NIST revises key computer security publication on random number generation

26 June 2015, by Chad Boutin

Credit: megainarmy/Shutterstock

In response to public concerns about cryptographic security, the National Institute of Standards and Technology (NIST) has formally revised its recommended methods for generating random numbers, a crucial element in protecting private messages and other types of electronic data. The action implements changes to the methods that were proposed by NIST last year in a draft document issued for public comment.

The updated document, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, describes algorithms that can be used to reliably generate random numbers, a key step in data encryption.

One of the most significant changes to the document is the removal of the Dual_EC_DRBG algorithm, often referred to conversationally as the "Dual Elliptic Curve random number generator." This algorithm has spawned controversy because of concerns that it might contain a weakness that attackers could exploit to predict the outcome of random number generation. NIST continues to recommend the other three algorithms that were included in the previous version of the Recommendation document, which was released in early 2012.

The revised version also contains several other notable changes. One concerns the CTR_DRBG—one of the three remaining random number algorithms—and allows additional options for its use. Another change recommends reintroducing randomness into deterministic algorithms as often as it is practical, because refreshing them provides additional protection against attack. The document also includes a link to examples that can help developers to implement the SP 800-90A random number generators correctly.

The revised publication reflects public comments received on a draft version, released late last year.

More information: Recommendation for Random Number Generation Using Deterministic Random Bit Generators (NIST Special Publication 800-90A Rev. 1) is available on NIST's website: www.nist.gov/manuscript-public … ch.cfm?pub_id=918489

Provided by National Institute of Standards and Technology