PLEASE NOTE: NIST Computer Security Division has received these public comments for Draft NISTIR 7977, *NIST Cryptographic Standards and Guidelines Development Process*. These comments that were received are from the:
FIRST PUBLIC DRAFT released February 2014.

We have provided these (first public draft) comments for historical purposes.

Publication Number: **NISTIR 7977 (First Public Draft)**

Title: **NIST Cryptographic Standards and Guidelines Development Process**

Publication Date: **February 2014**

- Historical Document (First Public Draft, February 2014): NISTIR 7977 that these comments were based from (January 2015 the 2nd public draft of NISTIR 7977 was released – see link below – 2nd to last bullet): *http://csrc.nist.gov/publications/drafts/nistir-7977/nistir_7977_draft.pdf*

- Information on the NIST Solicits Comments on its Cryptographic Standards Development Process **(NISTIR 7977 First Public Draft [from the February 2014])** can be found at: http://csrc.nist.gov/groups/ST/crypto-review/process-feb2014.html

- Information on the NIST Solicits Comments on its Cryptographic Standards Development Process **(NISTIR 7977 Second Public Draft (January 2015))** can be found at http://csrc.nist.gov/groups/ST/crypto-review/process.html

- *Link to NISTIR 7977 can be found on the CSRC NISTIR webpage at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7977*

Public Comments Received on
NISTIR 7977:
NIST Cryptographic Standards and
Guidelines Development Process (Draft)

From: carlos salinas <carlosgsalinas007@yahoo.com>
Subject: Comments
Date: February 21, 2014 at 9:14:43 AM EST
To: <crypto-review@nist.gov>

I believe the standards, guidelines and procedures published by NIST have been always the "Best". I can only say that all the people involve in all the publications including this draft, deserve not only the personal recognition and appreciation but also applause for a well done written documents. NIST standards have been my personal guidance during my IA carrier with DOD and DIA. Good job.

Sincerely
Carlos G. Salinas
Carlosgsalinas007@yahoo.com

From: BLUM Jurgen <Jurgen.BLUM@kbl-bank.com>
Subject: NIST Cryptographic Standards and Guidelines Development Process: some comments
Date: March 3, 2014 at 11:19:58 AM EST
To: "'crypto-review@nist.gov'" <crypto-review@nist.gov>

Dear Sir or Madam,

I just downloaded the draft document and would like to share some of my comments with you:

General – Because the document already contains 14 pages, a table of contents may improve overview and readability
Editorial – p.2 / line 46: a new line should be added in order to make appear "Continuous Improvement" in the next line
Technical – p.8 / Appendix: initiatives around FIPS 140-2/-3 may be added here because these are very well known examples across multiple industries

Kind regards,

Jürgen BLUM
Senior Leading Expert (CISSP-ISSAP, CISM, CSSLP, CISA, Lead Auditor ISO27001, Risk Manager ISO27005, CRISC)

KBL European Private Bankers S.A.
ITS Governance, Risk & Security
43, boulevard Royal
L-2955 Luxembourg
Tel.: +352 4797 2915

From: "Harris, Michael W. (CDC/OCOO/OCIO)" <fnb0@cdc.gov>
Subject: Comments on NISTIR 7977
Date: April 2, 2014 at 3:26:16 PM EDT
To: "'crypto-review@nist.gov'" <crypto-review@nist.gov>
Cc: CDC OCOO-OCISO Data Call <OCISODataCall@cdc.gov>, "Gatland-Lightner, Cheri (CDC/OCOO/OCIO)" <clg5@cdc.gov>, "Robinson, Colleen M. (CDC/OCOO/OCIO)" <cqr3@cdc.gov>

CDC has no comments to provide on the *draft NIST Interagency Report (NISTIR) 7977, NIST Cryptographic Standards and Guidelines Development Process*.

Thank you for the opportunity to review and comment.

Michael W. Harris, CISSP, Information Technology Specialist, Office of the Chief Information Security Officer (OCISO), Centers for Disease Control and Prevention (CDC)
Office: 770.488.8052, Cell: 770.283.9589, E-mail: fnb0@cdc.gov

From: ianG <iang@iang.org>
Subject: comments on NIST IR 7977
Date: February 24, 2014 at 7:27:18 AM EST
To: <crypto-review@nist.gov>

Comments on NIST IR 7977, use at will.

38 Balance:

No mention there of economics. NIST / FIPS processes are widely seen as too expensive to justify on economic grounds, and have contributed to a state-subsidised industry delivering expensive hammers to the federal government agencies that are often incompatible with that which the commercial sector adopts.

52 NIST's statutory responsibility is to develop cryptographic standards and guidelines for
53 protecting sensitive government information on non-national security systems. These are widely
54 used across the federal government.

Good. This could be improved by explicit mention that the federal government is the primary customer, and at the end of the day, the question that NIST defers to is whether the product protects the federal government. This is the showstopper, or it should be.

The reason for this is that people assume that there is one security model, one threat model. There isn't. People assume that the standards and recommendations created for federal government are equally useful to them; they are not always so.

Federal government has to face (eg) APTs whereas commercial industry doesn't. Setting the bar high for the former results in less security for the latter, because precious resources are diverted to meet inappropriately high standards.

This process was seen with the shift to long RSA numbers for CAs. On the basis of a state-financed attack on federal agencies, a higher number is called for. Yet, for commercial industry faces no such threat, and demonstrably, 1024 is totally secure today and smaller numbers have not been troubled.

The rollover to larger numbers has diverted the attention of the industry from the real issues. In this NIST was complicit, it should have been hammering the table about the vulnerability to phishing and poor UIs than concentrating on the mathematical elegance of 2048 being demonstrably stronger than 1024.

This is an example of blind following. Many communities pass their security leadership to NIST without thought, which leads to conflicts in the process when NIST is looking one way and they are not looking at all. Hence it is very important to stress that NIST serves federal government agencies' needs, above all.

68 Standards Developing Organizations (SDOs) have also adopted NIST cryptographic standards as
69 foundational building blocks for security protocols. For example, the Advanced Encryption
70 Standard (AES) block cipher is included in ISO/IEC 18033-3:2010, is the preferred block cipher
71 for IEEE 802.11 to secure wireless networks, and is mandatory to implement in version 1.2 of
72 the IETF's Transport Layer Security (TLS) protocol.

There is only careful or vague mention here of effects outside USA. NIST is a leader in standards around the world, and what it creates is often adopted without change around the world. I think more notice needs to be made of this, although I understand that local politics will often play a part in it.

211 Announcements and public review are vital, but only the externally visible part of the process.
...
218 .... As a result, cryptographers around the world
219 often know whom to contact at NIST in their area of interest. NIST encourages and receives
220 valuable informal advice, often based on independent cryptanalysis, from researchers.

Informal channels are a way to breach transparency. Especially, informal influence can destroy an agency's independence, because those seeking to drive the standards can make all their commentary closed to the public. Those who are seeking to keep the standard open and good for all are punching blind.

There are many solutions to this, but the primary principle is that the informal channels cannot be allowed to sway the process. If there is something important, it must be revealed to cross-examination by opposing counsel (to use a metaphor).

It may be possible to develop a 'licence' that all and any comments received by any means may be posted. Attribution may be reserved, but only in public postings. Most all stated reasons to keep comments secret can be traced back to commercial or influence grounds.

END, iang.

From: Susan Landau <susan.landau@privacyink.org>
Subject: Re: comments on NIST's Draft Cryptographic Standards and Guidelines Development Process
Date: April 4, 2014 at 11:00:04 PM EDT
To: <crypto-review@nist.gov>

Dear CTG,
Thanks for the clear exposition on the process for developing cryptography standards. Although I am pleased to see this document, I have some concerns regarding the draft. I feel the current document does not adequately address the issues raised by the adoption of Dual EC-DRBG. In avoiding doing so, you are missing an opportunity to directly acknowledge the problem. Addressing these concerns explicitly is critical for reestablishing trust in NIST's cryptographic processes. I strongly urge you to directly address the issues raised by the recommendation of Dual EC-DRBG i Special Publication 800-90A.

I suggest that around lines 317-324 you delineate the fact that despite concerns raised by the Shumow-Ferguson presentation at the 2007 Crypto Rump Session, there was no clear attempt by NIST to answer these issues (ways to do so include explaining how the constants in Dual EC-DRBG were arrived at or removing Dual EC-DRBG from Special Publication 800-90A). I would then go on to explicitly state that concerns raised later — and yes, probably here you need to reference the Snowden leaks — caused NIST to advise against using Dual EC-DRBG. I strongly believe you need to be specific here: state that you missed (or ignored) the importance of the Shumow-Ferguson presentation, and thus missed the opportunity to withdraw the Dual EC-DRBG recommendation earlier — and that in doing so, you promulgated a weak algorithm.

I have two other minor comments:

Lines 64-65: What do you mean by "NIST works closely with the NSA in the development of cryptography standards."? I know that the Computer Security Act and then FISMA made requirements in using NSA's technical expertise. But I think under the circumstances, this document should be much more clear as to what is entailed in "work[ing] closely." Does this mean that NSA provides the algorithms (per DSA)? Does it mean that NSA vets the crypto algorithms (per the AES competition)? Does it mean that it promotes algorithms provided by NSA (per Dual EC-DRBG)? Clarifying this working relationship going forward would be useful in reestablishing trust in NIST's cryptographic standards process (something that is, unfortunately, badly needed).

Lines 73-77: You mention widespread adoption of the NIST standards. AES is a great example of this, and you might want to mention it here. In any case, I believe it would be useful here to note that the open process through which NIST standards are adopted is key to the international adoption. I would also add that the adoption of NIST cryptographic standards increase security.

NIST does a highly admirable job in developing cryptographic standards and security guidelines. I was very disturbed to learn of the problems with Dual EC-DRBG. This problem has unfortunately tarnished NIST's reputation as a purveyor of trusted cryptographic algorithms. I'd very much like to see the agency regain the reputation it so much deserves.

Thanks for the opportunity to present comments.

Best,

Susan
Susan Landau

author, Surveillance or Security? The Risks Posed by New Wiretapping Technologies
co-author, Privacy on the Line: The Politics of Wiretapping and Encryption

www.privacyink.org

From: IAB Chair <iab-chair@iab.org>
Subject: IAB Comments on NISTIR 7977
Date: April 7, 2014 at 12:19:04 PM EDT
To: <crypto-review@nist.gov>
Cc: IAB <iab@iab.org>

Attached.

NIST Cryptographic Standards and Development Process

In the Matter of

NISTIR 7977 (NIST Standards and Development Process)

7 April 2014
Comments of the
Internet Architecture Board
c/o Internet Society
1775 Wiehle Avenue, Suite 201
Reston, VA 20190-5108
Website: http://www.iab.org
Email: iab@iab.org

NIST Cryptographic Standards and Development Process

In these comments, the Internet Architecture Board (IAB) responds to the comment period on NISTIR 7977, making recommendations relating to the review process for cybersecurity and cryptographic standards, in order to enhance transparency and openness.

Transparency and Accountability

The IAB appreciates the opportunity to comment on NIST's principles and practices afforded by the comment period on NISTIR 7977. NIST's focus on the principle of transparency is particularly welcome in light of the IAB's previous comments on SP 800-90 and our overall desire for transparency within the development of cryptographic standards.

The IAB wishes to call out in particular NIST's ongoing commitment to publish in the Federal Register the comments received on draft FIPS, as well as the dispositions of those comments. This provides both transparency and accountability, as it allows readers to understand the relationship between the comments received and the changes made. As the IAB made clear in its previous comments, this relationship is a key part of public trust in the development process.

We urge NIST to consider extending this publication of comments and dispositions to other NIST documents, including Recommendations and other Special Publications. While final publication might also be in the Federal Register, in order to provide continuity, the same information on a searchable portion of the NIST web site would serve the same purpose, as well as provide additional benefits. A searchable list of comments would enable NIST to provide a reply comment facility, something which is not possible with the current publication method. As noted in its previous comments, the IAB believes that a reply comment period and facility would improve not only transparency but the standards themselves, as it would give the research community and other interested technical individuals the opportunity to address issues which may have been raised to NIST.

