Dual EC DRBG and NIST Crypto Process Review

John Kelsey, NIST

Three Stories

- How Dual EC got into our standard
- What we did when we realized what had happened
- What we're doing now

What's the Issue?

- NIST and NSA coauthored a set of standards on cryptographic random number generation.
- NSA provided Dual EC DRBG.
- *Many reasons* we should have rejected or modified Dual EC DRBG
  - Instead, we left it in.
- News stories based on Snowden disclosures came out.
  - Suggest that Dual EC DRBG has an *intentional backdoor* put in by NSA, and exploited in the field.

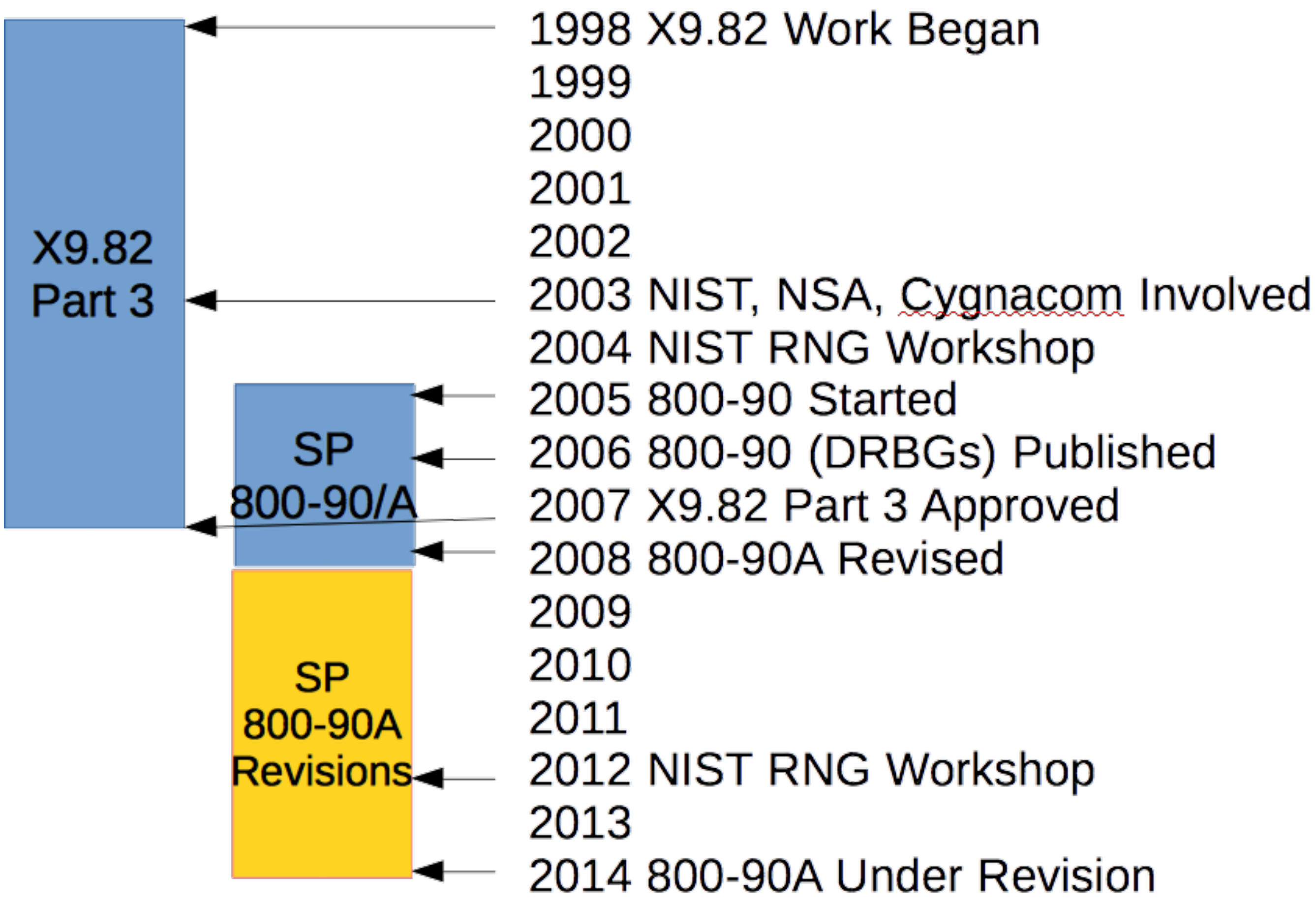
What Happened Next?

- Put out an ITL bulletin telling everyone to stop using Dual EC
- Put 800-90 documents out for comment
- Currently removing it from SP 800-90A
  - 2nd comment period just ended.
- Spent a fair bit of time trying to figure out:
  - What went wrong?
  - How to keep it from happening again.

What Are We Doing Now?

