NIST VCAT Report and Dual EC DRBG

John Kelsey, NIST

http://csrc.nist.gov/groups/ST/crypto-review/review_materials.html

http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf

What Happened?

- NIST and NSA wrote two standards on RNG
    - X9.82 and SP 800-90
- NSA provided Dual EC DRBG.
    - Looking back, many reasons we should have rejected or modified Dual EC DRBG
- News reports late last year:
    - Suggest that Dual EC DRBG has an intentional backdoor.
    - We told everyone to stop using it and put document back out for public comment.
    - Now removing it from 800-90A

http://csrc.nist.gov/groups/ST/crypto-review/review_materials.html

What are VCAT and COV?

- NIST asked VCAT (an advisory committee for NIST) to review what happened.
- Convened a panel of subject matter experts to review what went wrong with Dual EC and other NIST standards == COV
- We gave presentations and had discussions on our standards, and asked them for feedback.
- Result was the VCAT Report, including reports of individual COV members.

http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf

Process Improvements

- **Strong guidance from VCAT report**
  - Develop more independent crypto expertise
  - Rethink how we work with NSA
  - More open and transparent processes
- **What we're doing now**
  - Reviewing existing standards
  - Documenting and formalizing processes
  - Better tracking of comments and record keeping

http://csrc.nist.gov/groups/ST/crypto-review/

What's next for 800-90A?

- Revising 800-90A (second comment period)
  - Removing Dual EC DRBG
  - Fixing problem with KAT in Reseed
  - Fixing problem with requirements for additional input
- When this is finalized, Dual EC DRBG no longer approved

How can I find out more?

http://csrc.nist.gov/groups/ST/crypto-review/review_materials.html

http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf

crypto-review@nist.gov