Contents

NAME

Crypt::URandom - Provide non blocking randomness

VERSION

This document describes Crypt::URandom version 0.55

SYNOPSIS

```
        use Crypt::URandom();

        my $random_string_50_bytes_long = Crypt::URandom::urandom(50);
```

OR

DESCRIPTION

This Module is intended to provide an interface to the strongest available source of non-blocking randomness on the current platform. Platforms currently supported are anything supporting getrandom(2), /dev/urandom and versions of Windows greater than or equal to Windows 2000.

SUBROUTINES/METHODS

`urandom`

This function accepts an integer and returns a string of the same size filled with random data. It will throw an exception if the requested amount of random data is not returned. The first call will initialize the native cryptographic libraries (if necessary) and load all the required Perl libraries. This call is a buffered read on non Win32 platforms that do not support getrandom(2) or equivalent.

`urandom_ub`

This function accepts an integer and returns a string of the same size filled with random data. It will throw an exception if the requested amount of random data is not returned. The first call will initialize the native cryptographic libraries (if necessary) and load all the required Perl libraries. This call is a unbuffered sysread on non Win32 platforms that do not support getrandom(2) or equivalent.

`getrandom`

This function accepts an integer and returns a string of the same size filled with random data on platforms that implement getrandom(2). It will throw an exception if the requested amount of random data is not returned. This is NOT portable across all operating systems, but is made available if high-speed generation of random numbers is required. If an integer is not supplied as an argument, this function will return a empty string as a result (the same as if the integer 0 is supplied as an argument)

DIAGNOSTICS

`No secure alternative for random number generation for Win32 versions older than W2K`

The module cannot run on versions of Windows earlier than Windows 2000 as there is no cryptographic functions provided by the operating system.

`Could not import CryptAcquireContext`

CryptAcquireContext failed

The module was unable to call the CryptAcquireContextA function from the advapi32 dynamic library.

Could not import CryptGenRandom

The module was unable to load the CryptGenRandom function from the advapi32 dynamic library.

Could not import SystemFunction036

The module was unable to load the SystemFunction036 function from the advapi32 dynamic library.

The length argument must be supplied and must be an integer

The get method must be called with an integer argument to describe how many random bytes are required.

CryptGenRandom failed

The Windows 2000 CryptGenRandom method call failed to generate the required amount of randomness

RtlGenRand failed

The post Windows 2000 RtlGenRand method call failed to generate the required amount of randomness

Only read n bytes from path

The /dev/urandom device did not return the desired amount of random bytes

Failed to read from path

The /dev/urandom device returned an error when being read from

Failed to open path

The /dev/urandom device returned an error when being opened

CONFIGURATION AND ENVIRONMENT

Crypt::URandom requires no configuration files or environment variables.

If the environment variable CRYPT_URANDOM_BUILD_DEBUG is specified when running `perl Makefile.PL` or `make test` AND getrandom(2) or it's equivalents cannot be detected, extra debug will be shown to show the failures to detect these functions.

If the platform is Win32, the Win32::API module will be required. Otherwise no other modules other than those provided by perl will be required

INCOMPATIBILITIES

None reported.

BUGS AND LIMITATIONS

To report a bug, or view the current list of bugs, please visit https://github.com/david-dick/crypt-urandom/issues

AUTHOR

David Dick <ddick@cpan.org>

ACKNOWLEDGEMENTS

The Win32::API code for interacting with Microsoft's CryptoAPI was copied with extreme gratitude from Crypt::Random::Source::Strong::Win32 by Max Kanat-Alexander

LICENSE AND COPYRIGHT

DISCLAIMER OF WARRANTY

REDISTRIBUTE THE SOFTWARE AS PERMITTED BY THE ABOVE LICENCE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE SOFTWARE TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.