NIST Cryptographic Standards Process Review

Tim Polk
NIST
November 7, 2013
Outline

• Brief Historical Perspective
• NIST’s Goals and Objectives in Cryptographic Standards Development
• Current Events
• Future Plans
Historical Perspective on Cryptographic Standards

• NIST published its first open, strong encryption standard in 1977 (DES) as FIPS 46
  – The DES standardization process included three Federal register notices and two public workshops

• Since 1977, NIST’s catalog of cryptographic standards has grown into a significant suite of algorithms
  – All were developed in consultation with the ever growing cryptographic community
Authority, Stakeholders & Impact

• NIST’s statutory authority for cryptographic standards is limited to protecting the US Government’s non-national-security systems, but our stakeholders are far more diverse
  – Voluntarily adopted within the public and private sectors

• Widespread support for these standards has benefited all participating communities
  – Increased interoperability
  – Widespread availability of security products
  – Reduced cost
NIST Goals, Objectives, and Role

• Ensure specifications are technically sound and have full confidence of the community
  – Ongoing process, since Moore’s Law and mathematical advances constantly erode the security margin of current algorithms
• To achieve this, we strive for a public, inclusive, and transparent process
• NIST’s role is balancing stakeholder needs as a technically competent and impartial player
NIST Process

• Since 1976, NIST has used a variety of processes to develop cryptographic standards and guidelines, including:
  – International competitions,
  – Adoption of existing standards, and
  – Development of new cryptographic specifications in collaboration with industry, academia, and government.

• To achieve inclusiveness and transparency
  – Public workshops
  – Solicit public feedback on draft standards and guidelines, and
  – Actively engage the cryptographic community.
Recent Events

• Recent news reports have created concern from the cryptographic community and other stakeholders about the security of NIST cryptographic standards and guidelines
  – “N.S.A. Able to Foil Basic Safeguards of Privacy on Web” (NYT, 9/5/13)
  – “How a Crypto ‘Backdoor’ Pitted the Tech World Against the NSA (WIRED 9/24/13)
• NIST reopened the public comment on SP 800-90A and two related draft documents, and strongly recommended that users stop using Dual_EC_DRBG.
  – "NIST Reopens Draft Special Publication for Random Number Generation Using [DRBGs] for Review and Comment" (NIST 9/13)
  – IAB Comment on NIST Recommendation for Random Number Generation (IAB, 10/13)
Process Review & Update

• Document and publish NIST process
• Invite public comment on NIST process
• Independent evaluation to review the process and suggest improvements
• NIST will update process as necessary to:
  – Maximize openness and transparency
  – Support the development of the most secure, trustworthy guidance practicable
  – Maintain confidence of all stakeholders
Review of Existing Work

• NIST will also review existing body of cryptographic work and the process through which it was developed

• NIST will invite new public comments and/or withdraw standards or guidance if appropriate
In Conclusion

• The NIST cryptographic standards process is founded on the same principles as the IETF process.
• The NIST process is the most inclusive cryptographic standards process, with global participation from the cryptographic community.
• It is essential to identify and incorporate those process changes that will allow NIST to continue effectively serving the global community.
• IETF participants can be an important voice in this process.
How Can IETFers Contribute?

• When the public comment period for the NIST process is announced, offer your perspective
  – Are there features that are not present (or not consistently present) in NIST process that would ensure openness or promote transparency?
• To be effective, what are the critical attributes for the independent evaluation panel? What should be the scope of their review?
Questions?