The random number seed can be the weakest link

devblogs.microsoft.com/oldnewthing/20040412-00

April 12, 2004

Raymond Chen

Random number generation is hard. That's why you should leave it to the experts. But even if you choose a good random number generator, you still have to seed it properly. The best random number generator in the world isn't very useful if people can guess the seed. That's why seeding the random number generator with the current time is not very secure; it's not hard to guess the current time! So it's important to throw something unguessable into the seed. As the above paper notes, just the time and process id are not good enough.

So what should you do? Don't ask me; I'm not a cryptography expert. Here are some suggestions from other people. Maybe some of them are good, maybe not.

Raymond Chen

Follow