- Improving our process for writing standards
- Rethinking our relationship with NSA
  - NIST and NSA have different missions
- Hiring more cryptographers
- Building more links with academic crypto community
- Most important (and hardest to define): *Change in "corporate culture" in computer security division*.

Dual EC History



X9.82 Part 3

SP 800-90/A

SP 800-90A Revisions

1998 X9.82 Work Began
1999
2000
2001
2002
2003 NIST, NSA, Cygnacom Involved
2004 NIST RNG Workshop
2005 800-90 Started
2006 800-90 (DRBGs) Published
2007 X9.82 Part 3 Approved
2008 800-90A Revised
2009
2010
2011
2012 NIST RNG Workshop
2013
2014 800-90A Under Revision

X9.82 and SP 800-90

- NIST and NSA worked together on two different standards for cryptographic random number generation
  - X9.82 (1998-2007)
  - SP 800-90 (2005-Present)
- Two processes ran in parallel
  - X9 dragged on for years with little progress
  - Finally got going around 2003
  - Two processes ran in parallel, same authors

DRBGs
Deterministic Random Bit Generators

- Cryptographic random number generators come in two parts:
  - Unpredictable processes used to generate a *seed*
  - Algorithm to generate *random bits* from seed.
- ***DRBG = Deterministic Random Bit Generator***
  - *Algorithm* for generating random-looking bits.
  - Specified in X9.82 Part 3 and SP 800-90A.
  - Should produce outputs nobody can distinguish from random bits.
- In SP 800-90A:
  - *NSA provided two: Hash DRBG*, Dual EC*
  - *NIST provided two: CTR DRBG, HMAC DRBG*

* *Design was extensively modified by NIST*

Dual EC DRBG
Dual *Elliptic Curve* DRBG

- DRBG provided by NSA
- Security based on number theory problem
- Defined for three curves (three security levels)
- For each curve, some public parameters (P,Q) defined as part of DRBG definition.

Dual EC DRBG: P and Q

- Dual EC DRBG’s definition requires choosing some parameters: (P,Q)
  - Elliptic curve points.
- It is possible to choose (P,Q) so that you know a backdoor for the DRBG.
  - NSA is alleged to have done this.
- It is also possible to choose (P,Q) so that you can prove you don’t know a backdoor.
  - We have a mechanism to do this in our standards, but it seems never to have been used.

Issues with Dual EC DRBG

- **Bias** – Dual EC DRBG has a slight statistical bias
  - Theoretical weakness when DRBG is used to generate keys.
  - But it violates our requirements for DRBGs
- **Possible Backdoor** – (P,Q) may have been generated to allow NSA to know a backdoor.
  - This would be a practical (and very important) weakness

*Dual EC DRBG **should not** have been included in X9.82 or SP 800-90 in current form.*

What Went Wrong?

Dual EC: What Went Wrong?

- Dual EC DRBG had security issues that should have kept it out of X9.82 and SP 800-90.
  - Bias (from not throwing away enough bits)
  - Possible backdoor in (P,Q)
- Both issues identified during standards development process.
- Changes made to the standards failed to adequately address them.

Four Issues from our COV Presentation

1. NIST-NSA Relationship
   - *Relied on NSA for expertise we lacked on ECC*
2. Insularity of Editing Committee
   - *Ignored or minimized feedback from outside*
3. Standards Group Dynamics
   - *Dual EC had a champion on X9.82 editing committee*
   - *Wanted existing implementations to comply with standard*
4. Recordkeeping and Project Management Issues

What Happened Next?

Timetable

- **September-November 2013:**
  - News Reports and Subsequent Concerns over Crypto Standards, September 2013
  - Internal Discussion at NIST by NIST Staff and Leadership, Fall 2013
  - ITL Bulletin advising public to stop using Dual EC, 800-90 series out for public comment

- **February 2014:**
  - NIST Publishes Draft IR 7977, Cryptographic Standards and Guidelines Development Process, February 2014
  - NIST Director Sends Charge to VCAT to Review Cryptographic Activities, February 2014

- **April-July 2014:**
  - VCAT Subcommittee Forms Expert Committee of Visitors (COV), April 2014
  - NIST Conducts Series of Briefings to VCAT Subcommittee and COV, May 2014
  - COV Submits Individual Reports to VCAT Subcommittee, June 2014
  - Full VCAT Provide Consensus Recommendation to NIST Director, July 2014.

VCAT Report

- NIST management 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

Summary of 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.

What Are We Doing Now?

Process Review Overview

- The Dual EC disaster led to a rethink of how we manage computer security standards at NIST.
- We're working on a number of changes to our procedures.
- Some of these might make attacks on us like the one in SP 800-90 harder.
- Others will just make us less likely to make mistakes, and will make the documents easier to review.

Authorship and NSA

- We've had documents where NSA coauthors weren't listed as authors, but instead in the "acknowledgements" section. (SP 800-90A is an example.)
- Problem: This makes it difficult for readers of our documents to know whether NSA was involved.
- Solution: Future documents will require all coauthors to be listed as coauthors.

