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.

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~~ a hypothetical 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.

Sincerely,

Subject: Fwd: Draft response to Bruce Schneier
Date: Monday, November 19, 2007 11:54:23 AM Eastern Standard Time
From: Curt Barker
To: ddodson@nist.gov, Burr, William E., ebarker@nist.gov
Priority: High

Need feedback ASAP.

- Curt

X-Sieve: CMU Sieve 2.3
From: "Ben Stein" <benjamin.stein@nist.gov>
To: "'Curt Barker'" <curt.barker@nist.gov>
Cc: <gail.porter@nist.gov>
Subject: Draft response to Bruce Schneier
Date: Mon, 19 Nov 2007 09:51:07 -0500
X-Mailer: Microsoft Office Outlook, Build 11.0.5510
Thread-Index: Acgqu53Rpbk0O8awR0q2JpzvdPTIMA==
X-NIST-MailScanner: Found to be clean
X-NIST-MailScanner-From: benjamin.stein@nist.gov
X-NIST-MailScanner-Information:

Dear Curt,

Gail and I have come to the conclusion that we should initiate a response to the Schneier column. I'm thinking the best thing to do is to write him a letter (rather than send a letter directly to Wired, since this piece is online and may not make it into the print issue). The draft is attached. I have not yet designated the person who would sign the letter--feel free to send me a suggestion; otherwise I can sign it. We would send a finalized response to him, and then also send it to Wired. We'd also furnish it to any reporters who ask for our response. I'd also like to send it to the publications (such as Ars Technica and the Register) that have reported on his column.

We feel some response is warranted because it's an issue of public perception, image and reputation. This column could contribute to future misperceptions about NIST. We have the opportunity to make some valid points about the algorithm and to set the record straight.

I've given my counterparts at NSA a heads-up about our plans to do a response and I will send them the final letter as a courtesy.

Let me know if this works for you. After incorporating your comments, we could send the draft to Bill Burr for his comments, and afterwards to Mat and throughout the director's office. I'd be very happy to discuss this further.

Thanks,
Ben
x3097