Ruby - Bug #6990

test_s_random_bytes_without_openssl error on Windows x64

09/07/2012 07:36 AM - h.shirosaki (Hiroshi Shirosaki)

Status:	Closed		
Priority:	Normal		
Assignee:	h.shirosaki (Hiroshi Shirosaki)		
Target version:	2.0.0		
ruby -v:	ruby 2.0.0dev (2012-09-06 trunk 36917) [x64-mingw32]	**Backport:**	

Description

=begin

TestSecureRandom sometimes has an error on ci.rubyinstaller.

http://ci.rubyinstaller.org/job/ruby-trunk-x64-test-all/41/console

1. Error:
   test_s_random_bytes_without_openssl(TestSecureRandom):
   SystemCallError: unknown error - CryptGenRandom failed: The parameter is incorrect.
   C:/Users/Worker/Jenkins/workspace/ruby-trunk-x64-build/lib/securerandom.rb:116:in random_bytes'
   C:/Users/Worker/Jenkins/workspace/ruby-trunk-x64-build/test/test_securerandom.rb:12:in test_s_random_bytes'
   C:/Users/Worker/Jenkins/workspace/ruby-trunk-x64-build/test/test_securerandom.rb:97:in block in
   test_s_random_bytes_without_openssl' C:/Users/Worker/Jenkins/workspace/ruby-trunk-x64-build/lib/tmpdir.rb:88:in mktmpdir'
   C:/Users/Worker/Jenkins/workspace/ruby-trunk-x64-build/test/test_securerandom.rb:85:in
   `test_s_random_bytes_without_openssl'

This error seems to occur only on x64.

I guess the following scenario.

Pointer size of @hProv seems limited to 32bit with x64 ruby.
If the pointer value was larger than 32bit max, it would fail.

https://github.com/ruby/ruby/blob/trunk/lib/securerandom.rb#L106

I don't get the error at test-all on my local box, but I can get same error with the following script.
It takes long time to get the error.

```
require "openssl"
OpenSSL.send(:remove_const, :Random)
require "securerandom"

i = 0
loop do
SecureRandom.random_bytes
SecureRandom.send(:remove_instance_variable, :@has_win32)
p SecureRandom.send(:instance_variable_get, :@hProv).to_s(16) if (i % 10000) == 0
i += 1
end
```

I attached a patch. I also fixed encoding error which occurs if error message contains Japanese characters.

=end

Associated revisions

Revision 3207af4cb841872176ad0ba5cc62f868b83ee769 - 09/13/2012 01:01 PM - h.shirosaki (Hiroshi Shirosaki)

lib/securerandom.rb: fix errors on Windows

- lib/securerandom.rb (SecureRandom.random_bytes):
  Use 64bit value as pointer for Windows x64 to fix SystemCallError.

- lib/securerandom.rb (SecureRandom.lastWin32ErrorMessage):
  Set proper encoding to avoid invalid byte sequence error.
  [ruby-core:47451] [Bug #6990]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@36961 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 3207af4c - 09/13/2012 01:01 PM - h.shirosaki (Hiroshi Shirosaki)

lib/securerandom.rb: fix errors on Windows

- lib/securerandom.rb (SecureRandom.random_bytes):
  Use 64bit value as pointer for Windows x64 to fix SystemCallError.

- lib/securerandom.rb (SecureRandom.lastWin32ErrorMessage):
  Set proper encoding to avoid invalid byte sequence error.
  [ruby-core:47451] [Bug #6990]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@36961 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 9bb55f7633a1a6c88efb9bd3581cf7f71b20fc23 - 11/05/2012 02:00 PM - h.shirosaki (Hiroshi Shirosaki)

- ext/dl/win32/lib/Win32API.rb (Win32API#call): use 64bit pointer for x64
  Windows. This would fix
  TestSecureRandom#test_s_random_bytes_without_openssl error.
  [ruby-core:47451] [Bug #6990]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@37476 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 9bb55f76 - 11/05/2012 02:00 PM - h.shirosaki (Hiroshi Shirosaki)