NSA Contributions to NIST Standards

- NSA has contributed to NIST guidelines in several ways:
  - Coauthoring and commenting on publications
  - Contributing algorithms, e.g., SHA-1, SHA-2, DSA, AES Key Wrap
- NIST will clearly identify any NSA contributions
- We will encourage NSA to bring proposed algorithms to conferences and standards organizations
  - e.g., SIMON, SPECK
- NSA-developed algorithms will require public review and analysis to be considered for inclusion in NIST standards/guidelines

NIST Standards and Public Comment Periods

- FIPS and Special Publications follow a process like:
  - Draft version is published
  - 30-90 day public comment period
  - Comments received in period are addressed somehow by writers of the standard
- This is a major way we get feedback on our standards.

Comment Resolution

- Past: Comments handled differently depending on author preferences.
- Future: Comments handled consistently
  - Public comments will be made public
  - Every comment will be addressed in public
- This came up in reviewing how some comments on 800-90 were addressed.

Informal and Anonymous Comments

- Informal comments: Often useful feedback comes informally.
  - Personal conversation
  - Comment on a mailing list
- Private Comments: Public comments are better, but not everyone wants to make a public comment.
  - Some comments might be under NDA

We're still working out how to capture these and make them more-or-less public

Out of Season Comments

- Comments sometimes come in about documents that aren't out for public comment.
  - Errors or bugs
  - Attacks
  - Suggestions for future revisions
- Right now, it's not so clear where to send such comments.
- In the future, we plan to keep comment email addresses open for our documents all the time. Like rbg-comments@nist.gov

Recordkeeping

- In the past, our project management on documents has been ad-hoc.
- Different authors handled things their own way.
- It's often quite hard to find old versions of documents, notes, meeting minutes, internal analyses, etc., for old documents.
- All this came up in trying to work out what had happened to SP 800-90.

Recordkeeping (cont’d)

- We're planning to move to a more formal mechanism for managing projects in CSD.
  - Start a project with security requirements or problem statement
  - Keep intermediate documents, notes, internal analyses, etc.
- Not clear what technology we will use...
- ...but email is a lousy project management tool.

Public Communications and Transparency

- CSD works on a lot of documents, and it's not always easy for anyone to know what's going on.
- Problem: We lean heavily on public crypto community for review.
- Currently working on redesign of webpage to try make it easier to find information on each project:
    - Current document
    - Previous public comments and old versions of documents.
    - Supporting documents (like slide presentations)
    - Contact information for out of season comments.

NIST IR 7977 and Process Review

- NIST IR 7977 describes our process review
- Feb 2014 draft--mostly principles, not specifics.
- Current draft (early 2015)--more specific details
- Many issues being discussed:
  - Project management lifecycle- From how we identify standards efforts, to developing standards, to maintaining existing standards.
  - How we engage stakeholders in government, research community, and SDOs.
  - Intellectual property in proposed algorithms/standards

So, Will This Stuff Stop Another Dual EC From Happening?

- These changes might help, but mostly they're not enough
- What will help?
- Change in corporate culture at NIST
    - Very different interactions with NSA now than two years ago
- More independent crypto expertise
- Recognition of the threat environment we live in

Threat Environment?

- News reports from the last few years show that crypto standards and products are being targeted by serious attackers.
- Question: How do we develop processes to resist that kind of well-funded attack?
- Insider attacks on standards bodies
  - We’re used to IP-related “attacks”, not so much to trying to weaken standards for exploitation.

Summary

- Dual EC is bad, don't use it.
- We've spent a lot of time figuring out what went wrong and how to prevent it happening again.
- We've got a bunch of process improvements in the works.
- We're going to be hiring more cryptographers
- We live in a tough threat environment for crypto standards and product development.

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

Acknowledgements

- Lots of cryptographers outside of NIST have commented on these two standards, before and after the news stories based on Snowden's leaks, and I've drawn heavily on their comments and analyses.

Dan Bernstein, Dan Brown, Niels Ferguson, Kristian Gjosteen, Matt Green, Tanya Lange, Bruce Schneier, Berry Schoenmakers, Dan Shumow, Andrey Sidorenko

With apologies to anyone I've left out.

Bonus Slide: Elliptic Curves

- Lots of recent discussion about the NIST recommended elliptic curves
  - There are no known attacks of cryptographic significance on the NIST curves when implemented as described in our standards
  - But, 15 years has past, and newer curves offering better performance or more resistance to side channel attacks have been proposed.
- NIST is re-examining its current ECC mechanisms
  - Very interested in current TLS IETF WG / CFRG effort to select new curves
  - Interested in community's thoughts on current NIST curves
- Next steps
  - Will solicit comments on FIPS 186 and elliptic curves
  - Planning workshop on ECC standardization – tentatively scheduled June 11-12 in Gaithersburg