libosmocore - Bug #1694

integrate debian patches

04/22/2016 12:13 PM - msuraev

Status:	Resolved	**Start date:**	04/22/2016
Priority:	High	**Due date:**	
Assignee:	msuraev	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

The libosmocore (and other parts) have been integrated into debian/ubuntu repos. The packaging (debian/ directory) slightly differs from our repos: some patches etc. It might make sense to integrate relevant changes.

Related issues:

Related to libosmocore - Feature #2610: optimize GnuTLS fallback	**New**	**11/02/2017**

History

#1 - 11/09/2016 10:21 AM - laforge

- Assignee set to msuraev

#2 - 12/14/2016 12:45 PM - msuraev

- Status changed from New to Stalled

- % Done changed from 0 to 10

Gerrit #1426 has been sent for review.

#3 - 12/15/2016 03:14 PM - laforge

#4 - 12/19/2016 04:13 PM - msuraev

libosmocore in Debian got 6 patches:
1,6 - erroneous
2,4 - already applied
3,5 - specific to Debian build process

#5 - 12/20/2016 06:12 PM - msuraev

openbsc got 5 patches:
2 are already fixed,
1 is debian-specific,
2 others are adopted into gerrit #1463 and 1464

#6 - 12/20/2016 06:12 PM - msuraev

- Status changed from Stalled to In Progress

#7 - 12/21/2016 01:07 PM - msuraev

libosmo-sccp have 3 patches:
- already fixed
- debian-specific
- conflicting with current master
General changes to debian/ were sent for review in gerrit # 1468.

#8 - 12/22/2016 01:52 PM - msuraev

- % Done changed from 10 to 20

Changes submitted to gerrit in 1469, 1473, 1478-1481, 1483-1485. The more intrusive changes are left for further iterations.

#9 - 12/24/2016 12:35 PM - msuraev

- Status changed from In Progress to Stalled

#10 - 12/27/2016 11:03 AM - msuraev

- Related to Feature #1894: include gnutls into our sdk added

#11 - 12/27/2016 11:05 AM - msuraev

- Related to deleted (Feature #1894: include gnutls into our sdk)

#12 - 12/27/2016 11:05 AM - msuraev

- Blocked by Feature #1894: include gnutls into our sdk added

#13 - 06/15/2017 02:05 PM - msuraev

Gerrit 1464, 1526 are under review.

#14 - 10/05/2017 06:24 AM - laforge

ping? no status update for 3 months?

#15 - 10/05/2017 08:41 AM - msuraev

- % Done changed from 20 to 30

Blocked by on-going discussion on OpenSSL and getrandom(). The biggest piece which is still out there is license incompatibility due to use of OpenSSL functions.

Proposed solutions:
- use re-licensed (under Apache 2.0) OpenSSL
- use getrandom()

The patches implementing 2nd approach are available in gerrit 1526, 3819-3821.

The downsides:
- the process of re-licensing of OpenSSL is not finished yet, it's unclear from which version onwards it'll be under Apache 2.0 and when this version hits the repositories.
- exessive use of random might (in theory) deplete entropy pool.

The last problem is not specific to either solution but can occur on both of them. So far we've dealt with it by falling back to insecure random generator while logging warning message.

#16 - 10/11/2017 08:32 AM - laforge

- Priority changed from Normal to High

random-related patches have been merged, so please un-stall this.

#17 - 10/11/2017 12:03 PM - msuraev

- Status changed from Stalled to In Progress

- % Done changed from 30 to 40

Before merging related gerrit 3819-3821 we have to figure out why SYS_getrandom is undefined in case of our jenkins build. Initially I've suspected that configure test somehow fails but according to test results on gerrit 4193 that's not the case.

#18 - 10/12/2017 12:44 PM - msuraev

- Status changed from In Progress to Feedback

On OBS SYS_getrandom is detected properly on all distros with the exception of debian 8. The getrandom syscall was introduced in kernel 3.17, Debian 8 has 3.16 according to https://wiki.debian.org/DebianJessie

From libosmocore PoV it's fine, however applications which do not implement insecure random fallback won't work on Debian 8. Not sure what shall I do about it?

#19 - 10/12/2017 02:00 PM - laforge

On Thu, Oct 12, 2017 at 12:44:59PM +0000, msuraev [REDMINE] wrote:

> Issue #1694 has been updated by msuraev.
>
> Status changed from In Progress to Feedback
>
> On OBS SYS_getrandom is detected properly on all distros with the exception of debian 8. The getrandom syscall was introduced in kernel 3.17, Debian 8 has 3.16 according to https://wiki.debian.org/DebianJessie
>
> From libosmocore PoV it's fine, however applications which do not implement insecure random fallback won't work on Debian 8. Not sure what shall I do about it?

sigh. Guess we need a compile-time switch for libosmocore to use openssl, after all.

The default should be off, but on Debian 8 or other older environments, this could be enabled
at compile time, at which point ./configure must find openssl or otherwise abort.

I'd rather not leave this up to each application to resolve by itself.

lick here: https://osmocom.org/my/account

#20 - 10/16/2017 12:02 PM - msuraev

laforge wrote:

> **sigh**. Guess we need a compile-time switch for libosmocore to use openssl, after all.

This would not resolve the licensing issue - it will just move it from osmo-* to libosmocore and limit it to Debian 8 (which I think is as unlikely to get apache-licensed openssl as newer kernel with getrandom). I propose to use GnuTLS instead (it's license-compatible and available in Debian 8) as was the case with the earlier version of the patch.

> The default should be off, but on Debian 8 or other older environments, this could be enabled
> at compile time, at which point ./configure must find openssl or otherwise abort.

We can just enable it as a fallback to missing *getrandom instead of current "always return failure" fallback. Is there a case when we'd like to turn off this GnuTLS fallback and use current failure mode instead?

> lick here: https://osmocom.org/my/account

I'd rather not :-)

#21 - 11/02/2017 04:37 PM - msuraev

- Status changed from Feedback to Stalled

Gerrit 4593 with fallback implementation is under review. Once it's merged, 3819-3821 jenkins tests should be retriggered.

#22 - 11/02/2017 04:38 PM - msuraev

- Related to Feature #2610: optimize GnuTLS fallback added

#23 - 11/02/2017 04:38 PM - msuraev

- Blocked by deleted (Feature #1894: include gnutls into our sdk)

#24 - 11/21/2017 06:35 PM - msuraev

- % Done changed from 40 to 60

4593 is merged, 3819-3821 were updated.

#25 - 01/02/2018 03:54 PM - msuraev

- Status changed from Stalled to Resolved

- % Done changed from 60 to 100

Remaining patches 3819-3821 were merged. There's ongoing .deb packaging project - see https://osmocom.org/news/81 so we can close this ticket.