The IAB also wishes to commend NIST on the work it does on early public outreach and for its involvement in cryptographic research. We note, however, that this involvement is necessarily limited by time and budget. Given those limitations, the IAB believes that it is vital to have the output of those outreach efforts brought into the externally visible part of the process. The externally visible process is where the broader community evaluates the developed standards, and that community needs to understand the impact of early review in order to comment and contribute further. In this light, we would like to re-iterate our previous recommendation that NIST provide a detailed and substantial explanation of changes resulting from internal review (even in cases where public comment was not initiated). This ensures that community evaluation proceeds from a more complete understanding of the inputs into the process.

In closing, thanks again for the opportunity to provide comments on the guidelines for the NIST Standards development process.

From: GTW <gtw@gtwassociates.com>
Subject: GTW Associates comments on DRAFT standards development procedures
Date: April 11, 2014 at 2:59:04 PM EDT
To: <crypto-review@nist.gov>
Reply-To: GTW <gtw@gtwassociates.com>

Please find attached GTW Associates comments on ***DRAFT NIST Cryptographic Standards and Guidelines Development Process***

George T. Willingmyre, P.E.
President GTW Associates
1012 Parrs Ridge Drive
Spencerville MD 20868

Attachment follows

Comments of GTW Associates on

DRAFT NIST Cryptographic Standards and Guidelines Development Process

Reference text:

51 NIST's statutory responsibility is to develop cryptographic standards and guidelines for
52 protecting sensitive government information on non-national security systems. These are widely
53 used across the federal government

Comment: provide a link or reference to the cited statutory responsibility

Reference text:

132 Development of New Standards

133 When NIST identifies a requirement for a standard and determines that no suitable standard
134 already exists, NIST often develops a guidance document for use by Federal agencies.

Comment: The term "guidance document" line 134 is not consistent with the Title of the section line 132 "Development of New Standards." "Guidance" has one connotation and meaning and "Standard" has a different connotation and meaning. Perhaps the intention is to convey that NIST often develops documents which may be in the form of either "Guidance" or "standard" As text later makes clear the process described certainly produces documents with the term "standard" in its title. Take care to distinguish what will be the final work product of the development process.
Reference text:
125 The principles used to develop voluntary consensus standards within SDOs are outlined in OMB
126 Circular A-119, which instructs agencies to consider the use of these standards except where
127 inconsistent with law or otherwise impractical.

The references to OMB Circular A-119 should include its title "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities" including the subsections *Guidance on use of standards and participation in standards development* The policies in the Circular are intended to maximize the reliance by agencies on voluntary consensus standards and reduce to a minimum agency reliance on standards other than voluntary consensus standards, including reliance on government-unique standards. It would be helpful to provide a link to the current and proposed revision of the Circular

Question asked: "Are there other principles that we should use to drive our standards development efforts?"

Yes

1) The WTO Technical Barriers to Trade Annex 3: Code of good practice for the preparation, adoption and application of standards http://www.wto.org/english/res_e/booksp_e/analytic_index_e/tbt_02_e.htm#ann_3 might apply. Arguably and depending upon the nature of the standards produced and whether the NIST activity could be defined as one of perhaps several central government standardizing bodies, compliance with the Code of Good practice may be an obligation according to Article 4: Preparation, Adoption and Application of Standards of the TBT http://www.wto.org/english/res_e/booksp_e/analytic_index_e/tbt_01_e.htm#article4 .

   4.1 Members shall ensure that their central government standardizing bodies accept and comply with the Code of Good Practice for the Preparation, Adoption and Application of Standards

   In any event the principles in Annex 3 are worthy of consideration

2) Annex B. Decision Of The Committee On Principles For The Development Of International Standards, Guides And Recommendations With Relation To Articles 2, 5 And Annex 3 Of The Agreement found in DECISIONS and recommendations ADOPTED BY THE WTO COMMITTEE on Technical Barriers to trade SINCE 1 JANUARY 1995 at http://docsonline.wto.org/imrd/directdoc.asp?DDFDocuments/t/G/TBT/1R10.doc also contain worthy principles potentially applicable to the NIST standards process

From: "D. J. Bernstein" <djb@cr.yp.to>
Subject: Comments on nistir_7977_draft.pdf
Date: April 11, 2014 at 5:07:32 PM EDT
To: <crypto-review@nist.gov>

Dear Sirs,

Two independent public studies in early 2006, one by Gjøsteen and one by Schoenmakers and Sidorenko, showed clearly and indisputably that NIST's proposed Dual EC PRNG flunked the well-established definition of PRNG security. (I'm writing "NIST's" because, at the time, NIST was failing to properly attribute Dual EC to NSA.)

Did NIST drop this cryptographically unsound PRNG? No. NIST went ahead and standardized it.

Shumow and Ferguson in 2007 demonstrated that whoever had generated the Dual EC constants could easily have put a back door into Dual EC. Schneier wrote an essay saying that "both NIST and the NSA have some explaining to do" and recommending "not to use Dual_EC_DRBG under any circumstances." The consensus of the public cryptographic community was the Dual EC was dead and buried, never to be seen again.

Did NIST withdraw the standard? No. NIST continued to maintain and promote the standard. NIST issued 73 validation certificates for Dual EC implementations between July 2008 and March 2014.

News reports in September 2013 indicated that Dual EC did in fact contain a back door generated by NSA. Presumably this back door, a 78-digit secret number, is also known to many other organizations that have penetrated NSA's internal security. AP reported in June 2013 that half a million contractors have Top Secret clearance; other reports show that NSA makes heavy use of off-the-shelf hardware and software; I could keep listing reasons to question how well NSA keeps secrets, but I don't think that this is a matter of dispute.

Finally NIST took steps to withdraw the standard. NIST's "Cryptographic Standards and Guidelines Development Process" draft now acknowledges "security concerns" in the standard. But the big problem here is not the lack of security in this particular standard; the big problem here is the lack of attention to security in NIST's standardization process.

Does the draft acknowledge that NIST's standardization process is vulnerable to sabotage? Does the draft propose mechanisms that would protect the process against sabotage? No, and no. Instead the draft tries to convince the reader that NIST develops "the most secure and trusted cryptographic standards" and that these standards provide "high-quality, cost-effective security mechanisms."

Dual EC is not the only troublesome example of a NIST cryptographic standard. The DES key size was widely criticized from the outset, for example, but NIST continued to promote DES for two decades, making the inevitable upgrade vastly more expensive than it should have been. As

another example, DSA was widely criticized for many more reasons, is still promoted by NIST, and is responsible for a seemingly neverending series of security problems in deployed systems. The complete failure of ECDSA signature security in the PlayStation 3 was caused by exactly the DSA/ECDSA misfeature that two decades earlier Rivest had objected to as giving the "poor user ... enough rope with which to hang himself---something a standard should not do."

Does the draft acknowledge that for many years NIST was ignoring security feedback from the cryptographic community? Does the draft propose mechanisms to prevent NIST from promoting insecure cryptographic standards? No, and again no.

Even worse, in the past decade NIST has been rushing so many cryptographic standards out the door that the quality of review has obviously been compromised. Putting together one good standard, SHA-3, involved 200 cryptographers around the world and took years of sustained public effort, but during the same period NIST also published FIPS 186-3 (signatures), FIPS 198-1 (message authentication), SP 800-38E (disk encryption), SP 800-38F (key wrapping), SP 800-56C (key derivation), SP 800-57 (key management), SP 800-67 (block encryption), SP 800-108 (key derivation), SP 800-131A (key lengths), SP 800-133 (key generation), and SP 800-152 (key management), not to mention related protocol documents such as SP 800-81r1. Why should these NIST publications be trusted? Who has actually reviewed the security of these cryptographic mechanisms, and how comprehensive was the review?

I don't mean to suggest that public review during this period was focused entirely on SHA-3. For example, the cryptographic community caught a severe security flaw in EAX Prime, and a less severe but still troublesome flaw in the security "proofs" for GCM. One can view EAX Prime as a success story, where the flaw was caught early enough to stop NIST's standardization process. However, GCM is a failure story, where NIST standardization came years before the flaw was discovered. Is this because the discovery of the GCM flaw had been waiting for some critical scientific advance? No. It is because NIST keeps biting off more than it can chew, churning out so many proposed cryptographic standards that the time required for proper security review simply does not exist.

Let me now comment on some of the things that the draft does say.

The draft claims that, to be "widely adopted," standards must "be robust and have the confidence of the cryptographic community." The unfortunate reality is that NIST standardization has, time and time again, prompted wide adoption of algorithms that were not actually robust and that had received serious objections from the cryptographic community, such as DES and DSA. NIST standardization misled the implementors and users into thinking that these algorithms were particularly safe. The cryptographic community does have confidence in AES and SHA-3, thanks to the focused competitions that produced those standards, but very few of NIST's standards are produced by such competitions.

The draft lists "Transparency" as the first principle guiding NIST's standardization processes, but later states that NIST is "statutorily required to consult with the NSA on standards." Is there any statutory requirement for NIST to take _secret_ input from NSA? NIST might be able to regain some public trust by adopting a policy of recording and immediately publishing all

communication between NIST and NSA. This would not stop NSA from paying third parties to pass messages to NIST, but NIST could issue regulations requiring financial disclosures, and in any case the basic policy would be a useful first step towards true transparency.

The draft also states "Continuous improvement" as a guiding principle, claiming that "the cryptographic community is encouraged to identify weaknesses, vulnerabilities, or other deficiencies in cryptographic functions specified in NIST publications." But actions speak louder than words. After NIST ignored serious objections to DES, ignored serious objections to DSA, and ignored serious objections to Dual EC, why should cryptographers believe that NIST is actually interested in feedback? If NIST's procedures have changed recently, why doesn't the draft say so?

I'm also troubled by security feedback being labeled as a reason for "improvement." Given the reckless pace at which NIST has been publishing cryptographic standards, it's hardly a surprise that those standards have "weaknesses" and need "improvement." How can NIST believe that this innocent-until-proven-guilty approach to cryptographic standardization is producing "the most secure and trusted cryptographic standards"? NIST should delay standardization to wait for clear evidence of adequate public review, and should abort standardization if the public review does not produce a solid consensus on security.

When I heard about this draft I assumed that NIST had engaged in (1) an honest retrospective review of known security flaws in NIST standards and (2) an honest analysis of ways in which those flaws could have been avoided by modifications in NIST's standardization process. The current draft is, unfortunately, very far from this, and as a result is very difficult to take seriously.

---D. J. Bernstein
Research Professor, Computer Science, University of Illinois at Chicago
Professor, Mathematics and Computer Science, Technische Universiteit Eindhoven

From: Debbie Planet <deb1578q@yahoo.com>
Subject: RE: NIST IR 7977
Date: April 16, 2014 at 2:18:19 PM EDT
To: "crypto-review@nist.gov" <crypto-review@nist.gov>
Reply-To: Debbie Planet <deb1578q@yahoo.com>

Are there other principles that we should use to drive our standards?

1) Incorporate concepts of provable security (i.e. adversarial models, security games, and security proofs) into FIPS 140, games, and security proofs) into FIPS 140, FIPS 199, and SP800-53.

a) Standardization of provable security will lead to better implementations and higher levels of assurance in cryptography.

b) Revisions and updates to provable security standards will accommodate for an ever changing technological environment (e.g. C90, C99, C11, C14, etc.).

c) Fostering the development of provable security standards through development conferences, (e.g. Google summer 06 Code), grants will further NIST's principle of producing the strongest, most effective and most highly trusted cryptographic standard (plus enriched development and academic communities).

2) invest or find investment in the CM.VP. The backlog is a hindrance to the means of practical cryptography in today's age of technology where hardware development cycles for mass produced devices in within 2 years.

