Updates on NIST Cryptographic Standards Program

Matthew Scholl
Andrew Regenscheid
Computer Security Division, ITL, NIST

ISPAB, February 2015

NIST

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Timeline

- News Reports and Subsequent Concerns over Crypto Standards, *September 2013*
- Publishes Draft NISTIR 7977, Cryptographic Standards and Guidelines Development Process, *February 2014*
- NIST Director Sends Charge to VCAT to Review Cryptographic Activities, *February 2014*
- VCAT/COV Review, *April- July 2014*
- Status Update to VCAT/ISPAB, *October* 2014
- Second Draft, NISTIR 7977, *January 2015*
- Proposed Withdrawal of 6 FIPS, *January 2015*

VCAT Recommendations

- ***Openness and Transparency***
  - Develop and implement a plan to further increase the involvement of the cryptographic community, including academia and industry…
- ***Independent Strength/Capability***
  - Strive to increase the number of technical staff…
- ***Clarification of Relationship with NSA***
  - NIST may seek the advice of the NSA on cryptographic matters but it must be in a position to assess and reject it when warranted.
- ***Technical Work, Development and Processes***
  - NIST work openly with the cryptographic community to determine how best to address… the number of specific technical recommendations.

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Openness and Transparency

- Revised NISTIR 7977 clarifies NIST’s role and outlines process improvements
- Public attribution of all inputs, including authorship, comments and responses
- Reaffirms NIST use of standards developed by SDOs, and its commitment to work with them on global acceptance of standards
- Provenance of all new/proposed crypto standards will be described

Independent Strength and Capability

- FY2015 budget directed an additional $6M to NIST cryptography-related work
  - Actively recruiting to Crypto Technology Group
  - Planned grants to expand relationships with academic and research institutions
- FY15 workshops to solicit input from researchers and industry

Clarification of Relationship w/ NSA

- All NSA contributions to NIST will be acknowledged
  - Authors will be clearly identified in accordance with NIST authorship guidelines
  - Comments on drafts will be made public
- Planned revision to NIST-NSA MOU

Technical Areas

- NIST IR commits to promoting algorithms with security proofs
- Developing intellectual property policy
- Draft NIST SP800-90A-rev1, Nov. 2014
- Elliptic Curve standards
- Proposed withdrawal of six FIPS released in Jan. 2015

NIST IR 7977

- Revised draft released Jan. 23, 2015
- Comment period ends March 27th
- Incorporated changes based on VCAT/COV review and initial public comments
- Added principles of usability and IP, expanded others
- Outlined 7-stage crypto standards lifecycle

Crypto Process Lifecycle

1. Identify and Evaluate the Need
2. Announce Intent
3. Consider Requirements and Solutions
4. Define Specific Plan/Process
5. Develop FIPS or SP (if applicable)
6. Global Acceptance- SDOs
7. Maintenance

Priorities

- Quantum-Resistant Cryptography
- Privacy-Enhanced Cryptography
- Usability
- Elliptic Curve Standards
- Lightweight Cryptography
- Hash function standards and guidelines

Upcoming Events

- IACR's *Public Key Cryptography*, March 2015
- *Workshop on Cybersecurity in a Post-Quantum World*, April 2015
- *Workshop on Elliptic Curve Cryptography Standards*, June 2015
- *Lightweight Cryptography Workshop*, July 2015

http://csrc.nist.gov/news_events/events.html

Discussion Items

- Strategic directions
- Outreach efforts
- Collaboration with SDOs
- Implementation of recommendations and standards/guidelines lifecycle

National Institute of Standards and Technology
U.S. Department of Commerce

More Information

NIST IR 7977 available at:

http://csrc.nist.gov

Contact Information

Matthew Scholl
Matthew.Scholl@nist.gov

Andrew Regenscheid
Andrew.Regenscheid@nist.gov