLIB_COMP_TEST_VECTORS,
+ ZLIB_DECOMP_TEST_VECTORS);
test_hash("crc32c", crc32c_tv_template, CRC32C_TEST_VECTORS);
test_hash("hmac(md5)", hmac_md5_tv_template,
HMAC_MD5_TEST_VECTORS);
@@ -1701,6 +1704,12 @@ static void do_test(void)
test_hash("rmd320", rmd320_tv_template, RMD320_TEST_VECTORS);
break;

+ case 43:
+ test_comp("zlib", zlib_comp_tv_template,
+ zlib_decomp_tv_template, ZLIB_COMP_TEST_VECTORS,
+ ZLIB_DECOMP_TEST_VECTORS);
+ break;
+
case 100:
test_hash("hmac(md5)", hmac_md5_tv_template,
HMAC_MD5_TEST_VECTORS);
--- a/crypto/tcrypt.h
+++ b/crypto/tcrypt.h
@@ -8512,6 +8512,87 @@ static struct comp_testvec lzo_decomp_tv
};
```

[patch 2/3] tcrypt: Add a self test for the zlib crypto module

```
/*
+ * Zlib test vectors (null-terminated strings).
+ * Params: winbits=DEF_WBITS, Z_DEFAULT_COMPRESSION, MAX_MEM_LEVEL.
+ */
+#define ZLIB_COMP_TEST_VECTORS 2
+#define ZLIB_DECOMP_TEST_VECTORS 2
+
+static struct comp_testvec zlib_comp_tv_template[] = {
+ {
+ .inlen = 70,
+ .outlen = 44,
+ .input = "Join us now and share the software "
+ "Join us now and share the software ",
+ .output = "\x78\x9c\xf3\xca\xcf\xcc\x53\x28"
+ "\x2d\x56\xc8\xcb\x2f\x57\x48\xcc"
+ "\x4b\x51\x28\xce\x48\x2c\x4a\x55"
+ "\x28\xc9\x48\x55\x28\xce\x4f\x2b"
+ "\x29\x07\x71\xbc\x08\x2b\x01\x00"
+ "\x7c\x65\x19\x3d",
+ }, {
+ .inlen = 191,
+ .outlen = 128,
+ .input = "This document describes a compression method based on the DEFLATE"
+ "compression algorithm. This document defines the application of "
+ "the DEFLATE algorithm to the IP Payload Compression Protocol.",
+ .output = "\x78\x9c\x5d\x8d\x31\x0e\xc2\x30"
+ "\x10\x04\xbf\xb2\x2f\xc8\x1f\x10"
+ "\x04\x09\x89\xc2\x85\x3f\x70\xb1"
+ "\x2f\xf8\x24\xdb\x67\xd9\x47\xc1"
+ "\xef\x49\x68\x12\x51\xae\x76\x67"
+ "\xd6\x27\x19\x88\x1a\xde\x85\xab"
+ "\x21\xf2\x08\x5d\x16\x1e\x20\x04"
+ "\x2d\xad\xf3\x18\xa2\x15\x85\x2d"
+ "\x69\xc4\x42\x83\x23\xb6\x6c\x89"
+ "\x71\x9b\xef\xcf\x8b\x9f\xcf\x33"
+ "\xca\x2f\xed\x62\xa9\x4c\x80\xff"
+ "\x13\xaf\x52\x37\xed\x0e\x52\x6b"
+ "\x59\x02\xd9\x4e\xe8\x7a\x76\x1d"
+ "\x02\x98\xfe\x8a\x87\x83\xa3\x4f"
+ "\x56\x8a\xb8\x9e\x8e\x5c\x57\xd3"
+ "\xa0\x79\xfa\x02\xe\x32\x45\x4e",
+ },
+};
+
+static struct comp_testvec zlib_decomp_tv_template[] = {
+ {
+ .inlen = 128,
+ .outlen = 191,
+ .input = "\x78\x9c\x5d\x8d\x31\x0e\xc2\x30"
+ "\x10\x04\xbf\xb2\x2f\xc8\x1f\x10"
+ "\x04\x09\x89\xc2\x85\x3f\x70\xb1"
```

[patch 2/3] tcrypt: Add a self test for the zlib crypto module

```
+ "\x2f\xf8\x24\xdb\x67\xd9\x47\xc1"
+ "\xef\x49\x68\x12\x51\xae\x76\x67"
+ "\xd6\x27\x19\x88\x1a\xde\x85\xab"
+ "\x21\xf2\x08\x5d\x16\x1e\x20\x04"
+ "\x2d\xad\xf3\x18\xa2\x15\x85\x2d"
+ "\x69\xc4\x42\x83\x23\xb6\x6c\x89"
+ "\x71\x9b\xef\xcf\x8b\x9f\xcf\x33"
+ "\xca\x2f\xed\x62\xa9\x4c\x80\xff"
+ "\x13\xaf\x52\x37\xed\x0e\x52\x6b"
+ "\x59\x02\xd9\x4e\xe8\x7a\x76\x1d"
+ "\x02\x98\xfe\x8a\x87\x83\xa3\x4f"
+ "\x56\x8a\xb8\x9e\x8e\x5c\x57\xd3"
+ "\xa0\x79\xfa\x02\xe\x32\x45\xe",
+ .output = "This document describes a compression method based on the DEFLATE"
+ "compression algorithm. This document defines the application of "
+ "the DEFLATE algorithm to the IP Payload Compression Protocol.",
+ }, {
+ .inlen = 44,
+ .outlen = 70,
+ .input = "\x78\x9c\xf3\xca\xcf\xcc\x53\x28"
+ "\x2d\x56\xc8\xcb\x2f\x57\x48\xcc"
+ "\x4b\x51\x28\xce\x48\x2c\x4a\x55"
+ "\x28\xc9\x48\x55\x28\xce\x4f\x2b"
+ "\x29\x07\x71\xbc\x08\x2b\x01\x00"
+ "\x7c\x65\x19\x3d",
+ .output = "Join us now and share the software "
+ "Join us now and share the software ",
+ },
+};
+
+/*
+ * Michael MIC test vectors from IEEE 802.11i
+ */
+#define MICHAEL_MIC_TEST_VECTORS 6
```

—
With kind regards,

Geert Uytterhoeven
Software Architect

Sony Techsoft Centre Europe
The Corporate Village • Da Vincilaan 7–D1 • B–1935 Zaventem • Belgium

Phone: +32 (0)2 700 8453
Fax: +32 (0)2 700 8622
E–mail: Geert.Uytterhoeven@xxxxxxxxxxxxx
Internet: <http://www.sony-europe.com/>

A division of Sony Europe (Belgium) N.V.
VAT BE 0413.825.160 • RPR Brussels

[patch 2/3] tcrypt: Add a self test for the zlib crypto module

Fortis Â· BIC GEBABEBB Â· IBAN BE41293037680010

—

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to majordomo@xxxxxxxxxxxxxxxx

More majordomo info at <http://vger.kernel.org/majordomo-info.html>

Please read the FAQ at <http://www.tux.org/lkml/>