NIST removes cryptography algorithm from random number generator recommendations

April 22 2014, by Jennifer Huergo

Following a public comment period and review, the National Institute of Standards and Technology (NIST) has removed a cryptographic algorithm from its draft guidance on random number generators. Before implementing the change, NIST is requesting final public comments on the revised document, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (NIST Special Publication 800-90A, Rev. 1).

The revised document retains three of the four previously available options for generating pseudorandom bits needed to create secure cryptographic keys for encrypting data. It omits an algorithm known as Dual_EC_DRBG, or Dual Elliptic Curve Deterministic Random Bit Generator. NIST recommends that current users of Dual_EC_DRBG transition to one of the three remaining approved algorithms as quickly as possible.

In September 2013, news reports prompted public concern about the trustworthiness of Dual_EC_DRBG. As a result, NIST immediately recommended against the use of the algorithm and reissued SP 800-90A for public comment.

Some commenters expressed concerns that the algorithm contains a weakness that would allow attackers to figure out the secret cryptographic keys and defeat the protections provided by those keys. Based on its own evaluation, and in response to the lack of public confidence in the algorithm, NIST removed Dual_EC_DRBG from the

Rev. 1 document.

The revised SP 800-90A is available at csrc.nist.gov/news_events/index.html#apr21 along with instructions for submitting comments. The public comment period closes on May 23, 2014. NIST will take those comments into consideration in making any revisions to SP 800-90A.

NIST recommends that vendors currently using Dual_EC_DRBG who want to remain in compliance with federal guidance, and who have not yet made the previously recommended changes to their cryptographic modules, should select an alternative algorithm and not wait for further revision of the Rev. 1 document.

NIST advises federal agencies and other buyers of cryptographic products to ask vendors if their cryptographic modules rely on Dual_EC_DRBG, and if so, to ask their vendors to reconfigure those products to use alternative algorithms.

A list of cryptographic modules that include Dual_EC_DRBG can be found at csrc.nist.gov/groups/STM/cavp/ … ts/drbg/drbgval.html. Most of these modules implement more than one random number generator. In some cases, the Dual_EC_DRBG algorithm may be listed as included in a product, but another approved algorithm may be used by default. If a product uses Dual_EC_DRBG as the default random number generator, it may be possible to reconfigure the product to use a different default algorithm.

Draft versions of related guidance, 800-90 B: Recommendation for the Entropy Sources Used for Random Bit Generation and 800-90 C: Recommendation for Random Bit Generator (RBG) Constructions, were also released for comment in September 2013 and are still under development.

The concerns raised over the development of SP 800-90 and the inclusion of Dual_EC_DRBG prompted NIST to review its cryptographic standards development process. In February 2014, NIST released NIST IR7977: DRAFT NIST Cryptographic Standards and Guidelines Development Process for public comment. The public comment period on NIST IR 7977 closed on April 18, 2014.

NIST's primary federal advisory committee, the Visiting Committee on Advanced Technology, has also been asked to review NIST's cryptographic standards process, and the committee plans to produce a public report of its findings and recommendations.

Provided by National Institute of Standards and Technology