# strongSwan - Bug #474

## test_rsa.c:123:E:generate:test_gen fails with timeout on exotic architectures

31.12.2013 05:39 - Jonathan Davies

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 31.12.2013 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Tobias Brunner | **Estimated time:** | 0.00 hour |
| **Category:** | testing | | |
| **Target version:** | 5.1.2 | | |
| **Affected version:** | 5.1.1 | **Resolution:** | Fixed |

**Description**

Hello,

After enabling units tests on package builds for the Ubuntu packages, I noticed that the builds would fail on "exotic" architectures but not amd64 or i386:

- https://launchpad.net/ubuntu/+source/strongswan/5.1.1-0ubuntu8

Build logs can be found on the linked arches pages, but a full build log can be found here:

- https://launchpad.net/ubuntu/+source/strongswan/5.1.1-0ubuntu8/+build/5396718/+files/buildlog_ubuntu-trusty-armhf.strongswan_5.1.1-0ubuntu8_FAILEDTOBUILD.txt.gz

The failure message "FAIL: test_runner" isn't very descriptive. However, I manually ran the build on a porter machine (log attached) and discovered that it was:

"test_rsa.c:123:E:generate:test_gen:4: (after this point) Test timeout expired"

...that was failing.

Changing the "tcase_set_timeout(tc, 8);" for the generate unit test to 30 - makes the build work again fine (anything lower - failed).

Should I patch the code to make it 30? Or should I make the package test which arch it's building on?

### Associated revisions

**Revision 303ec395 - 20.01.2014 15:40 - Tobias Brunner**

unit-tests: Add environment variable to reduce the number of generated keys

If TESTS_REDUCED_KEYLENGTHS is set RSA and ECDSA keys are only generated
for the lowest configured key length.

Fixes #474.

### History

**#1 - 31.12.2013 08:55 - Jonathan Davies**

Jonathan Davies wrote:

> Changing the "tcase_set_timeout(tc, 8);" for the generate unit test to 30 - makes the build work again fine (anything lower - failed).

So I was able to resolve this on armhf and arm64 by setting the environment variable CK_TIMEOUT_MULTIPLIER to 6.

Setting it up to 10 didn't fix it on powerpc - I'm going to try and find one and test variables on it there rather than cog the buildd system with package uploads. In the mean time, I've disabled unit tests on powerpc.

**#2 - 03.01.2014 07:32 - Jonathan Davies**

I've also noticed that this occasionally hangs on i386.

Would it be possible to have an option to have the test suite read data from /dev/urandom ?

#### #3 - 06.01.2014 18:58 - Tobias Brunner

*- Category set to testing*

*- Status changed from New to Feedback*

*- Assignee set to Tobias Brunner*

> So I was able to resolve this on armhf and arm64 by setting the environment variable CK_TIMEOUT_MULTIPLIER to 6.

This won't work with 5.1.2 anymore because we now use our own test runner (but we could, of course, add a similar option if that would help you).

> Would it be possible to have an option to have the test suite read data from /dev/urandom ?

The test runner already configures this for the *random* plugin. The problem is, though, that if the *openssl* plugin is enabled (which is listed before the *gmp* plugin in the default plugin list) the RSA keys are generated by OpenSSL, which reads from /dev/urandom but also from /dev/random so it might still take a while if not enough entropy is available (OpenSSL's entropy source can't be changed dynamically).

If increasing the timeout works for you, then adding an environment variable to do so might be an option.

Alternatively, we could add an environment variable to disable these potentially blocking test cases (test_gen in test_rsa.c and test_ecdsa.c) e.g. TESTS_DISABLE_KEY_GEN=1.

#### #4 - 07.01.2014 18:35 - Jonathan Davies

Tobias Brunner wrote:

> > So I was able to resolve this on armhf and arm64 by setting the environment variable CK_TIMEOUT_MULTIPLIER to 6.
>
> This won't work with 5.1.2 anymore because we now use our own test runner (but we could, of course, add a similar option if that would help you).
>
> > Would it be possible to have an option to have the test suite read data from /dev/urandom ?
>
> The test runner already configures this for the *random* plugin. The problem is, though, that if the *openssl* plugin is enabled (which is listed before the *gmp* plugin in the default plugin list) the RSA keys are generated by OpenSSL, which reads from /dev/urandom but also from /dev/random so it might still take a while if not enough entropy is available (OpenSSL's entropy source can't be changed dynamically).
>
> If increasing the timeout works for you, then adding an environment variable to do so might be an option.

There is something strange happening here. Here's where it failed once with i386:

- https://launchpadlibrarian.net/161726105/buildlog_ubuntu-saucy-i386.strongswan_5.1.2~dr2-0~10365~ubuntu13.10.1_FAILEDTOBUILD.txt.gz

As you can see, it actually timed out in this case:

```
  Running suite 'rsa':
    Running case 'generate': +++++-
      Failure in 'test_gen': timeout(14) (i = 5)
 dumping 1 stack frame addresses:
    [0x55a773ca]
```

However, on my package upload yesterday, it failed on armhf with:

https://launchpadlibrarian.net/161760200/buildlog_ubuntu-trusty-armhf.strongswan_5.1.2~dr2%2Bgit20130106-0ubuntu2_FAILEDTOBUILD.txt.gz

```
  Running suite 'rsa':

Session terminated, terminating shell... ...terminated.
    Running case 'generate': ++++make[3]: *** wait: No child processes.  Stop.
make[3]: *** Waiting for unfinished jobs....
make[3]: *** wait: No child processes.  Stop.
make[2]: *** [check-recursive] Terminated
make[1]: *** [check] Terminated
make[5]: *** [check-recursive] Terminated
make[4]: *** [check] Terminated
make[7]: *** wait: No child processes.  Stop.
make[7]: *** Waiting for unfinished jobs....
make[7]: *** wait: No child processes.  Stop.
```

```
make: *** [build-arch] Terminated
make[6]: *** [check-am] Error 2
Build killed with signal 15 after 360 minutes of inactivity
```

For 6 hours, the build sat and did nothing.

I could reproduce the above on a amd64 cloud instance by running "make check" repeatedly. Occasionally, the suite would just hang for whatever reason.

> Alternatively, we could add an environment variable to disable these potentially blocking test cases (test_gen in test_rsa.c and test_ecdsa.c) e.g. TESTS_DISABLE_KEY_GEN=1.

This is an option, but ideally, I'd like the test suite to run back-to-back to make sure we're covered. :)

#### #5 - 20.01.2014 15:47 - Tobias Brunner

*- Tracker changed from Issue to Bug*

*- Status changed from Feedback to Closed*

*- Target version set to 5.1.2*

*- Resolution set to Fixed*

With the associated commit, and if the TESTS_REDUCED_KEYLENGTHS environment variable is set, keys are generated with the lowest configured key length only.

### Files

| | | | |
|---|---|---|---|
| strongswan-unit-test-build-failure.log | 1.05 KB | 31.12.2013 | Jonathan Davies |