3) Deprecate older cryptographic standards faster. What are the most effective processes identified in the draft for engaging the cryptographic community for providing the necessary inclusivity and transparency to develop strong, trustworthy standard? Are there other processes we should consider?

1) FISMA 2002 is problematic for developing trustworthy standards and the trustworthiness of NIST CSRC. Edward Snowden revealed the efforts made by the NSA to subvert implementations of cryptography. FISMA 2002 required NIST to consult the NSA on cryptographic standards. This is a conflict of interest to NIST,s principles of trustworthy standards and raises doubt of their strength. The most effective process to receive full support and faith from the cryptographic community is to address the conflict of interest in congressional hearings and remove the NSA from the consultancy process. With legislation that strikes out the verbiage of the NSA consultancy requirement in FISMA 2002 and any other relevant legislation. In a addition to this, have the legislation prevent the NSA or other departments from issuing gag orders on the development of cryptographic standards (including gag orders from the past, present, and /or future). There is no point for the cryptogrphic community to participate in a

standards development process that is half baked when it could do so in the process that is not half baked.

2) Have a stack overflow like forum for cryptography development

Sincerely,

Nikolas Bourbaki

From: Thomas Hales <hales@pitt.edu>
Subject: Public comments on NIST Cryptographic Standards and Guidelines Development Process
Date: April 17, 2014 at 4:40:53 PM EDT
To: <crypto-review@nist.gov>

Dear NIST Cryptographic Technology Group,

I am writing to suggest the increase use of formal methods in the development of cryptographic standards. (By way of introduction, I am a mathematician at the University of Pittsburgh, who has received various national and international awards for work on complex computer-assisted mathematical proofs.)

I have attached an analysis I made of the level of mathematical rigor in NIST 800-90A algorithms for random bit generators. In that analysis, I point out that "one of the most effective ways to subvert a cryptographic standard is to muddle the math." As a mathematician who has worked for over a decade in the area of formal mathematics, I find the level of mathematical rigor in the NIST standard quite appalling.

Researchers in formal proofs have successfully completed numerous projects that are more difficult than the formal verification of cryptographic standards. In particular, I mention Xavier Leroy's group (compcert.inria.fr). They have made a full formal verification of a C compiler.

Ultimately, nothing but formal methods can avert future disasters in cryptographic standards and their implementations in code. Traditional forms of peer review of standards are simply inadequate for a task as important as the verification of major cryptographic standards.

Best,
Thomas Hales
Mellon Professor
Mathematics
University of Pittsburgh.

Attachment follows.

Jigger Wit

Formalizing NIST standards

NOVEMBER 4, 2013 | THALES | 3 COMMENTS

Thomas C. Hales
University of Pittsburgh

Based on Snowden documents, the New York Times reported (http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html) that the NSA worked to subvert NIST cryptographic standards. This article discusses general weaknesses in the NIST standard 800-90A for pseudo-random number generation. Among other defects, this NIST standard is deficient because of a pervasive sloppiness in the use of mathematics. This, in turn, prevents serious mathematical analysis of the standard and promotes careless implementation in code. We propose formal verification methods as a remedy.

Levels of Mathematical Rigor

We may categorize mathematical argument as informal, rigorous, or formal.

Informal mathematics is the vulgar product of the popular press. Informally, a function is continuous if it can be sketched without lifting a pencil from a sheet of paper; chaos is the unpredictable effect of a butterfly flapping its wings in Brazil; and a pseudo-random number is one that is paradoxically deterministic yet effectively random. Informal mathematics is not wrong so much as it is unsuitable for careful science and engineering.

A more rigorous approach to mathematics became necessary in the final decades of the nineteenth century to resolve paradoxes in Cantor's set theory and other troubles. For example, disputes about continuity were resolved by clarifying definitions, eventually refining a single

intuitive notion of continuity into a family of related notions: continuity, uniform continuity, and so forth. Most professional mathematical publications now adhere to widely accepted standards of mathematical rigor, enforced through the diligence of human referees.

Formal mathematics (www.ams.org/notices/200811/tx081101370p.pdf) is yet a higher standard. English and other natural languages are abandoned and replaced with languages whose syntax and semantics are designed with mathematical precision. The system specifies every admissible rule of logic and every mathematical axiom. Quality is enforced by a computer, which exhaustively checks every logical step of a proof.

Formal verification becomes appropriate in proofs whose complexity surpasses the capabilities of checking by hand. (A wiki page catalogues (http://en.wikipedia.org/wiki/Longest_proof) numerous long mathematical theorems that might benefit from formalization.) Formal methods are well-suited for many computer-assisted mathematical proofs. In fact, at the formal level the line is erased between algorithms implemented as computer code and mathematical reasoning. A single software system handles the formal verification of both.

Formal methods have been under development for decades, and in recent years the verification of complex software systems, hardware, and intricate theorems has become a reality. Already in 1989, it was possible to formally specify and verify a simple computer system from high-level language to microprocessor. As recent examples, we mention the full verification of a C compiler (http://compcert.inria.fr/) and complex mathematical theorems such as the Feit-Thompson theorem and the Four-Color theorem.

Formal Verification in Cryptography

Formal verification of computer code can be advised when human life or large economic interests are at stake: aircraft control systems, widely adopted cryptographic standards, or nuclear reactor controllers. Formal verification reduces the software defect rate to a level that is scarcely attainable by other means.

For several reasons, cryptography calls out for formal verification. The field is highly mathematical. Many key algorithms can be implemented as small blocks of code. A tiny defect can potentially defeat the entire algorithm. Adversaries actively seek out bugs to exploit. Cryptography safeguards large financial interests and fundamental human freedoms.

Various formal tools have been constructed (http://www.di.ens.fr/~blanchet/MPRI/2011-12/poly-mpri-2-30-draft.pdf) especially for application to cryptography. The pi-calculus has been adapted to cryptographic protocols. Projects in the Isabelle proof assistant include protocol verification through inductive definitions (http://www.cl.cam.ac.uk/~lp15/papers/Auth/index.html) and game analysis (http://scidok.sulb.uni-saarland.de/volltexte/2013/5469/pdf/thesis_berg.pdf). In the Coq proof assistant, there have been successful formal verifications of cryptographic primitives

(http://arxiv.org/pdf/0904.1110.pdf) and code-based cryptographic proofs (http://www-sop.inria.fr/everest/Benjamin.Gregoire/Cours/popl09.pdf). Significantly, formal methods have started to enter the standardization process (http://www.dtic.mil/dtic/tr/fulltext/u2/a465281.pdf).

The working group on the *Theoretical Foundations of Security Analysis and Design* (http://www.dsi.unive.it/IFIPWG1_7/) and the Computer Security Foundations Symposium of the IEEE (http://www.ieee-security.org/CSFWweb/) (CSF 2013) (http://csf2013.seas.harvard.edu/index.html) promote formal methods in cryptography.

In truth, our imperfect knowledge prevents the comprehensive verification of cryptographic systems. We are stymied by notorious problems like P versus NP and the existence of one-way functions. We lack definitive lower bounds on the computational complexity of concrete problems such as factoring of integers. Research into security reductions is ongoing. There is no comprehensive security model. For example, the Dolev-Yao model works at a high level of abstraction, assuming that cryptographic primitives function perfectly, while other models operate at various levels of detail.

Nevertheless, we can work with these limitations, implementing a collection of interrelated formal proofs grounded in current technological capabilities, and move forward from there.

The informality of NIST standards

Earlier critiques (http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html) of the NIST standard 800-90A for pseudo-random number generation have focused on specific defects (http://eprint.iacr.org/2006/190). Here, we argue that mathematical weaknesses run throughout the standard. Amid the accusations that the NSA has undermined NIST cryptographic standards, we remind NIST that one of the most effective ways to subvert a cryptographic standard is to muddle the math.

The first requirement of a standard is to set the tone and level of discourse that reflects the current technological capabilities of the matter at hand. By choosing to present an informal standard, avoiding both rigor and formal mathematics, NIST has produced a standard that is out of step with the technology of the time.

Some definitions in the NIST standard are merely informal. For example, the NIST standard defines[1] pseudo-randomness as "deterministic yet also effectively random" (NIST 800-90A, p.7). A mathematically rigorous definition of pseudo-random generators requires much more care, referencing rigorous notions of measure, probability, and complexity theory. Properly formulated definitions are given in Luby, Yao, Blum and Micali. As it is manifestly impossible to base rigorous or formal mathematical proofs on something so vague as "deterministic yet effectively random," the early pages of the NIST standard effectively ward off careful mathematical analysis.

The lack of rigor continues throughout the document. Algorithms are described with English-text pseudo-code. With more care, NIST might have provided a formal specification and a reference implementation in executable code in a language with precise semantics. Overall, the standard gives few mathematical arguments, and these do not inspire confidence. The document slips into convenient inaccuracies: heuristics rather than proofs, fixed-point arithmetic, and Shannon entropy rather than min-entropy. (See NIST 800-90A, Appendix C.2.) In fact, the standard is imprecise to such a degree that competing definitions of entropy are largely irrelevant.

An example of NIST reasoning

This section goes into detail about a particular mathematical argument that appears in the NIST standard.[2] For our purposes, the topic of discussion matters less than the nature of the NIST committee's mathematical thought. Do they reason as a mathematician in an unbroken chain of logic, or is the committee satisfied by a lesser standard?

The context is the following. Let E be an elliptic curve defined over a finite field $\boldsymbol{F}_p$, defined in affine coordinates by a polynomial equation $y^2 = f(x)$. The pseudo-random generator extracts bits from the x coordinates of a sequence of points $P_1, P_2, \ldots$ on the elliptic curve. The construction of the sequence of points does not concern us here. The issue is this: if points are sampled uniformly at random from $E(\boldsymbol{F}_p)$, then their x coordinates are not uniformly distributed in the finite field; in fact, the x coordinates obviously belong to the subset of the finite field on which $f(x)$ is a square. Research estimates are needed to determine how big an issue this is. Aggressive truncation of bits from the binary representation of x might improve pseudo-randomness but would make the algorithm less efficient.[3]

NIST quotes the research of El Mahassni and Shparlinski as "an additional reason that argues against increasing truncation." There are numerous gaps in NIST reasoning.

- A bound on discrepancy is not the same as uniform distribution.
- Uniform distribution is not the same as cryptographically secure pseudo-randomness.
- The sets $\{P_i\}$ of points used in real-world implementations have cardinalities far too small to be relevant to the given asymptotic estimates.
- The research does not support the specific NIST rule that "the recommended number of bits discarded from each x-coordinate will be 16 or 17" and does not convincingly "argue against increasing truncation."

Nevertheless, NIST uses the research to make the inflated claim that "certain guarantees can be made about the uniform distribution of the resulting truncated quantities" (NIST 800-90A). This is proof by intimidation.

Assurances

The NIST standard 800-90A states that "a user of a DRBG for cryptographic purposes requires assurance that the generator actually produces (pseudo) random and unpredictable bits. The user needs assurance that the design of the generator, its implementation and its use to support cryptographic services are adequate to protect the user's information" (NIST 800-90A). We agree.

What assurances does NIST actually provide about the generator? The document contains no mathematical proofs of pseudo-randomness and no supporting citations. Indeed, careful proofs would be impossible, because as we have noted, definitions are more informal than rigorous. Instead, the user of the standard must rely on NIST's authoritative claim that "the design of each DRBG mechanism in this Recommendation has received an evaluation of its security properties prior to its selection for inclusion in this Recommendation." That one sentence is the extent of NIST assurance of design. That's it! It seems that for NIST, assurance means to comfort with soothing words. To a mathematician, this attitude is exasperating. There is no mathematical statement of what those security properties are, and no discussion of the methods that were used to reach the conclusion. We are not told who made the evaluation or what the results of the evaluation were.

Based on the *Memorandum of Understanding* between NIST and NSA from 1989, quoted in Schneier (p. 601) (https://www.schneier.com/book-applied.html), we might wonder whether NIST's part in the evaluation was limited. According to the memo, "The NIST will … recognize the NSA-certified rating of evaluated trusted systems under the Trusted Computer Security Evaluation Criteria Program *without requiring additional evaluation*" (emphasis added).

