# When I call CryptProtectData with the same parameters, why aren't the results identical?

devblogs.microsoft.com/oldnewthing/20181008-00

October 8, 2018

Raymond Chen

If you call `CryptProtectData` twice in a row with the same parameters, you get different results. Why are the results inconsistent?

The plaintext is the same. The entropy is the same. The key is the same. Shouldn't the result be the same?

If those were the only inputs to the encryption algorithm, then the results should be the same. But they aren't the only inputs to the encryption algorithm. The `CryptProtectData` function adds in some bonus random data. This extra data is recorded in the encrypted blob so that it can also be used during decryption.

The purpose of the extra data is to prevent exactly what you're trying to do. Without the extra data, an attacker could recognize that two encrypted blobs were identical and conclude that they had the same plaintext.

For example, suppose an attacker sees that two passwords have the same encrypted blob. The attacker can try to extract the plaintext from one of the blobs by some other means. Maybe one of the blobs corresponds to a site which suffered a security breach that leaked a bunch of passwords. Or maybe the site transmits passwords unencrypted. Or perhaps the site is one the attacker is good at phishing for. However the attacker gets the plaintext for one site, it now knows the plaintext for the other site.

Adding extra random data means that multiple encryptions of the same plaintext with the same key and entropy will nevertheless produce different results. This foils attacks based on comparing encrypted results.

Raymond Chen

**Follow**