Comments Received on SP 800-131A

From: "McDorman, Doug" <Douglas.McDorman@t-mobile.com>
Date: July 10, 2015

Some brief comments:

COMMENT #1
In section 1.2.1, it says 112 bits of security strength is now required.

> *“For the Federal government, a minimum security strength of 112 bits is required for applying cryptographic protection (e.g., for encrypting or signing data). Note that prior to 2014, a security strength of 80 bits was* ***approved*** *for applying these protections,”*

Later it says in Table 1 that Three-key TDEA Encryption and Decryption is Acceptable.

However in SP 800-57 it essentially says three-key TDEA provides only 80 bits:

> *“However, if the attacker can obtain approximately 240 such pairs, then 2TDEA has strength comparable to an 80-bit algorithm (see [ANSX9.52], Annex B).”*

NIST Special Publication 800-57 Recommendation for Key Management — Part 1: General (Revised), March, 2007
http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

So in summary should Three-key TDEA Encryption be Disallowed and Decryption be Legacy-use?

NIST: SP 800-57, Part 1 indicates that two-key TDEA provides only 80 bits of security. However, with the additional restriction that no more than 2^{20} 64-bit blocks can be encrypted under the same key, two-key TDEA provides 100 bits of security. While this is still less than 112 bits, this exception to the 112-bit security rule was granted by NIST through the end of 2015.

Three-key TDEA is estimated to provide 112 bits of security. This is consistent with SP 800-57, Part 1. Therefore, the use of three-key TDEA of encryption continues to be Acceptable.

COMMENT #2
Section 7 Key Wrapping specifically calls out for two-key TDEA “the total number of blocks of data wrapped with the same cryptographic
key **shall not** be greater than 220” NIST: Read as 2^{20}.

Given the potential weakness with three-key TDEA and 2^40 of plain and cipher pairs should there be a similar statement:

> *“the total number of blocks of data wrapped with the same cryptographic key* ***shall not*** *be greater than 240”,*

or perhaps at least recommend not (instead of shall not) to be used for more than 2^40.

NIST: No. We consider that wrapping with three-key TDEA to provide 112 bits of security without the use restriction. The restriction only applies to two-key TDEA.

COMMENT #3
These two items say not defined but do not describe why they are not defined.
Table 10

CCM and GMAC Generation TDEA Not defined
CCM and GMAC Verification TDEA Not defined.

NIST: CCM and GMAC are specified for block ciphers with block sizes of 128 bits. See SP 800-38C and SP 800-38D. TDEA has a block size of only 64 bits. However, those entries have been removed to prevent confusion.

From: Kramer, Timothy L CIV SPAWARSYSCEN-ATLANTIC, 58820"
<tim.kramer@navy.mil>
Date: July 13, 2015

Please consider the following comments, relating to the draft SP 800-131 A-Rev.1:

- In Section 1.2.1, second paragraph on page 8: there is a disparity between the date in third sentence (i.e., "2014") and that provided by the referenced IG Section 7.5 (i.e., "2010"). Was there a separate document which extended the allowed use of 80-bits between 2011 and 2014?

NIST: IG 7.5 will be updated.

- In Appendix B, page 22: FIPS 186-2 is listed as a reference (and is used repeatedly in the draft 800-131A) but it is not available via the FIPS web site. Should all references to 186-2 be updated to reflect 186-4?

NIST: No, the references to 186-2 are valid. FIPS 186-2 is available at http://csrc.nist.gov/publications/PubsFIPSArch.html.

- In Appendix B, page 22: Date for FIPS 202 is listed as March 2014 but web page lists it as May 28, 2014. Was there an update?

NIST: Now that FIPS 202 has been completed, the reference has been corrected.

Very respectfully,
Tim Kramer

From: Manoj Maskara <mmaskara@corsec.com>
Date: Monday, July 13, 2015

Please see my 3 comments below:

1) On Page 14 of Draft SP 800-131A,

   The text towards the end of the page says: "Non-compliant DH and MQV schemes using finite fields:
   The use of these schemes is **disallowed** if |*p*| < 2048 bits or |*q*| < 224 bits.

   Through December 31, 2015, the use of these schemes is **deprecated** if |*p*| ≥ 2048 bits and |*q*| ≥ 224 bits. All of these schemes will become **disallowed** after 2017."

   The last column of Row 3 of Table 4 of this document for "Non-compliant DH and MQV schemes" using finite fields for ">=112 bits of security strength:" says "Deprecated through 2017; Disallowed after 2017" whereas, the above text in the document refers to deprecated through December 31, 2015.

   NIST: The reference to 2015 has been changed to 2017 to be consistent with the table. Thanks for catching this.