Here is the NIST assurance of *HMAC_DRBG* (deterministic random bit generation based on hash message authentication codes). It states, "In general, even relatively weak hash functions seem to be quite strong when used in the HMAC construction. On the other hand, there is not a reduction proof from the hash function's collision resistance properties to the security of the DRBG" (NIST 800-90A Appendix E.2). Note the informal tone of the discussion, the reassurance that a weakness is strength, the brevity, and absence of mathematical theorems.

Cryptographic standards derive their security through the underlying mathematics. We can place our trust in mathematics but not in assurances such as these.

Conclusions

According to NIST aspirations (http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf), "NIST works to

publish the strongest cryptographic standards possible." Our analysis shows that judged by professional mathematical standards, NIST is very far from its goal. Indeed, the current NIST standard was written in a pre-Snowden era of unverified assurances.

NIST sets the standard both by its choice of algorithms and by its attitude towards rigor. Overall, its general careless tone will facilitate vulnerable implementations of the standard.

Better approaches to standardization are available. In fact, a number of formal verification projects have been completed (such as a formal verification of a C compiler mentioned above) that dwarf what we specifically ask NIST to do. Please adopt verification technologies in widespread use! Improvement in the formal specification of NIST standards is the first critical step in a larger process of formal verification along the entire chain, including the underlying mathematical concepts, cryptographic primitives, protocols and algorithms, and end implementations in computer code.

End Notes

1. [Here is the full definition from NIST: "A process (or data produced by a process) is said to be pseudorandom when the outcome is deterministic, yet also effectively random, as long as the internal action of the process is hidden from observation. For cryptographic purposes, `effectively' means `within the limits of intended cryptographic strength.'" Speaking of the data, we may ask with Knuth, "is 2 a random number?"] (return to text)
2. [We pick the most extensive mathematical argument in the document. It is telling that this argument is used to justify weakening the standard for the sake of efficiency.] (return to text)
3. [In light of the much discussed back door to the elliptic curve algorithm, NSA had a secret interest in persuading users not to discard many bits from x; aggressive truncation would make the back door more difficult to use.] (return to text)

References

M. Abadi and C. Fournet, *Mobile values, new names, and secure communication*, In POPL '01: Proceedings of the 28th ACM SIGPLAN-SIGACT symposium on the principles of programming languages (2001), 104–115.

M. Abadi and A. D. Gordon, *A calculus for cryptographic protocols: The spi calculus*, Information and Communication **148** (January 1999), 1–70.

NIST 800-90A, (http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf) E. Barker and J. Kelsey, *Recommendation for random number generation using deterministic random bit generators*, NIST Special Publication 800-90A (2012).

W. R. Bevier, W. A. Hunt Jr., J Strother Moore, and W. D. Young, *An approach to systems verification*, Journal of Automated Reasoning **5** (1989), 411–428 and 422–423.

M. Blum and S. Micali, *How to generate cryptographically strong sequences of pseudo-random bits*, SIAM Journal on Computing **13** (1984), 850–864.

D. Dolev and A. C. Yao, *On the security of public-key protocols*, IEEE Transaction on Information Theory **2** (March 1983), 198–208.

M. Drmota and R. F. Tichy, *Sequences, discrepancies and applications*, Lecture Notes in Mathematics, Springer, 1997.

G. Gonthier et al. (http://hal.inria.fr/docs/00/81/66/99/PDF/main.pdf), *A machine-checked proof of the odd order theorem*, Lecture Notes in Computer Science **7998** (2013), 163–179.

G. Gonthier, *Formal proof — the four colour theorem*, Notices of the AMS **55** (December 2008), no. 11, 1382–1393.

J. Harrison (http://www.cl.cam.ac.uk/~jrh13/slides/lics-22jun03.pdf), *Formal verification at Intel, Proceedings. 18th Annual IEEE Symposium on Logic in Computer Science (2003), 45–54.*

M. Luby, *Pseudorandomness and cryptographic applications*, Princeton University Press, 1996.

E. El Mahassni and I. Shparlinski (http://web.science.mq.edu.au/~igor/EC-PRNG.ps), *On the uniformity of distribution of congruential generators over elliptic curves*, Discrete Mathematics and Theoretical Computer Science (2002), 257–264, Sequences and their Applications.

R. Milner, *Communicating and mobile systems: the pi-calculus*, Cambridge University Press, 1999.

A. Yao, *Theory and applications of trapdoor functions*, FOCS (1982), 384–400.

3 thoughts on “Formalizing NIST standards”

1. Pingback: Trust the math? An Update | Not Even Wrong

2. **BEN LUND** *says:*
   Hi Prof. Hales,

I noticed another problem with the argument you criticize in "An example of NIST reasoning."

Even if it is true that a sufficiently large interval contains approximately the expected number of x-coordinates of points on the elliptic curve (as you point out, NIST's argument does not show this), the conclusion that would follow from NIST's argument is essentially the opposite of what they claim.

In particular, the set of elements of F_p that have a fixed s low-order bits is an arithmetic progression of size approximately 2^{log(p) – s}. Hence, if there are approximately the expected number of x-coordinates in each sufficiently large interval, then we get a guarantee that approximately the same number of points on the elliptic curve correspond to each possible s-bit output, provided that s is sufficiently small. I have written up a more detailed explanation of the problem on my blog (http://bendlund.wordpress.com/2013/12/23/nists-truncation-argument/).

DECEMBER 23, 2013 AT 9:42 PM | REPLY

3. Pingback: NIST's truncation argument | Ben Lund's Blog

From: tom watt <tomdwatt@yahoo.com>
Subject: Viloations of our Rights!
Date: April 18, 2014 at 2:45:11 PM EDT
To: <crypto-review@nist.gov>

No knock entry of our backdoors.

From: tom watt <tomdwatt@yahoo.com>
Subject: Violations. They hurt.
Date: April 18, 2014 at 2:49:53 PM EDT
To: <crypto-review@nist.gov>

No knock entry of our backdoors.

From: Joseph Lorenzo Hall <joe@cdt.org>
Subject: CDT's comments on NIST-IR 7977
Date: April 18, 2014 at 3:04:49 PM EDT
To: <crypto-review@nist.gov>
Cc: Runa Sandvik <runa@cdt.org>

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

To Whom It May Concern:

Please find attached a PDF of the Center for Democracy & Technology's comments on NIST Interagency Report 7977. Please do not hesitate to contact us with questions or requests that we might be able to assist with.

Sincerely,

Joseph Hall

- --
Joseph Lorenzo Hall
Chief Technologist
Center for Democracy & Technology
1634 I ST NW STE 1100
Washington DC 20006-4011
(p) 202-407-8825
(f) 202-637-0968
joe@cdt.org
PGP: https://josephhall.org/gpg-key

Attachment follows.

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMENTS ON: DRAFT NIST INTERAGENCY REPORT 7977, CRYPTOGRAPHIC STANDARDS AND GUIDELINES DEVELOPMENT PROCESS

18 April 2014

The Center for Democracy & Technology (CDT) is pleased submit these comments to the National Institute of Standards and Technology (NIST) on NIST Interagency Report 7977, "NIST Cryptographic Standards and Guidelines Development Process."[1]

NIST has long been recognized as a forum for unbiased technical research, analysis, and standards development. Cryptographic technologies are a critical technology component that supports assurance and trustworthiness in computing and networking environments. As such, these components are a particularly important aspect of the work of NIST's Computer Science Division.

Given the prominent role NIST cryptographic standards play in computing and networking contexts, it is crucial that NIST remain demonstrably free from bias or undue influence. NIST cryptographic standards are widely adopted, placing considerable pressure on NIST to be systematic, open, transparent, committed to well-defined principles and processes, and to be responsive to global concerns. We are pleased that NIST recognizes this and has initiated a review of its cryptographic standards, starting with NIST-IR 7977.[2]

Our comments begin with general comments on NIST-IR 7977. We then discuss the principles listed in the document as well as additional principles. Lastly, we consider mechanisms and outreach that we believe will further these principles.

I. General Comments

The document's title and abstract should make it clear that the document is a high level statement of the principles and procedures that NIST follows in the development of cryptologic standards and guidelines. A more descriptive title would be "The NIST Cryptographic Standards and Guidelines Development Process: Overview of Principles and Procedures."

---

[1] "NIST Cryptographic Standards and Guidelines Development Process," National Institute of Standards and Technology, NIST-IR 7977, (February 2014), *available at:* http://csrc.nist.gov/publications/drafts/nistir-7977/nistir_7977_draft.pdf.

[2] "Cryptographic Standards Development Process Review," National Institute of Standards and Technology, Computer Security Division, Cryptographic Technology Group, *available at:* http://csrc.nist.gov/groups/ST/crypto-review/index.html (accessed on 17 April 2014).

We were expecting to see much more detail on how NIST makes decisions when faced with competing proposals, configuration choices, and other trade-offs. While principles are by definition somewhat abstract, processes, procedures, and mechanisms should be well documented with clear rationales explaining how they each support the principles. The description in the appendix to NIST-IR 7977 of evaluation criteria for proposed block cipher modes is exactly the kind of evaluation specification we expected to see documented throughout the document, not just in the appendix. In order to adequately describe how NIST makes decisions, each genre of cryptographic primitive or cipher mode included in NIST Federal Information Processing Standards (FIPS) or Special Publications (SP) must have clear sets of evaluation criteria that support the overarching principles.

Finally, for each FIPS and SP we would like to see documented in those publications the efforts that NIST has engaged in to enfranchise the stakeholder community, from talks, to events, to smaller outreach efforts. To the extent that engagement is important for a sound standards process, that engagement should be documented in the standard.

II. Cryptographic Standardization Principles

The principles listed in NIST-IR 7977 are a great start, but we feel there are some missing – due process and avoiding undue influence — and that a few others – technical merit and integrity – could be refined.

A. Due Process

One principle that is not explicitly stated, but should be, is that of due process.[3] Due process requires fair treatment to all stakeholders throughout the standards process, ensuring there are adequate opportunities for stakeholders to object to or amend certain decisions and that no stakeholder or set of stakeholders are disadvantaged or privileged throughout the process. For example, NIST often works privately with the authors of a mode proposal or the winner of an algorithm design competition to further refine the proposal before committing it to a written FIPS or SP document. However, as this refinement occurs in private, there are other important interests that may be neglected, including those of the authors of competing proposals that may have had their proposals or designs rejected and may have technical objections or enhancements to these post-selection changes that should be heard before a draft goes out for public comment. Any changes to proposed algorithms or standard parameters should be fair and transparent, with check-ins with the larger community and clear, documented rationale for the changes grounded in technical merit. The recent case of SHA-3's post-competition standardization is an example of changes to algorithm parameters that proved problematic to a number of people in the cryptographic community.[4] NIST should examine past comments about the standards process and decide if there are certain operating procedures that could be adopted to reduce shortcomings of due process.

[3] The principle of due process should be stated on its own in this document as it only fits partially under a number of the principles already identified in the document, including integrity, balance, and transparency.

[4] Joseph Lorenzo Hall, "What the heck is going on with NIST's cryptographic standard, SHA-3?," Center for Democracy & Technology (September 24, 3012), *available at:* https://cdt.org/what-the-heck-is-going-on-with-nist%E2%80%99s-cryptographic-standard-sha-3/.

B. Avoiding Undue Influence

A key part of integrity is avoiding undue influence, which has the potential to undermine each of the other principles stated in this document. NIST should acknowledge that improper influence is a threat to NIST's interests and the public interest in developing secure, efficient, and interoperable cryptographic standards, and that vigilance in the standard-setting process from all participants – NIST staff included – is key to ensuring that all principles are upheld. To discourage undue influence, NIST should make all steps in the standard-setting process as transparent as possible, including documenting each feature of a cryptographic standard and the rationale behind choosing particularly critical parameters or features.

