How secure are GUIDs? Can I use it to generate passwords?

July 1, 2015

Raymond Chen

GUIDs are globally unique identifiers, and given their rather incomprehensible presentation, some people may be tempted to use them (or parts of them) as passwords. For example, one person wondered whether it was okay to use the first eight characters of a GUID as a temporary account password.

This is a really bad idea. GUIDs are designed for uniqueness, not for security.

For example, we saw that underline substrings of GUIDs are not unique. For example, in the classic v1 algorithm, the first part of the GUID is a timestamp. Timestamps are a great technique for helping to build uniqueness, but they are horrifically insecure because, well, duh, the current time is hardly a secret!

Using the first eight characters of a v1 GUID as a password is equivalent to using the current time as a password. And given that the current time isn't a secret, you made things an awful lot easier for the bad guys. All they need to know is what time you generated the GUID and they can get the first eight characters. Even if they don't know the exact time, if they can narrow it down to a range of a few minutes, they can brute-force the remaining options.

Even if you use one of the other GUID generation algorithms, that doesn't solve the problem, because the purpose of a GUID is to be globally unique, not to be unguessable.

Besides, the first eight characters of a GUID carry only 32 bits of entropy, because they come from a very limited alphabet: They can be a digit, or a letter from A to F. That's it.

If you want something cryptographically secure, then use a cryptographically-secure random number. Don't use something that "looks random to me." And use more entropy than 32 bits.

(Yes, this is basically a rehash of an earlier article, but I wanted to address directly the matter of using GUIDs as passwords.)

Raymond Chen

Follow