

IAB/IESG Statement on Cryptography

Steven M. Bellovin

smb@research.att.com

908-582-5886

AT&T Labs Research

Murray Hill, NJ 07974

What's an IESG?

- Internet Engineering Steering Group
- Manages the development of Internet standards.
- Each IESG member oversees a particular area (Operational Requirements, Security, Routing, etc.)
- Currently, one of thirteen members is non-U.S. About half are from industry; the rest from academe.

What's an IAB?

- Internet Architecture Board
- Provides architectural oversight for the Internet's protocols.
- Acts as an appeals body from the IESG.
- Currently, four out of twelve members, including the chair, are non-U.S. Most of the current U.S. members work for industry, not academe or government.

What We Said

- No export controls on cryptography.
- No key length limitations.
- No mandatory key escrow.
- No restrictions on use of cryptography.

The statement was carefully crafted to apply equally to all countries around the world. It is very specifically not restricted to the U.S. Nor, of course, was the U.S. exempted.

Why We Said This

- The Internet cannot be secured without cryptography.
- Knowledge of how to use cryptography is world-wide, and cannot be “erased” by government fiat.
- Export controls serve solely to put exporters at a disadvantage.
- Usage controls afflict anyone in such countries.
- Escrow mechanisms inevitably weaken security.
- Export and usage controls are restricting the deployment of security technologies at the same time as the Internet is growing and attacks are increasing.

Key Size

- Limited key sizes do not keep out many of the attackers we're concerned about (i.e., governments, some large corporations).
- Current exportable systems are attackable by students. DES is almost within range. (Imagine a DES-cracker embedded in a popular Java applet.)
- Many conversations need to be protected for years to come.

Key Escrow

- Escrow system always weaken security: there is now a new place to attack.

“Why is it necessary to destroy yesterday's [key] . . . list if it's never going to be used again?”

“A used key, Your Honor, is the most critical key there is. If anyone can gain access to that, they can read your communications.”

(trial of Jerry Whitworth, a convicted spy.)

- Key recovery, though useful for files, is never applicable to network conversations.
- The concepts of a “key certifying agency” and a “key escrow agency” must not be confused.
- Some forms of key escrow are incompatible with “perfect forward secrecy”.


What About the Bad Guys?

- There are very few wiretaps actually used in the U.S. (less than one thousand/year).
- Very few bad guys (spies, terrorists, drug dealers, etc.) follow the rules anyway.
- From an international perspective, one nation's spies are another nation's patriots. Would the U.S. share escrowed keys with a nation we suspect of spying on our commercial traffic? Would we want victimized companies to use weak keys? Would the other nation want such companies to use strong keys?

Does this Contradict the NAS Report?

- We essentially agree on key length, key escrow, and usage controls.
- We disagree somewhat on export.
- But the IAB and IESG are international bodies; from that perspective, export controls don't apply.

The Latest Government Scheme

- It blurs the distinction between transient conversation keys and long-term file storage keys.
 - The easing of restrictions on exports is conditional and temporary.
 - Some of the technology involved appears to be dubious — it adds new vulnerabilities, and seems to make it easier for the bad guys to override it.
-  In my opinion, it confirms our objections, rather than answering them.

Conclusions

- Cryptography is a very powerful tool to secure the Internet.
- The prospective gains from restrictions on cryptography do not ease the harm that will result.
- It is hard to find a solution that will work well from the perspective of all countries involved.