In addition, NIST should detail what mechanisms and process elements currently exist to mitigate sources of undue influence. For example, are NIST personnel trained to spot potential subversion? do they have mechanisms and procedures they can feel comfortable using to report potential instances of undue influence? NIST should go further than describing what mechanisms currently exist and affirmatively state as part of the principle of undue influence that NIST will not engage in weakening or biasing a standard – e.g., backdoors, trapdoors, or RNG state exposure – at the request of an intelligence agency or law enforcement entity.

C. Comments on Technical Merit

The principle of technical merit is not adequately defined. Certainly, the requirement that "security properties are well understood" – listed at the end of the paragraph on technical merit – contributes to technical merit, but there is certainly more to it. In this document, NIST must define what makes a particular standard or decision good. Are there evaluation criteria from past standards efforts that tend to result in a particularly good algorithm in practice? Vice versa, are there lessons about decision-making in standards setting processes that tend to weaken, impair, or undermine a standard?

Part of the definition of technical merit lies in the text associated with the balance principle, where the document stresses NIST's goal to "develop cryptographic standards that are secure, efficient, and promote interoperability." These three criteria, at a minimum, should be explicitly included and defined as part of the principle of technical merit. NIST must also describe how these three technical merit criteria interact: do they depend on each other? can any of them be absent? how are they evaluated during the standards process for different primitives, modes, and guidelines? are there other criteria that should be included in evaluating technical merit? Technical merit is the core consideration for the adoption of a cryptographic standard and providing a more detailed discussion of the components of technical merit is critical in this document.

D. Comments on Integrity

The document's explanation of the principle of integrity is overly narrow; integrity is much more than being impartial and objective. Integrity also involves sound construction, a lack of corruption, and honest conduct based on strong moral principles. NIST should describe a richer notion of integrity here and pledge in this document to conduct its standards activities with utmost integrity.

There are powerful adversaries engaged in the cryptographic standardization process. While we recognize that the intelligence community is an invaluable source of technical and theoretical expertise in cryptography, NIST must be more open and transparent about the extent of its collaboration with these agencies (both in formal and informal settings) and how these activities further the principles outlined in this document. NIST should also explicitly state measures it will not engage in. For example, it should be relatively easy for NIST to state in this document that never will a deliberate backdoor or intentional bias be introduced into a standard on behalf of the intelligence community or a law enforcement entity. Finally, NIST should outline administrative measures for NIST staff that are caught undermining standards processes, such as dismissal.

III. Mechanisms and Outreach

In addition to internal mechanisms mentioned above for NIST staff to report potential cases of undue influence, we also have comments on other possible mechanisms that could help improve NIST's standardization process. A critical question is: based on what evidence is a re-evaluation of a standard triggered? In the case of SP 800-90A – which contains Dual_EC_DRBG – the re-evaluation of that document appears to be based on significant "community commentary."[5] But certainly evidence of specific technical weakness should trigger a re-evaluation. Would internal evidence brought to light at NIST also trigger a re-evaluation and, if so, what kinds of circumstances might warrant a re-evaluation? While this set of triggers cannot be exhaustive or strict, they should be written down for illustrative purposes here.

There seems to be no type of lightweight publication between a press release and a Special Publication. NIST could better communicate with the public and the cryptographic community by posting more frequent public updates about cryptographic standards news and developments. For example, a blog-like venue on crsc.nist.gov for the cryptographic technology group could publish posts on current work, such as a series of posts that detail changes made to a winning competition algorithm during the post-competition standardization process. NIST could also use this opportunity to engage new audiences and encourage more people to get involved in security, cryptography, and cryptographic standardization activities and events.

In addition, NIST could expand the scope of some of its communication channels. For example, NIST could conduct outreach to non-cryptographic communities about the importance of cryptography for assurance. These broader outreach efforts should not just focus on cryptographers, engineers, and computer scientists, but also reach out to civil society, the cybersecurity community and policy audiences. These communities rely on cryptographic standards every day and NIST and the standards process itself could benefit from wider understanding of the value of cryptography and cryptographic standards. NIST could use an expanded but modest social media presence, with groups like Cryptographic Technology using those venues to keep interested stakeholders informed about current activities and events as well as engaging with the community directly.

Finally, NIST in its cryptographic standards role must engage with global interests explicitly, rather than implicitly. Since these standards are the building blocks of assurance online and in digital environments, NIST cannot afford to prioritize US interests or discount international

[5] "Supplemental ITL Bulletin For September 2013," National Institute of Standards and Technology, Information Technology Laboratory (September, 2013), *available at:* http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf.

perspectives. NIST should explicitly commit to recognizing international interests in its standards work.

IV. Conclusion

Thank you for the opportunity to comment on NIST-IR 7977. We offer our comments in the hope that the ongoing cryptographic standards review process will solidify NIST as an unbiased arbiter of technical cryptographic standards setting. These principles are a crucial first step in establishing a foundation for the detailed review work and process specification to come. The resultant post-review cryptographic standards process will be more robust for having engaged in this hard work.

For further information contact:

- Joseph Lorenzo Hall, Chief Technologist, (202-407-8825, joe@cdt.org)
- Runa A. Sandvik, Staff Technologist, (202-407-8838, runa@cdt.org)

From: "Tim Myers (SECURITY)" <timmyers@exchange.microsoft.com>
Subject: Comments on Draft NIST Interagency Report 7977, NIST Cryptographic Standards and Guidelines Development Process
Date: April 18, 2014 at 3:22:48 PM EDT
To: "crypto-review@nist.gov" <crypto-review@nist.gov>

Microsoft offers comments on the DRAFT NIST IR 7977 in the attached Word document. The same text appears below.

Comments on Draft NIST Interagency Report 7977, *NIST Cryptographic Standards and Guidelines Development Process*
By Niels Ferguson, Principal Software Development Engineer, Microsoft Corporation
April 18, 2014

Cryptographic standardization is a far bigger issue than it is presented here. Cryptography secures the Internet, and that makes it of vital importance to everybody. Until recently, NIST has had international credibility to essentially set the cryptographic standards for the world. That has changed; unassisted, NIST will not be able to set effective cryptographic standards going forward. In this area, credibility is everything, and recent revelations have sown enough doubt around the world that NIST-driven standards will no longer be acceptable, at least for a significant part of the worldwide market.

If cryptographic standards were to fracture into different national domains, the damage would be hard to contain. Interoperability would be damaged, and there is a big risk of security weaknesses along the edges of different cryptographic algorithm domains. National fragmentation of cryptographic standards is a threat to US industry; compliance with local cryptographic standards it is one of the leavers used to drive US companies out of competing in other countries. The Department of Commerce, and NIST in particular, could help the US industry by ensuring that cryptographic standardization is done in a manner that is widely accepted throughout the world.

Recommendation: NIST should drive an effort to create an international consensus system for setting cryptographic standards. This should include agencies of various governments (e.g. Brazil, China, France, Japan, Russia, UK, US, …), major industry players that drive adoption (Apple, Google, Microsoft, …), and the academic community (IACR).

Best regards,
Tim

Tim Myers | Security Program Manager | FIPS 140-2 Security Evaluations
Trustworthy Computing Security | Microsoft Corporation | +1 (425) 707-9422

From: <Kent_Landfield@McAfee.com>
Subject: Intel comments in response to NIST IR 7977, ²NIST Cryptographic Standards and Guidelines Development Process (Draft)
Date: April 18, 2014 at 6:37:11 PM EDT
To: <crypto-review@nist.gov>

Hello crypto-review@nist.gov,

Intel appreciates the opportunity to respond to the Request for Comments on NISTIR 7977 "NIST Cryptographic Standards and Guidelines Development Process (Draft)" noticed February 18, 2014.

Intel recognizes the indispensable work NIST has done to protect the cybersecurity interests of the United States and to provide industry with cryptographic technologies that have had broad applicability and utility. As the use of cryptographic technologies has become more widespread, the importance of NIST's role has never been more apparent. Intel is hopeful these comments will provide feedback that will help NIST improve the process of developing cryptographic standards and to further strengthen NIST's role.

Thank you.

Kent Landfield
Director, Standards and Technology Policy
McAfee. Part of Intel Security
+1.817.637.8026

Attachment follows.

April 18, 2014

Via e-mail to crypto-review@nist.gov

Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Re: Intel comments in response to NIST IR 7977, "NIST Cryptographic Standards and Guidelines Development Process (Draft)"

Intel appreciates the opportunity to respond to the Request for Comments on NISTIR 7977 "NIST Cryptographic Standards and Guidelines Development Process (Draft)" noticed February 18, 2014.

Intel recognizes the indispensable work NIST has done to protect the cybersecurity interests of the United States and to provide industry with cryptographic technologies that have had broad applicability and utility. As the use of cryptographic technologies has become more widespread, the importance of NIST's role has never been more apparent. Intel is hopeful these comments will provide feedback that will help NIST improve the process of developing cryptographic standards and to further strengthen NIST's role.

Throughout our response there are several key themes in our comments and recommendations.

- Increased collaboration with SDO's rather than NIST-driven standards
- Global adoption and attention paid to international standards work
- Transparency for evaluation and development processes
- Transparency for remediation and change processes

Besides the comments in our response below, there are several additional points we would like to mention.

- NIST should define a global acceptance strategy for every cryptographic standard anticipated for use in commercial mass-market technology. A key element of those strategies includes working with industry SDOs, preferably international standards bodies, instead of inviting industry to participate in a NIST standards development process. This approach, consistent with OMB Circular A-119, would result in standards that are better recognized as global/international, which would accelerate acceptance and implementation.
- For completeness and transparency, NIST should clearly describe the process for responding to problems discovered in cryptographic standards. The current draft does not adequately address this issue. These issues need to be resolved through community engagement, not by NIST offering a consultation to interested experts.
- A clear statement on the purpose and background of the IR should be stated at the beginning of the document. The cryptographic community is aware of the recent events

impacting the creation of this document. Referencing the purpose of the IR at the end of the document may negatively impact the perception of the IR.

- NIST should add comments on Implementation Guidance. While NIST talks about the three major document types, there are no statements on Implementation Guidance documents critical to implementing, for example, FIPS 140-2. As Guidelines are in the title, it seems a missing piece and often the implementation guidelines can impact development as much as a specific standard does.

Please see our narrative comments, concerns and recommendations below regarding the draft, organized by section.

Principles

Intel is in full agreement the principles listed in the draft should be guiding principles for cryptographic standards development. We recommend one additional principle be included for standards intended to have commercial impact: Strategy for *Global Acceptance*.

Global Acceptance

While the primary focus of NIST is the United States, the result of NIST's work has become relevant worldwide, because industry has adopted NIST crypto standards as the best available. However, because NIST is not recognized as a developer of international standards, NIST specifications on their own are not accepted everywhere and, recently, have caused concerns among the experts due to perceived lack of transparency.

Since the ecosystem is global, impact of adoption outside of the United States is crucial for success of the standards.

NIST should develop a global acceptance strategy for each standard it is involved with developing that it anticipates having a commercial impact. A key element of those strategies should be a stronger and more consistent preference for participating and contributing to security standards developed by open and fair international standards development organizations and then adopting the resulting standards for use by the U.S. Government.

To highlight one specific opportunity, NIST could better leverage standards in ISO/IEC JTC 1 SC27 rather than duplicate those efforts. For example, SC27 WG2 is currently working on entropy standards and NIST should be leading that effort to harmonize and strengthen SP 800-90, which should simply reference the resulting ISO/IEC standard. Duplicative efforts can result in small but critical differences between SP 800-90 and the ISO/IEC standard.

NIST should also be aware of efforts to develop similar regional standards and work with the entities engaging in regional standardization to ensure their requirements are incorporated where possible, to avoid fragmentation in security standards worldwide.

Recommendation: Intel recommends the addition of "Global Acceptance" as a guiding principle and attention to the development of regional standards, to increase potential for global adoption.

