[Date Prev][Date Next][Thread Prev][Thread Next][Date Index][Thread Index]

PKP sellout = betrayal

- *To*: cypherpunks@toad.com
- *Subject*: PKP sellout = betrayal
- *From*: ""L. Detweiler"" <ld231782@longs.lance.colostate.edu>
- *Date*: Sun, 13 Jun 93 00:00:45 -0600
- *Cc*: ld231782@longs.lance.colostate.edu
- *In-Reply-To*: Your message of "Sat, 12 Jun 93 08:01:05 EDT." <9306121202.AA16880@toad.com>

```
S. Bellovin <smb@research.att.com>
>I don't see the hand of conspiracy here; rather, I see an encouraging
>trend, that the private sector is able to compete in cryptographic
>competence with NSA.
>
>I am encouraged by the pledges to allow non-commercial use -- note the
>lack of any RSAREF-like interface -- and to engage in non-discriminatory
>licensing.

By cooperating with NIST on DSA and Clipper, they are implicitly
sending the message that the poorly-to-outrageously directed standards
making processes for both are wholly acceptable assuming PKP directly
profits.  That is, that is the weak `nonconspirational' interpretation.
The conspirational interpretation is that this announcement is just a
blatant indication that PKP, in addition to NIST, is controlled by the NSA.

Let me remind everyone that Capstone has a yet-unspecified exchange
protocol. Denning suggested on RISKS that Diffie-Hellman (covered by
PKP patents) `could be used'.  There is some serious evasion going on
here. If Capstone is already built, with a public-key algorithm
installed, it suggests that PKP has been cooperating on the
Clipper/Capstone proposals all along.  It will be most interesting to
hear announcements on Capstone that announce its key exchange mechanism.

PKP `had' the ability to murder Clipper/Capstone in its crib if it so
desired, more so than any other single nexus, by denying the right to
use public key algorithms (on which it now has a strangling,
monopolistic lock). Gad, I can't believe it didn't occur to me to lobby
them to do so. In retrospect, it wouldn't have done anything more than
heighten the inevitable betrayal.

Maybe Mr. Bellovin can clarify how this agreement represents an
`encouraging trend in the private sector to compete with the NSA' --
Good lord man, not unless you think that PKP represents the entire
private sector in cryptographic applications. Uh, touche' -- you do and it does.

Does anybody feel like raiding PKP dumpsters? :(

P.S. doubt P.R.Z. will be in a docile mood after hearing this one...
```

- **References**:
  - **Re: PKP sellout?**
    - *From:* smb@research.att.com

- Prev by Date: **what happens when you reply to nobody@cicada.berkeley.edu ?**
- Next by Date: **alt.whistleblowing**
- Prev by thread: **Re: PKP sellout?**
- Next by thread: **Re: PKP sellout?**

- Index(es):
  - **Date**
  - **Thread**