Information Security and Privacy Advisory Board Past and Future: Some Comments

Susan Landau
Distinguished Engineer
Sun Microsystems Laboratories

Control of Federal Civilian Computer Security Belongs to a Civilian Agency

- *Brooks Act (1965): The Secretary of Commerce to "make appropriate recommendations ... relating to the establishment of Federal automatic data processing standards." Totally non-controversial law. Called FIPS, fit in with NIST's role as standards organization.*
- *Computer Security Act (1987): put NIST in charge of federal civilian agency computer security, established CSSPAB.*

Then Along Came the Clipper Chip ...

- April 9, 1993: Announcement of key escrow for encryption of voice, fax, and computer information over a telephone system.
- 80-bit algorithm (DES was 56 bit).
- Keys split and escrowed with two agencies of the federal government (eventually decided to be NIST and Department of Treasury Automated Services Division).
- Keys only available under “legal authorization.”

CSSPAB Role

- Clipper announced in April 1993.
- CSSPAB holds six days of hearings on Clipper in May and June 1993.
- Speakers include Computer and Business Equipment Manufacturers Association, ACLU, Addison Fischer (Fischer International Systems Corp.), numerous consultants. There was an overwhelmingly negative response to escrowed keys, a secret algorithm developed in classified setting, the lack of transparency ...

CSSPAB Resolutions

- CSSPAB issues resolution 93-5 on EES:
  o A convincing statement of the problem that Clipper attempts to solve has not been provided.
  o The Clipper/Capstone proposal does not address the needs of the software industry.
- CSSPAB issues resolution 93-6 on EES: [I]n deciding cryptographic policies and standards in the US ... we believe the scope of that review needs to include adequate industry input."

What Happened to Clipper?

- Clipper arose out of AT&T plan to market secure phones; AT&T envisioned a large market.
- By fall of 1995, sales were about 17K, largest block being 9K bought by FBI to seed market.
- “Clipper is dead.”
- Advanced Encryption Standard: competition started in 1997, completed in 2001.
- AES: 128-,192-, 256-bit key, accepted internationally.

What happened next?

- We learned some things about NSDD-145, DSA, Clipper, and the efficacy of wiretaps in criminal investigations.
- The creation of DHS.
- Computer Security Division stayed at NIST.
- CSSPAB becomes ISPAB.
- FISMA and increase of CSD budget.
- RealID, PIV, implementations of the Privacy Act, privacy breaches, CPOs, FISMA compliance, industry initiatives (Identity Management, TCG), ...

What are the big issues we are facing now?

What are the big issues we are facing now?

- Cyber Initiative: NSA to monitor Internet-based networks supporting critical infrastructure (electric power grid, subways, nuclear power plants) to prevent unauthorized cyber intrusion/attacks.
- Done in conjunction with DHS.
- Details highly classified.
- Isn't this civilian computer security? Where is NIST on this initiative?

Susan Landau
susan.landau@sun.com