2) The above comment also applies to "Non-compliant DH and MQV schemes using elliptical curves" in Table 4 and text on Page 14.

   NIST: The reference to 2015 has been changed to 2017 to be consistent with the table. Thanks for catching this.

3) The last column of the first row in Table 9 for SHA-1 says "Disallowed, except in a TLS handshake". The use of SHA-1 in SSH is also allowed when used for server authentication provided the key size used is greater than or equal to 2048 bits. Please see below:

   Per SP800-57 Part 3 REV1, Section 10.2.1.3: *SHA-1 is no longer allowed for generating digital signatures. However, in this protocol, SHA-1 is allowed for server authentication, as long as the public key size of the signing function (either RSA or DSA) is at least 2048 bits.*

   NIST: The exception has been expanded to include SSH.

Thanks,
Manoj

From: Mark D. Baushke <mdb@juniper.net>
Date: July 18, 2015

I am pleased to respond to the National Institute of Standards and Technology (NIST) with comments on the draft NIST Special Publication 800-131A dated July 2015.

Table 9 of Draft NIST SP [800-131A_r1] lists four of the SHA-3 family of hash functions described in [FIPS 202]. However, no mention is made of the two eXtendable-Output Functions (XOFs) named SHAKE128 and SHAKE256. It is not clear to what extent they are FIPS approved, or if they should be considered as FIPS non-approved functions for now.

NIST: The XOFs have not been approved as hash functions. FIPS 202 approves them as functions whose use will be specified in future Special Publications. A note was inserted in Section 9 for clarification.

The slides on SHA-3 presented by Ray Perlner (see URL: http://csrc.nist.gov/groups/ST/hash/sha-3/Aug2014/documents/perlner_XOFs.pdf) seem to indicate that they should be a type of FIPS Approved Hash.

NIST: The slides to not claim that the XOFs are hash functions.

I understand that NIST is not able to guarantee that an XOF is able to replace existing approved hash functions, but I would very much like to see an official note in 800-131A_r1 concerning the state of these XOFs.

NIST: The XOFs will be used to construct other approved functions. Since these other functions are not publicly available even in draft form, it is premature to include them in SP 800-131A. They will be included in a future revision of SP 800-131A.

Best Regards,

Mark

Mark D. Baushke
Distinguished Engineer, Junos Security
Juniper Networks, Inc.
mdb@juniper.net
www.juniper.net
+1 408-745-2952

From: Chris Brych <chris.brych@oracle.com>
Date: Monday, July 20, 2015

After reviewing the specification internally, I noticed that we may have an issue with a short coming in one of the symmetric key establishment mechanisms that is not specifically mentioned. NIST SP 800-131A call for compliance with NIST SP 800-38F and some of its derivative authenticated encryption algorithms like NIST SP 800-38C (CCM Mode) and NIST SP 800-38D (GCM Mode) for transporting keys. The specification also allows for KDF's based on NIST SP 800-108 and authentication mechanisms specified in NIST SP 800-38B (CMAC).

What is not easily determined is if the Global Platforms Secure Channel Protocol (SCP03) is considered an allowed key establishment protocol. To me, the standard utilizes allowed algorithms like AES and 3-Key Triple-DES, allowed integrity mechanisms like CMAC, and approved pseudo random functions for deriving keys but it does not specify whether the "SCP Protocol" is "Allowed" as an approved key establishment mechanism. Clarity in the NIST SP 800-131A Standard to call out whether it is Allowed protocol or mechanism would be appreciated.

NIST: SP 800-131A does not discuss protocols per se, except for a reference to TLS and SSH as exceptions in Table 9 of Section 9.

Thank you.

Cheers,

Chris

From: "Gibbons, Lee D (Doug)" <ldgibbons@avaya.com>
Date: Wednesday, August 5, 2015 at 6:04 PM
To: cryptotransitions <cryptotransitions@nist.gov>
Subject: SP 800-131A Comments

Table 2 has added a Legacy-use section and relaxed the lower bound of the key length from 1024 to 512 bits. Though this is addressed in footnote 5, there is no mention of the relaxation in Appendix C. This change is significant as there now exist validated modules (based on the original 800-131A) which refuse to verify signatures with keys now considered acceptable for legacy use. Please add a note to Appendix C so that this change becomes obvious to implementers.

NIST: The change has been included in Appendix C.

Typos:
Section 1.1, paragraph 2: missing period at end of last sentence.
Appendix C:

3. The use of keys that provide less than 112 bits of security strength for digital signature generation ~~are~~ is no longer allowed; however, their use for digital signature verification is allowed for the verification of already-generated digital signatures.