Transparency

Line 21 states "…access to essential information". While previous cryptographic competitions have been open, and evaluation criteria available, the weighting of various criteria is not always clear. Lack of understanding of the criteria for evaluation can lead to uncertainty as to the relative merits of one choice over another. Does NIST consider throughput more important than size? Or more precisely, what is the relative weight of throughput in relationship to size of code. Knowing these criteria and how they are applied will make the processes more transparent and alleviate concerns among experts.

In order for NIST to provide more specific evaluation criteria, early in the process of cryptographic standards development, NIST needs to make it clear whether the focus of a standard is primarily for government consumption or for commercial impact. NIST needs to define its evaluation criteria for standards intended first and foremost for commercial impact.

Recommendation: "access to essential information" needs to be clarified through the use of examples such as … evaluation criteria, relative weighting of the evaluation criteria, …". As it stands now the statement gives the impression NIST is limiting information provided to interested parties to a small subset. Providing examples of 'essential information' would improve understanding of the intent of the statement. Engaging independent experts as observers in the evaluation process will also help build trust.

Openness

While algorithm competitions have been great examples of open participation, there has been a perception that some internal cryptographic standards development at NIST follows a closed process. For any NIST publication where adoption by industry is expected, NIST should follow a fully open process.

Recommendation: Provide the reasoning and guidance in the document as to when NIST will follow the open participation/competition model versus when NIST will create a new publication without open participation/competition. Include alternative avenues of standards creation where NIST collaborates with SDOs to develop new cryptographic standards.

Technical Merit

The aspects of technical merit should be more clearly and specifically explained. For example, the anticipated use model drastically affects the technical merits of a standard or guideline. What is appropriate for a server may be very inappropriate for a cell phone. Security properties require tailoring to the specific use model. Examples would make this a more valuable section. With technologies changing very quickly and new usage models appearing with great frequency, NIST should consider greater flexibility in recommendations in response to a very dynamic environment.

Recommendation: Provide more specific details of "technical merit". Ensure the requirements are flexible to be attuned to the dynamic computing environment.

Balance

The balance between stakeholders has a bias towards enterprise stakeholders. This is not surprising as the vast majority of NIST stakeholders are, in essence, enterprise customers. But the security standards established by NIST have huge implications towards non-enterprise use. In fact, in many cases, the vast majority of the uses of the NIST standards would be in non-enterprise situations.

Recommendation: Add "… government, industry, academia, and individual users worldwide, …"

Integrity

NIST needs to be perceived as an impartial technical authority. Recent events impacting the creation of this document unfortunately call the impartial nature of NIST into question, especially outside of the United States. NIST should be proactive and show leadership to reinforce its fundamentally impartial role - NIST should work harder at being more open, more transparent, and work much closer with international organizations like ISO/IEC and the IETF in order to fight global misperceptions to the contrary.

Continuous Improvement

The use of competitions, and the ability to modify submissions relative to deficiencies, is a critical aspect of openness and transparency. NIST should ensure this type of feedback is always present in the development of security standards.

On line 48… "When vulnerabilities are identified, NIST engages with the broader cryptographic community to address them." This statement misses the opportunity to describe how NIST engages with the community. If this document is to be taken as a credible description of NIST's processes, the fundamentals of engagement the community can expect should be described here.

Stakeholders

The Balance principle highlights a missing stakeholder, the individual. The mention of private sector, in line 59, is still referencing enterprise use and not the individual. As many, if not all, of the private sector individuals referred to have, at a minimum, access to the Internet, and represent potential attack points, the security at these individuals' endpoints is critical to an overall security solution. The use of NIST standards in these devices will be a deciding factor in the ability of critical infrastructure to interoperate with the individual and their device. Ensuring NIST standards are applicable to an individual's devices argues for the inclusion of the individual in the list of NIST stakeholders.

Recommendation: Add ", individual," to all references to academia, industry and government. Ensure strong coverage for consumer uses and applications worldwide.

Development of New Standards

Line 133 states "… determines that no suitable standard already exists". What is not apparent is the criteria in use to determine suitability. Just as the creation of new standards should follow the guiding principles, the determination of "suitable" should also follow those same principles. The openness, transparency, and inclusion of industry and academia should be mandatory inputs

when determining if existing standards are suitable. NIST should make explanations of how it has reached these determinations available for public review.

Recommendation: Clearly state the process NIST uses for evaluating that no suitable standard exists and include a public review. Broaden the evaluation of suitable standards to regional bodies, to ensure they are coopted and not in opposition and that resulting standards are well positioned for global adoption.

Public Review and Outreach

Historically, Intel has had varied success in collaborating with NIST. The AES and SHA competitions and the creation of SP 800-147 are examples of highly successful industry and government partnership. However, work related to the Random Number Generators in SP 800-90 and X9-82 has been frustrating and not productive. In the first instance, NIST partnered closely with industry and incorporated feedback, but in the latter case, such partnership was not as evident.

While this draft IR is a good start, it seems to be light on specifics, details and examples. We believe this is an opportunity for NIST to demonstrate to the cryptographic community it is working hard to be extremely transparent in all aspects of cryptographic standards development. Enhancing this document with more details, using successes of the past as examples, would go a long way to assure the community NIST is serious about their concerns and is working hard to prove it.

Thank you again for the opportunity to provide our inputs to this process. Now more than ever we must find way to better leverage the expertise of the cryptographic community and to work with international SDOs in developing the means to protect our global, corporate, business and personal information. We welcome the opportunity to continue this constructive dialog with NIST as it continues to improve the process of developing cryptographic standards.

From: Amie Stepanovich <amie@accessnow.org>
Subject: Comment Submission: NIST IR 7977
Date: April 18, 2014 at 7:22:15 PM EDT
To: <crypto-review@nist.gov>
Cc: Jochai Ben-Avie <jochai@accessnow.org>

To Whom It May Concern -

Thank you for the opportunity to provide feedback on NIST IR 7977. Please find attached comments from Access, Advocacy for Principled Action in Government, CEI, EFF, EPIC, Fight for the Future, OTI, OpentheGovernment.org, Silent Circle, Student Net Alliance, Sunlight Foundation, and TechFreedom.

If you have any questions or comments, you can contact me at amie@accessnow.org. Please confirm receipt of this email and the attachment.

Thank you,

Amie Stepanovich

Amie Stepanovich
Senior Policy Counsel
Access Washington, D.C. | accessnow.org

tel: +1.863.697.0009
@astepanovich
PGP: 1C1DA0C7

Attachment follows.

In the Matter of NIST Cryptographic Standards and Guidelines Development Process
NIST IR 7977 (Draft)

April 18, 2014
Submitted via e-mail to crypto-review@nist.gov

On February 19, 2014, the National Institute of Standards and Technology ("NIST") published *NIST Cryptographic Standards and Guidelines Development Process (NIST IR 7977)*, a draft document that "outlines the principles, processes, and procedures of NIST's cryptographic standards efforts."[1] The draft document sets out key guiding principles and methods for engagement and outreach to ensure that adopted standards are "robust and have the confidence of the cryptographic community."[2]

On September 5, 2013, in joint reports by The Guardian,[3] The New York Times,[4] and ProPublica,[5] it was revealed that the National Security Agency ("NSA") had exerted influence over NIST in order to intentionally weaken NIST cryptographic standards. Under federal law, NIST is required to consult with NSA on the development of cryptographic standards.[6] One of NSA's primary missions is "information assurance," under which it "ensure[s] appropriate security solutions are in place to protect and defend information systems."[7] However, this mission is often at odds with NSA's other primary directive - signals intelligence, under which it conducts its communication surveillance activities. The President's Review Group on Intelligence and Communications Technologies has recommended significant structural changes to the NSA in order to separate these missions, but such separation has not yet occurred.[8]

---

[1] *NIST Cryptographic Standards and Guidelines Development Process (Draft),* NAT'L INST. OF SCI. AND TECH. (Feb. 2014), *available at* http://csrc.nist.gov/publications/drafts/nistir-7977/nistir_7977_draft.pdf [hereinafter NIST IR 7977].
[2] *Id.* at 1.
[3] James Ball, Julian Borger & Glenn Greenwald, *Revealed: How U.S. and U.K. Spy Agencies Defeat Internet Privacy and Security*, THE GUARDIAN, Sept. 5, 2013, *available at* http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.
[4] Nicole Perlroth, Jeff Larson & Scott Shane, *NSA Able to Foil Basic Safeguards of Privacy on Web,* N.Y. TIMES, Sept. 5, 2013, *available at* http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0.
[5] Jeff Larson, Nicole Perlroth & Scott Shane, *Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security*, PROPUBLICA, (Sept. 6, 2013), http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.
[6] *See* Federal Information Security Management Act of 2002 § 303(c)**,** 44 U.S.C. § 3541; *see also* NIST IR 7977 at 2 ("NIST works closely with the NSA in the development of cryptographic standards. This is done because of the NSA's vast expertise in cryptography and because NIST, under the Federal Information Security Management Act of 2002, is statutorily required to consult with the NSA on standards.").
[7] *About IA. at NSA*, NAT'L SEC. AGENCY, http://www.nsa.gov/ia/ia_at_nsa/.
[8] The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, 21 (Dec. 12, 2013), *available at*

In regard to its conflicting missions, NSA's ability to wield influence over NIST remains central to the cryptography community's decreased confidence in the Agency. On September 10, 2013, NIST responded to the reports regarding the NSA:

> NIST has a long history of extensive collaboration with the world's cryptography experts to support robust encryption. The National Security Agency (NSA) participates in the NIST cryptography development process because of its recognized expertise. NIST is also required by statute to consult with the NSA. Recognizing community concern regarding some specific standards, we reopened the public comment period for Special Publication 800-90A and draft Special Publications 800-90B and 800-90C to give the public a second opportunity to view and comment on the standards.[9]

NIST has not publicly revealed to what extent or in what ways the NSA influenced these standards, or if evidence exists that other standards have been similarly undermined. In order to re-build confidence in NIST, it is necessary that the Agency takes pro-active steps toward implementing a more transparent, accountable process for standards development.

NIST IR 7977 sets out and elucidates guiding principles in the standards-setting process: transparency, openness, technical merit, balance, integrity, and continuous improvement. In order to meet NIST's goals, NIST guiding principles should be modified and amended to provide greater transparency and access. We address each of the six guiding principles in turn.

Transparency

Transparency is perhaps the area where NIST can best act to increase confidence in its internal processes and procedures. The draft document explains that NIST works toward transparency in its "selection and evaluation criteria, specification, security and performance characteristics, and provenance of proposed standards and guidelines."

In the development or adoption of standards, NIST should further commit, to the extent that it does not invade personal privacy interests, to transparency on the identity and affiliation of individuals and organizations that consult on the development process.

Specifically in regard to the NSA, NIST should establish a policy wherein the Agency publicly explains the extent and nature of the NSA's consultation on future standards and any modifications thereto made at NSA's request. Further, NIST should begin a review process to ensure that wherever possible the same information is published for standards that are currently

---

http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf ("NSA should be clearly designated as a foreign intelligence organization. Other missions (including that of NSA's Information Assurance Directorate) should generally be assigned elsewhere.").

[9] *Cryptographic Standards Statement*, NAT'L INST. OF SCI. AND TECH. (Sept. 10, 2013), http://www.nist.gov/director/cybersecuritystatement-091013.cfm.

in use. A full accounting of the interactions between the two Agencies will allow the cryptography community, oversight bodies, and the public at large to judge to what extent the NSA's signals intelligence mission is interfering with a process to develop the most secure standards.

Openness

NIST maintains a public-facing website on which it publishes its draft and final documents, standards, and other information. NIST also utilizes the Federal Register to publish documents on which a public comment opportunity is available. These sources are all used to create an open process.

Although not detailed in NIST IR 7977, NIST also maintains a Twitter account where information is often published and linked to, @USNISTgov.[10] The Twitter account was recently used during NIST's Privacy Engineering Workshop to "live-tweet" the panels and events of the event. For further example, the Office of the Director of National Intelligence recently launched a page on popular social networking website Tumblr to centralize the publication of information on national security issues.[11] The website has been generally well-received and considered a useful resource.

