Background-Public Concerns and Initial Steps

Donna Dodson
Chief Cybersecurity Advisor
Information Technology Lab

Andy Regenscheid
Mathematician
Cryptographic Technology Group, CSD
Information Technology Lab

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

September 2013 News Reports

Sept 2013- NYT: *NSA Able to Foil Basic Safeguards of Privacy on Web*

"Cryptographers have long suspected that the agency planted vulnerabilities in a standard adopted in 2006 by [NIST]…"

"Classified N.S.A. memos appear to confirm that the fatal weakness… was engineered by the agency."

Reference: http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html

NIST Response on SP800-90A

- These articles referred to the Dual Elliptic Cure Random Bit Generator (Dual_EC_DRBG) in SP800-90A
- Based on these concerns, we reopened the SP800-90 series:
  - Released ITL Security Bulletin, September, 2014
  - http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf
  - Recommended against use of Dual_EC_DRBG
- Revised Draft SP800-90A to remove Dual_EC_DRBG
  - Released new draft SP800-90A in April, 2014
  - http://csrc.nist.gov/groups/ST/toolkit/800-90A-RFC.html
  - Currently out for 30 day comment period

Review of Crypto Standards Program

- These reports led to broader questions on the integrity of NIST's standards development process
- In November 2013, NIST announced a review of its cryptographic standards and guidelines program
  - Will consider improvements to development process
  - Include a review of existing body of work
  - See: http://csrc.nist.gov/groups/ST/crypto-review/
- Announced intent to include an independent organization

Purpose and Scope of NIST IR 7977

- As part of the review, Draft NIST Interagency Report 7977, *NIST Cryptographic Standards and Guidelines Development Process*
  - Released February 18th
  - *Available at*: http://csrc.nist.gov/groups/ST/crypto-review/process.html
- Draft explains how we develop standards
- Developed to facilitate public feedback through a public comment period on the draft
- Intended to serve as basis for the review of existing body of work

Overview of Crypto Standards Process

The draft identifies:

- Our Principles
- Stakeholders and Collaborators
- Standards and Guidelines Publications
- Development Processes
  - International Competitions
  - Adoption of Existing Standards
  - Development of New Standards
- Public Review and Outreach

Public Comments

- Public comments closed April 18th
- NIST received 18 comments
  - Available at: http://csrc.nist.gov/groups/ST/crypto-review/public-comments-nistir7977.pdf
- General themes:
  - Requests for more detail on procedures
  - Collaboration with international standards organizations
  - Call for greater transparency

More Information

NIST publications available at:

csrc.nist.gov

Crypto Toolkit:

csrc.nist.gov/groups/ST/toolkit/