5. The use of the RNGs specified in [FIPS 186-2], [X9.31] and [X9.62] ~~are~~ is **deprecated** until December 31, 2015, and **disallowed** thereafter.

6. The use of keys that provide less than 112 bits of security strength for key agreement ~~are~~ is now **disallowed**.

7. The use of non-approved key-agreement schemes ~~for key~~ is **deprecated** through December 31, 2017, and **disallowed** thereafter.

11. The SHA-3 family of hash functions specified in [FIPS 202] ~~have~~ has been included in Section 9 as **acceptable**.

NIST: The typos have been fixed.

From: "Harris, Michael W. (CDC/OCOO/OCIO)" <fnb0@cdc.gov>
Date: Monday, August 10, 2015
To: cryptotransitions <cryptotransitions@nist.gov>

CDC has no comments to provide on the *Draft Special Publication 800-131A Revision 1, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*.

Thank you for the opportunity to review and comment.

NIST: Thanks for your comment.

From: Stephanie Eckgren <seckgren@infogard.com>
Date: August 14, 2015

Attached please find InfoGard's comments on Draft SP 800-131A Revision 1.

Let us know if you have any questions.

Regards,
Stephanie Eckgren

InfoGard Comments on Revision of SP 800-131A

Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths

- Assuming an end of year final publication of the SP 800-131A update, 2 years for a transition is reasonable if there is some way of dealing with services that are "outward facing", i.e. not within or between federal agencies under the scope of FISMA. Currently CMVP allows non-Approved services to occur intermingled with Approved services, but this is handled in an undocumented way. CMVP and/or the CT Group should clarify how agencies acting under FISMA can legally interact with outside entities not under the FISMA scope, for example with customer facing web services that include key agreement or key transport mechanisms that are no longer allowed.

  NIST: Out-of-scope for SP 800-131A; refer to CMVP guidance. Currently, the decision is left to each Federal agency. Future CMVP guidance will provide a further clarification.

- On page 11, the footnote describing the meaning of the absolute value bars should really be in a notation section near the front of the document. This notation is used throughout the rest of the document, not just for Table 2.

  NIST: OK.

- In Section 6, the last sentence of the first paragraph makes very little sense. Possible alternate phrasing: "While there are allowed RSA-based Key Transport schemes that are not compliant with SP 800-56B, only RSA-based Key Agreement schemes compliant with SP800-56B are allowed."

  NIST: The sentence has been reworded.

- On the sunset date for non-SP800-56A compliant key agreement schemes: It's clear that the general intent here is to allow some path to compliance for certain prominent commercial protocols (such as IKE, TLS, and SSHv2) within the framework of SP800-56A, but it isn't clear that this is practical. Some of these protocols (IKE, SSHv2) use pre-established parameter sets whose associated parameter lengths are not the one established within the SP800-56A / FIPS 186-4 documents. It's important to further note that within these pre-defined groups the "large prime-ordered group" approach specified by NIST could be made to work, but the size of "q" in this case would be much larger than required by FIPS 186-4 / SP800-56A / SP 800-57 Part 1. The group parameters specified for these groups are "safe primes", such that p = 2q + 1 (so, in the notation of this draft, we then have |q| = |p|-1), and the specified generator generates this q-order group. SP800-56A is not structured to allow for this type of parameter set. Instead, these "safe primes" are *more* conservative than required by FIPS 186-4 (in particular, the security of these large-q systems does not depend on the cofactor being non-smooth!). In other cases (group exchanges in SSHv2, TLS), there is no capacity to send the additional parameter "q", so the only way these can be made to work is by restricting all servers and clients to operating with certain pre-established parameters that do follow these guidelines (as would be possible using the parameters specified in RFC 5114). This approach is not widely adopted today, and enforcing this behavior would break interoperability. Again, to emphas breaking compatibility in order to enforce a level of security that could be reasonably seen as "weaker" isn't a very good public position, particularly in the aftermath of the Dual_EC_DRBG fiasco (which we note that you address here). Long term, we suggest to either explicitly adopt the option of using "strong primes" as moduli for Diffie-Hellman exchanges (and require that the generator generate this prime-ordered group), or explicitly adopt the relevant MODP parameters specified in RFC 3526. Both of these would likely require an update to SP800-56A.

NIST: Out-of-scope for SP 800-131A; Will consider for the SP 800-56A revision, along with any other proposals.

- The CAVP test tool does not allow testing of SHA-1 even though it is allowed in some cases (i.e. in the TLS handshake).

NIST: Out-of-scope for SP 800-131A. However, the comment has been provided to the CAVP and CMVP.