- ext/dl/win32/lib/Win32API.rb (Win32API#call): use 64bit pointer for x64
  Windows. This would fix
  TestSecureRandom#test_s_random_bytes_without_openssl error.
  [ruby-core:47451] [Bug #6990]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@37476 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 09/12/2012 12:23 AM - luislavena (Luis Lavena)

=begin
I can confirm that after reaching 1.9GB of RAM usage, it fails with:

"7e7e6cb0"
C:/Users/Worker/Code/ruby-2.0.0-r36949-x64-mingw32/lib/ruby/2.0.0/securerandom.rb:116:in random_bytes': unknown error - CryptGenRandom failed: The parameter is incorrect. (SystemCallError) from a.rb:7:in block in '
from a.rb:11:in loop' from a.rb:11:in '

I'm applying the patch now and doing a build to confirm.

=end

#2 - 09/12/2012 01:05 AM - luislavena (Luis Lavena)

- Category set to test

- Status changed from Open to Assigned

- Assignee set to usa (Usaku NAKAMURA)

- Target version set to 2.0.0

I can confirm patch work.

Usa, do you have any objection with path?

Thank you.

#3 - 09/12/2012 12:36 PM - usa (Usaku NAKAMURA)

Most it's okay.
There is a problem in the last chunk.

Rather than filesystem encoding, I think that locale encoding is suitable.

#4 - 09/12/2012 12:40 PM - usa (Usaku NAKAMURA)

If you can agree with my opinion, Luis, please correct the patch
and commit it.
Or if you cannot agree by any means, please commit it as it is :)

#5 - 09/13/2012 01:10 AM - luislavena (Luis Lavena)

- Assignee changed from usa (Usaku NAKAMURA) to h.shirosaki (Hiroshi Shirosaki)

Thank you Usa,

Hiroshi, leaving to you to commit.

#6 - 09/13/2012 09:59 PM - h.shirosaki (Hiroshi Shirosaki)

=begin
Language of FormatMessage seems not affected by console code page.

Test using locale:
msg[0, len].force_encoding("locale").tr("\r", '').chomp

"locale" means console code page on Windows ruby.
But changing console code page doesn't affect message language. Message seems always cp932 Japanese on Windows 7.

```
type message.rb
require "openssl"
OpenSSL.send(:remove_const, :Random)
require "securerandom"


SecureRandom.random_bytes
SecureRandom.send(:instance_variable_set, :@hProv, 0)
SecureRandom.random_bytes
```

```
chcp 932
ruby message.rb
V:/ruby19_mingw/lib/ruby/2.0.0/securerandom.rb:117:in random_bytes': unknown error - CryptGenRandom   failed: □□□□□□□□□□□□□□□□
(SystemCallError)         from message.rb:7:in '
```

```
chcp 65001
ruby message.rb
V:/ruby19_mingw/lib/ruby/2.0.0/securerandom.rb:264:in tr': invalid byte sequence in UTF-8 (Argument  Error)         from
V:/ruby19_mingw/lib/ruby/2.0.0/securerandom.rb:264:in lastWin32ErrorMessage'
from V:/ruby19_mingw/lib/ruby/2.0.0/securerandom.rb:117:in random_bytes'         from message.rb:7:in '
```

```
chcp 1252
ruby message.rb
V:/ruby19_mingw/lib/ruby/2.0.0/securerandom.rb:117:in random_bytes': unknown error - CryptGenRandom   failed: ??????????????
(SystemCallError)         from message.rb:7:in '
```

But on Windows XP, message language seems determined by console code page. With not 932 code page, message is English.

To avoid invalid byte sequence error with String#tr, I would like to set filesystem encoding.
If you know better way, please correct it.

=end

#7 - 09/13/2012 10:01 PM - Anonymous

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r36961.
Hiroshi, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

---

lib/securerandom.rb: fix errors on Windows

- lib/securerandom.rb (SecureRandom.random_bytes):
  Use 64bit value as pointer for Windows x64 to fix SystemCallError.

- lib/securerandom.rb (SecureRandom.lastWin32ErrorMessage):
  Set proper encoding to avoid invalid byte sequence error.
  [ruby-core:47451] [Bug #6990]

Files

fix_securerandom_x64.patch	1.35 KB	09/07/2012	h.shirosaki (Hiroshi Shirosaki)