Dear Dr. Schneier,

In light of your November 14, 2007 Wired commentary (http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115), we would like to take the opportunity to provide a few clarifications on NIST Special Publication 800-90.

NIST would never knowingly support the inclusion of an algorithm with secret features such as a "back door" in its standards. We do not think there is an intentionally placed back door or any other secret feature in the Dual_EC_DRBG pseudorandom-number generator.

If we discovered a back door in any algorithm in a NIST standard, we would withdraw the algorithm as soon as practical. We have no evidence that someone knows the existence of the "secret numbers" that Dan Shumow and Niels Ferguson have shown would provide advance information about the pseudorandom numbers that Dual_EC_DRBG would generate. Therefore, we have no plans to withdraw the algorithm at this time.

As you note, the Dual_EC_DRBG algorithm has also been approved as an ANSI international standard. The algorithm was vetted through the ANSI X9 subcommittee, of which Neils Ferguson (one of authors of the paper that claims a back door) is a participant. As Drs. Shumow and Ferguson state in their presentation, they do not believe that NIST would have intentionally created a back door in Dual_EC_DRBG, and they state that even the algorithm's designer may not have been aware of having potentially created such a feature.

Comment [EBB1]: was

It is also worth noting that no one is required to use Dual_EC_DRBG or any other algorithm based on its appearance in NIST Special Publication 800-90. Moreover, as you point out in your column, Appendix A of SP 800-90 gives users the information that is needed to generate alternative values which should preclude any chance of the secret trap door in the scenario that Shumow and Ferguson have presented.

NIST special publications, including this one, undergo a rigorous review process, including a public comment period. We take all comments on our publications very seriously and regularly update topics in our special publications. We appreciate the opportunity to comment on this standard.

Comment [EBB2]: publication?

Sincerely,

November 28, 2007

Dear Bruce,

In your November 14, 2007 Wired commentary (http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115), you suggested that the Dual_EC_DRBG random number generator published in NIST Special Publication 800-90 has a property "that can only be described as a back door." We have no evidence that anyone has, or will ever have, the "secret numbers" for the back door that were hypothesized by mathematicians Dan Shumow and Neils Ferguson, that would provide advance information on the random numbers generated by the algorithm. For this reason, we are not withdrawing the algorithm at this time. NIST Special Publication 800-90, which includes a method for randomly generating points if there is a concern about a back door, underwent a rigorous review process that included a public comment period before it was published,. All NIST algorithms, including the Dual_EC_DRBG, undergo continual review throughout their lifetime. If successful attacks are found on an algorithm, the algorithm is withdrawn.

Sincerely,

Elaine Barker
Lead Author, NIST SP 800-90
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD