

Re: PuTTY keygen

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2002-06/0169.html>

From: Jon McClelland (dowot69@hotmail.com)

Date: 06/12/02

From: dowot69@hotmail.com (Jon McClelland)

Date: 12 Jun 2002 03:38:26 -0700

Simon Tatham <anakin@pobox.com> wrote in message news:<gQn*vasqp@news.chiark.greenend.org.uk>...

> *Jon McClelland* <dowot69@hotmail.com> wrote:

> > *Has anyone come across a command-line version of puttygen.exe?*

> > *I don't want our users to have to select RSA-2, wiggle the mouse &*

> > *(worst of all) save the key in the right place!*

>

> *If we were to produce a command-line PuTTYgen, where would you want*

> *it to get its random numbers from if it didn't accept mouse input*

> *from the users?*

>

> *The other points are merely UI changes and in principle I wouldn't*

> *have a problem with a command line supplying a different UI. But to*

> *generate a key you _need_ a large amount of high-quality entropy,*

> *and if you know of a place I can get that from without asking for*

> *user input then feel free to mention it.*

Simon,

I appreciate the offer to produce a command line PuTTYgen. Some digging around shows that Microsoft has some inbuilt APIs to produce random numbers. Here's some of the info I found (sorry if this something you've already looked into)...

In Windows, call a function such as CryptGenRandom, which has two of the properties of a good random number generator, unpredictability and even value distribution. This function, declared in Wincrypt.h, is available on just about every Windows platform, including Windows 95 with Internet Explorer 3.02 or later, Windows 98, Windows Me, Windows CE v3, Windows NT 4, Windows 2000, and Windows XP.

CryptGenRandom gets its randomness, also known as entropy, from many sources in Windows 2000, including the following:

The current process ID (GetCurrentProcessID).

The current thread ID (GetCurrentThreadID).

The ticks since boot (GetTickCount).

The current time (GetLocalTime).

Various high-precision performance counters (QueryPerformanceCounter).

comp.security.ssh: Re: PuTTY keygen

A Message Digest 4 (MD4) hash of the user's environment block, which includes username, computer name, and search path.

High-precision internal CPU counters, such as RDTSC, RDMSR, RDPMC (x86 only—more information about these counters is at developer.intel.com/software/idap/resources/technical_collateral/pentiumii/RDTSCPM1.HTM <<http://developer.intel.com>>).

Low-level system information, such as idle time, kernel time, interrupt times, commit limit, page read count, cache read count, nonpaged pool allocations, alignment fixup count, operating system lookaside information.

Such information is added to a buffer, which is hashed using MD4 and used as the key to modify a buffer, using RC4, provided by the user. (Refer to the CryptGenRandom documentation in the Platform SDK for more information about the user-provided buffer.) Hence, if the user provides additional data in the buffer, this is used as an element in the witches brew to generate the random data. The result is a cryptographically random number generator.

Also, note that if you plan to sell your software to the United States federal government, you'll need to use FIPS 140-1-approved algorithms. The default versions of CryptGenRandom in Microsoft Windows CE v3, Windows 95, Windows 98, Windows Me, Windows 2000, and Windows XP are FIPS-approved. Obviously FIPS-140 compliance is necessary but not sufficient to provide a properly secure source of random data.

- ***Next message:*** [Stefan Schumacher: "Re: PuTTY keygen"](#)
- ***Previous message:*** [Stefan Schumacher: "Re: How do I get OpenSSH to require both RSA and password authorization?"](#)
- ***Maybe in reply to:*** [Jon McClelland: "PuTTY keygen"](#)
- ***Next in thread:*** [Stefan Schumacher: "Re: PuTTY keygen"](#)
- ***Reply:*** [Stefan Schumacher: "Re: PuTTY keygen"](#)
- ***Messages sorted by:*** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)