NIST should attempt to maximize reach and engagement and limit barriers to access in order to conduct the best possible outreach to the public. Formally embracing communication tools that allow for greater public outreach will put NIST on the forefront of online engagement and help ensure that interested parties are engaged in the NIST processes. In deciding on platforms, NIST should not only consider reach, level of engagement, and barriers to access, but also the ability to search for and access historical content to ensure persistence and continuity.

Technical Merit

While NIST may "strive[] to standardize cryptographic algorithms, schemes, and modes of operation whose security properties are well understood," it sometimes fails to provide the proper basis for external expert analysis. For example, prominent cryptography expert Matthew Green has highlighted how NIST's habit of not providing security proofs with its standards -- including the Dual_EC_DRBG standard suspected of having a backdoor[12] -- makes it more difficult for outside experts and stakeholders to evaluate the technical merits of the standards and participate in the standards process.[13] NIST should commit to always providing a security proof for standards when the standard is put out for public comment. NIST should also commit

[10] @usnistgov, https://www.twitter.com/usnistgov.
[11] IC ON THE RECORD, http://icontherecord.tumblr.com/.
[12] Stephen Checkoway, Matthew Fredrikson, Ruben Niederhagen, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, & Hovav Shacham, *On the Practical Exploitability of Dual EC in TLS Implementations*, *available at* http://dualec.org/DualECTLS.pdf (last visited Apr. 18, 2014).
[13] Matthew Green, *The Many Flaws of Dual_EC*_DRBG, A FEW THOUGHTS ON CRYPTOGRAPHIC ENG'G (Sept. 18, 2013), http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html.

to explaining the justification for, origin, and means of generation for any parameters supplied in NIST standards.

Balance

The balance principle, under which NIST accepts input from all stakeholders to "ensure its standards...meet the needs of the federal government as well as the broader user community," should be narrowed. The provision should specify that, unless necessary, NIST will only take into account information assurance needs of government in establishing cryptography standards, and should, under no circumstances, consider the signals intelligence needs of the NSA or any other intelligence or law enforcement need of any agency.

Integrity

In Integrity, NIST explains that the Agency "serves as an impartial technical authority when developing cryptographic standards and guidelines."[14] However, as discussed above, NIST's requirement to consult with the NSA and the likelihood that the NSA has degraded certain standards calls this into question. In order to truly preserve the integrity of the Agency, NIST should act on the all of the recommendations in this document so that dealings with entities in the intelligence community are well-known and can be assessed in terms of their impact on a given standard.

Continuous Improvement

NIST's commitment to accepting expert feedback is commendable. The "open source" technique of inviting feedback to identified vulnerabilities is specifically in line with identified best practices.

In addition to these six guiding principles, NIST should also add a seventh – usability.

Usability

Even theoretically strong cryptography standards may be exploited in practice. In fact, "[u]ser errors cause or contribute to most computer security failures."[15] Cryptographer and programmer Daniel J. Bernstein has explained how standards that appear technically sound "when properly implemented and used for the purposes for which they…are designed," may still be extremely

[14] NIST IR 7977, *supra* note 1, at 2.
[15] Alma Whitten & J.D. Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0 in* IN SECURITY AND USABILITY: DESIGNING SECURE SYSTEMS THAT PEOPLE CAN USE (eds. L. Cranor & G. Simson, O'Reilly, 2005) pp. 679-702, at 679, *available at* http://www.cs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf; *see also* Mike Hearn, Uability of Crypto Software (Mar. 5, 2014), Medium, https://medium.com/bitcoin-security-functionality/d04ea6a2c771 ("The security community has a problem, and we all know it. Too often, the people we wish were using our software can't figure it out.").

fragile and easy to use incorrectly.[16] Certain implementation errors may be anticipated or planned for such that it would render the implementation of a standard unsafe.[17]

In other industries, NIST has recognized usability, or "how easily someone can use [a product] for its intended purpose," as a key consideration.[18] NIST should extend this to its cryptography work to ensure that security standards are not weaker in practice than anticipated by examining only the underlying mathematics.

NIST has traditionally served an important and unique role in the technical community. As Matthew Green has pointed out, "we're highly dependent on NIST standards."[19] If NIST is to continue to play this role, it needs to take drastic and affirmative actions to re-commit itself to its core mission and to remove any traces of impropriety.

Thank you for your request for public comment. We look forward to further engaging with NIST on this and other important matters.

Sincerely,

Access
Advocacy for Principled Action in Government
Competitive Enterprise Institute ("CEI")
Electronic Frontier Foundation ("EFF")
Electronic Privacy Information Center ("EPIC")
Fight for the Future
New America Foundation's Open Technology Institute
OpentheGovernment.org
Silent Circle
Student Net Alliance
Sunlight Foundation
TechFreedom

[16] Daniel J. Bernstein, How to Design an Elliptic-Curve Signature System (Mar. 23, 2014), The cr.yp.to blog, http://blog.cr.yp.to/20140323-ecdsa.html.
[17] *Id*.
[18] Press Release, NIST, NIST Releases Technical Guidance for Evaluating Electronic Health Records (Mar. 20, 2012), http://www.nist.gov/itl/iad/ehr-032012.cfm; *See also* NIST, Usability, http://www.nist.gov/healthcare/usability/ (last visited Apr. 18, 2014).
[19] Matthew Green, *On the NSA*, A FEW THOUGHTS ON CRYPTOGRAPHIC ENGINEERING (Sept. 15, 2013), http://blog.cryptographyengineering.com/2013/09/on-nsa.html.

From: Tanja Lange <tanja@hyperelliptic.org>
Subject: Comments on NISTIR 7977
Date: April 18, 2014 at 10:54:52 PM EDT
To: <crypto-review@nist.gov>

Dear Ladies and Gentlemen,
Please find below my comments on NISTIR 7977.

Best regards
Tanja Lange

Prof. Dr. Tanja Lange
Coding Theory and Cryptology, MF6.104 B
Department of Mathematics and Computer Science
Technische Universiteit Eindhoven
P.O. Box 513
5600 MB Eindhoven
Netherlands

Those who cannot remember the past are condemned to repeat it

In the aftermath of the Snowden revelations on Project Bullrun and the Sigint Enabling Project, NIST is reviewing its procedures of how cryptographic standards should be developed. It is a laudable development to have the procedures publicly discussed and to request feedback on them. The cryptographic competitions organized by NIST were also laudable efforts to involve the cryptographic community at large.

However, most of the document describes essentially the status quo -- how are standards developed presently and in the past -- and does not state anywhere that a change of procedure is needed; unless of course, this description is presenting what will happen in the bright and glorious future and is a departure of what was there before. To clarify that change is coming, and I do hope that this time change is coming, it is necessary to highlight where the future procedures will be different from current and past procedures and how the future procedures will prevent targeted influencing of standards by government agencies. This should happen as part of this document (or as a separate report, to be released at the same time) detailing the vulnerabilities of the old system. Obviously these considerations of how the new system improves on the old should include the threat of subversion by the agencies but also the problem of companies pushing modifications that give them IPR related benefits (the case of the Certicom patent on alternative points for Dual_EC comes to mind, here).

As a researcher in cryptography I could not imagine that NIST had not dropped support for Dual_EC back in 2007, but I have to admit that I failed to check. I think that for security standards the comments phase should never end -- NIST should always be open for comments

showing vulnerabilities in their published standards and commit to reacting to such comments publicly. I, like many others, misinterpreted the silence after the back door announcement and widespread publication (e.g. by Schneier in WIRED) as a sign that this problem was dealt with and the RNG was no longer supported. A look on http://csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgval.html shows how wrong I was. How could this happen? What are the lessons for the future to prevent repetition. Since this document is a meta-standard on how to make standards a reflection on what went wrong in the past is important.

Instead of promising change, the current document praises NSA's work in the "Stakeholders" part and says "NIST works closely with the NSA in the development of cryptographic standards. This is done because of the NSA's vast expertise in cryptography and because NIST, under the Federal Information Security Management Act of 2002, is statutorily required to consult with the NSA on standards." After this statement I would like to see a clear explanation that NIST is emancipating itself and that in the future the collaboration will be restricted to 'consulting with the NSA' rather than 'taking input from the NSA without requiring additional evaluation.' Is there a memorandum of understanding (similar to the one in http://epic.org/crypto/dss/nsa_abernathy_letter.html) accompanying the Federal Information Security Management Act? Are the agreements between NIST and the NSA beyond this?

The "Stakeholders" part is an example of the huge influence that NIST's recommendations enjoy, but with great power comes great responsibility. This power is also a weakness of the system: if a target of the agencies is likely to adopt a NIST standard, the standard becomes a valuable target for sabotage and NIST needs to be aware of this and should demonstrate awareness as part of this document.

I am sympathetic to the feelings of NIST employees that they had not expected the NSA to deal with them in the way revealed on 5 September 2013, however, in historic perspective, SP800-90 (and whatever else further research will find) are just some more recent examples of a collaboration between two unequal partners. This case too closely mirrors the comments reported in the "New NIST/NSA Revelations" from May 1993 (!) (see e.g. http://epic.org/crypto/dss/new_nist_nsa_revelations.html) 'the "NSA problem" was apparently the intelligence agency's demand that perceived "national security" considerations take precedence in the development of the DSS. From the outset, NSA cloaked the deliberations in secrecy.' (and other reports of tension between NIST and the NSA stated in that report). There are further parallels between the DSS case and the SP800-90 case: in both cases the public was left in the dark about the providence of the algorithms, in both cases the public perception was that the algorithms were developed by NIST, while in fact they were developed by the NSA.

It is important that future standardization efforts correctly attribute authorship of algorithms and other inputs. This is already the case for input from the academic community and to some extent also for input from security researchers and companies but not at all the case for input from government agencies. Some standards, including SP800-90, include acknowledgments to NSA employees (mentioned by name), but there is no indication of their role in the standard and it is unclear whether they were the only NSA employees involved.

If changes to a standard become necessary, the change log should include acknowledgments and justifications for the changes. See https://projectbullrun.org/dual-ec/standard-change.html for reasons.

I recommend to amend the section on "Transparency" to expand "and provenance of proposed standards or guidelines" to "and provenance of proposed standards, guidelines, and input on drafts and standards, by giving names and affiliations".

I recommend to amend the section "Openness" by including as a final sentence "All inputs received will be made available publicly, this includes, but is not limited to, the initial draft including references for design and analysis of the included components, all comments received in public and internal consultations, presentations at workshops, etc." I understand that certain provisions need to be made for companies reporting on IPR, but I would like to have these to be as public as possible; this is a must if they are instrumental in making choices. As the bare minimum there should be a time limit on how long such comments can remain private.

I would like to see a clear mission statement that NIST's mission is to achieve security, which includes security against attackers inside the security agencies. Cases such as the DSS where even the public announcement included "Among the factors that were considered during this process were [..] impact on national security and law enforcement" should be a thing of the past. This should also be reflected in the paragraph titled "Balance".

There are several other things in the draft that should change before adoption:

l.46 New paragraph before "Continuous Improvement:"; there were also some missing spaces in the text.

l.46 The text on "Continuous Improvement:" should include mechanisms how NIST reacts to vulnerabilities discovered after a standard has been adopted. This should include a commmitment to address the concerns publicly.

l.50 I hope that also the government agencies are encouraged to identify weaknesses and inform the public and NIST about them.

l.60-67 This is backwards for the part on elliptic curves included in Suite B. NIST received them from the NSA and then some of them were included in Suite B. This is an appropriate place to clarify this. It is public knowledge and has not been denied but it is not on public record and the presentation given here distorts the facts.

l.218 The randomness beacon should not be used for generating cryptographic key material, as correctly stated on that site; so why is it included here? To the very least include "for testing purposes" in the description.

l.283 Is this the correct story? This is the version you will be held accountable for. Was it NIST to take initiative, as claimed in "NIST recognized", or the community or the NSA?

l.295 Who provided this document to ISO? NIST or ANSI?

l.308/309 the inclusion of Hash_DRBG is inadequately explained; whose request was this?

l.315/316 "All such feedback was considered for incorporation into the SP 800-90 documents." is disgraceful to those who were told that their comments were too late since the standard had already been implemented by companies.

