8.6.7 Nonce

A nonce is required to construct a seed during instantation. The nonce **shall** be either:

a. A random value with at least (*security_strength*/2) bits of entropy,

b. A non-random value that is expected to repeat no more often than a (*security_strength*/2)-bit random string would be expected to repeat.

The nonce is required for instantiation to provide *security_strength* bits of security for the DRBG, even when it is instantiated many times and used in a way in which a single DRBG compromise leaks some long-term secret. For example, imagine an ECDSA implementation with a 128-bit security level which instantiates its DRBG with 128 bits of entropy before each signature. After 2^{32} signatures, an attacker expects to be able to determine the private ECDSA signing key with 2^{96} work, because he can guess 2^{96} different starting values with 128 bits of entropy, and expect that one of these values instantiated one of the DRBG instances used. By instantiating the DRBG either with 128 bits of entropy and a nonce, this attack doesn't work—each guess of the 128 bits of entropy must be tried independently of all the others, and after 2^{96} guesses, the attacker has only a 2^{-32} probability of having guessed a DRBG seed.