I'm happy to see that NIST has recently published some more public comments but this still does not seem to cover all comments made regarding SP800-90 in general, and Dual_EC in particular.

l.317-319 "Some in the cryptographic community have expressed concern": This does not report the facts correctly. Several in the cryptographic community have expressed concern about the security since the very first draft of SP800-90 back in 2004; the potential back door was widely publicized in 2007. At that point NIST should have dropped support for Dual_EC; dropping it in September 2013 is better than never but significantly too late.

It is unclear to the public at which point NIST became aware of the possibility of a back door in Dual EC; Certicom filed for a patent on using this back door in January 2005; did they inform NIST at that point? There are stories that the potential back door was discussed at meetings before summer 2007 and that the possibility was discarded -- when was this and who deserves credit for finding that Dual_EC is backdoorable and what arguments were used to ignore it? We need to understand the history to avoid a repetition of this!

From: Karen McCabe <k.mccabe@ieee.org>
Subject: Contribution to public review of NIST IR 7977
Date: April 21, 2014 at 8:19:01 PM EDT
To: <crypto-review@nist.gov>

Dear NIST
Please find attached a contribution from the IEEE Standards Association in response to the call for public comment on NIST Cryptographic Standards and Guidelines Development Process (NIST IR 7977).

Best Regards
Karen McCabe
Senior Director, Collaboration and Consensus Community
IEEE Standards Association
445 Hoes Lane
Piscataway, NJ 08855 USA
k.mccabe@ieee.org
+1 732 562 3824

Attachment follows.

NIST
100 Bureau Drive, Stop 1070
Gaithersburg, MD 20899-1070

18 April 2014

The IEEE Standards Association (IEEE-SA) is pleased to provide feedback to the National Institute of Standards and Technology (NIST) with respect to IR 7977, based upon the questions it has posted to the public. As a baseline statement, the IEEE-SA brings to the attention of the reader the principles of Open-Stand (open-stand.org).

The IEEE-SA believes that standards developed in accordance with Open-Stand principles are among the most effective in the world due to the multi-stakeholder, market-driven, bottoms-up approach. Such standards are created within a framework that provides all stakeholders with full access to the views and objections of all participants throughout the process as well as meaningful opportunities to participate at all stages of standards development, including final approval. Processes that are in accordance with the spirit and values of Open Standard result in documents that are widely vetted by professed experts with a multitude of affiliations, and are expected therefore, to be free of dominance from any single entity.

The IEEE-SA has the following specific recommendations for NIST.

NIST may consider the creation of a public, digital community of experts that provides for wide and transparent vetting of all views, verbatim, at the pre-standards stage. NIST may also consider introducing a level of transparency around its final vetting process. At the moment, final approvals are granted by NIST, but the manner in which those approvals are granted and the criteria for approval are not clearly documented. Additionally, during the drafting and final approval, dissenting views are not publicly shared, verbatim. The IEEE-SA suggests that the summarization of publicly solicited comments does not provide an adequate level of transparency. It is also suggested that NIST considers implementing an appeals process.

The IEEE-SA appreciates the opportunity to provide these comments to NIST and looks forward to further discussions on the matter.

The Institute of Electrical and Electronics Engineers, Inc.
445 Hoes Lane Piscataway, NJ 08854, USA Phone +1 732 562 3800 Fax +1 732 562 1571 standards.ieee.org

From: "Salaets, Ken" <ksalaets@itic.org>
Subject: ITI-ITAPS comments on draft NISTIR 7977
Date: April 22, 2014 at 6:11:02 PM EDT
To: "crypto-review@nist.gov" <crypto-review@nist.gov>
Cc: "Boyens, Jon M" <jon.boyens@nist.gov>, "Sedgewick, Adam"<adam.sedgewick@nist.gov>

To Whom It May Concern:
I am happy to submit the attached comments regarding draft NISTIR 7977 on behalf of my colleagues at the Information Technology Industry Council and the Information Technology Alliance for Public Sector. We very much appreciate the opportunity to respond after the April 18 deadline.

We would be happy to respond to any questions and provide additional details, as appropriate.

Best regards,
Ken Salaets

Ken J. Salaets
Director, Global Policy
Information Technology Industry Council
1101 K Street NW, Suite 610
Washington, DC 20005
+202-626-5752
Mobile: +301-437-3349
Website: www.itic.org
Twitter: @TechElect

Attachment follows.

Information Technology Industry Council

IT Alliance for Public Sector

April 22, 2014

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Via e-mail to: crypto-review@nist.gov

RE: ITI and ITAPS comments on Draft NIST Interagency Report 7977, *NIST Cryptographic Standards and Guidelines Development Process*

The Information Technology Industry Council (ITI) and IT Alliance for Public Sector (ITAPS) appreciate the opportunity to comment on Draft NIST Interagency Report (NISTIR) 7977, *NIST Cryptographic Standards and Guidelines Development Process*.

ITI is the premier voice, advocate, and thought leader in the United States for the information and communications technology (ICT) industry. ITI's members comprise the world's leading ICT companies, with headquarters worldwide. ITAPS, a division of ITI, is an alliance of leading companies building and integrating innovative technologies for the government customer.

Our companies strongly support NIST's work developing computer security standards and guidelines for U.S. federal non-national security (NSS) information systems, as required under the U.S. Federal Information Security Management Act (FISMA) of 2002.[1] Many of our companies provide input into the development and selection of these standards and guidelines, including for cryptography. Our companies also are involved in an array of work in a multitude of global standards development organizations (SDOs) to develop cryptographic standards and guidelines for voluntary use in commercial and other markets. We are heavily involved in both of these work streams because cryptography is essential for security and privacy and is demanded by businesses, governments, and citizens worldwide.

Over the last decade, the use of cryptography has blossomed from a niche technology deployed mainly by governments and militaries/intelligence communities to becoming a ubiquitous, integral part of everyday life, as demonstrated by the widespread availability of commercial products supporting strong cryptography. In many ways, cryptography is now a core component of Internet and e-commerce development – and therefore economic growth. At the same time, ICT products and the cryptography they contain must be globally interoperable. The global nature of technology and cyberspace underscore the essential nature of strong, robust, and globally accepted and deployed cryptographic standards to enable interoperability, trust, and security.

[1] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf,

We appreciate NIST developing this NISTIR and soliciting public comment. Over the past nine months, the integrity of NIST's processes with regard to its development of cryptographic standards has been called into question since press reports surfaced in 2013 about the National Security Agency's (NSA) involvement in the development of the NIST SP 800-90A Dual Elliptic Curve Deterministic Random Bit Generation standard. We applaud NIST for putting this standard and related guidance back out for a 60-day public comment period in September 2013[2] as a testament to NIST's commitment to a transparent and trustworthy public process to rigorously vet its standards and guidelines. Full stakeholder input into the new review is just as important as it was during the original standard's development. It is imperative that trust in the integrity of the process be reaffirmed, both in terms of this particular standard and the NIST process overall. We hope and expect that this NISTIR will contribute to that reaffirmation.

Our comments below focus on two main areas: the content itself of NISTIR 7977, and NIST's processes developing and/or contributing to cryptographic standards development.

NISTIR 7977 content: Suggested additions/clarifications

We are eager for this NISTIR to serve an important role in fully describing NIST's process in a way that highlights the processes' transparency (including ensuring that stakeholder input is sourced and traceable). The international community, in particular, needs to clearly understand what this process entails. We believe the NISTIR will benefit by the elaboration or addition of some key items.

The NISTIR should clarify what NIST is and is not. The NISTIR should clearly state that NIST is a technology-based, not policy-based, agency.

The NISTIR should better describe the two very distinct roles NIST plays with regard to developing security standards. The NISTIR begins by describing NIST's responsibility under FISMA for developing standards and guidelines for use in U.S. federal non-national security information systems. It is not until line 116, "Adoption of Existing Standards," that NIST's other role is described, i.e., that of being one of many stakeholders contributing technical expertise to voluntary, global, consensus-based standards developed by SDOs. These are two distinct roles that are important to differentiate, particularly for a global audience. Examples of how NIST works on cryptographic standards in each case would be illuminating. At the same time, NIST should make clear that the purpose of the NISTIR is to describe the former work, which is related to NIST's statutory role relative to U.S. federal information systems.

The NISTIR should better explain NIST's work developing standards for U.S. federal information systems. The NISTIR should make very clear that:

- This work is not specific to cryptography but, rather, is part of a much broader statutory requirement to develop computer security standards and guidelines;

[2] http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf

- Federal government standards developed by NIST are only applicable to federal non-NSS information systems;
- NIST standards and guidelines for federal information systems are developed using extensive stakeholder input;
- NIST standards and guidelines for federal information systems are found by many stakeholders to be highly secure and very relevant such that these stakeholders (including state and local governments, private entities, and even non-U.S. entities) voluntarily choose to implement them;
- There is a distinction between non-NSS and NSS systems and that NIST develops standards and guidelines for the former, and the NSA for the latter; and
- The requirement that NIST consult with the NSA on security standards development is only with regard to NIST's work developing standards for federal information systems under FISMA section 3543 Section 303 (b) (1), not with regard to NIST's other work contributing technical expertise to voluntary standards developed by SDOs.

Suggestions regarding NIST process

NIST should more fully leverage open, global standard bodies for its U.S. federal-focused work. While the U.S. Office of Management and Budget, via Circular A-119,[3] directs NIST to first consider the use of SDOs' voluntary consensus standards when the agency is developing standards for federal information systems, in many past cases, NIST has not found adequate standards in the cryptographic space, leading the agency to develop new standards for cryptography for U.S. federal information systems.

We strongly encourage NIST to devote more resources to contributing work to open, global SDOs that develop cryptographic standards used globally. NIST's cryptographic standards have a large impact commercially. As a result, where possible, NIST should adopt relevant international standards as the basis for Federal Information Processing Standards (FIPS).

By transitioning early work into the global work stream, NIST will achieve two positive outcomes. First, doing so will send a strong and much-needed message to global stakeholders about the U.S. government's commitment to a global, industry-led, voluntary, consensus-based, transparent, unbiased and trustworthy standards development process. Second, given the growing ubiquity of cryptography in both government and commercial markets, the work being conducted by global SDOs will increasingly be viewed as critical to driving trust in the Internet and e-commerce. Further, where NIST expects a broad range of industry to support its standards in their products, it will be increasingly important for that work to be progressed in open global SDOs.

[3] http://www.whitehouse.gov/omb/circulars_a119

We appreciate that this recommendation is not necessarily new or precedent-setting. In fact, NIST previously adopted two private sector-developed cryptographic standards for encrypting federal information in non-national security information systems. The Data Encryption Standard (DES), adopted by NIST as a federal standard in 1976, was based on work conducted by IBM during the early 1970s.[4] In 2001, NIST selected Rijndael, an algorithm submitted by two Dutch academics, to be the Advanced Encryption Standard (AES) for use by U.S. federal agencies.[5] We encourage the agency to refocus its efforts to participate in, and contribute technical expertise to, cryptographic work in SDOs to develop globally accepted, voluntary standards that can be used in the U.S. federal space.

Conclusion

Thank you again for the opportunity to share our views on these important issues. We appreciate NIST's commitment to working with global stakeholders to develop cryptographic standards. We look forward to continuing to work with you.

Sincerely,

Danielle Kriz
Director, Global Cybersecurity Policy
Information Technology Industry Council

Pam Walker
Sr. Director, Homeland Security
IT Alliance for Public Sector
Information Technology Industry Council

[4] See http://www.nist.gov/director/planning/upload/report01-2.pdf. NIST retired DES as a federal standard in 2001.
[5] See http://csrc.nist.gov/archive/aes/round2/r2report.pdf and http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.