Ensuring Strong Keys

Without introducing new vulnerabilities

Phillip Hallam-Baker

Comodo Group Inc.

IPR Statement

- Rights currently reserved.
  - [We don’t know what they are]
  - [We did apply for a patent]

Debian Weak Keys

```
// Purify complains
// MD_update (&m, buf, j);
```

Naïve Solution

- Alice can’t pick a good public key
  - Let Henry provide trustworthy hardware

- No
  - Henry might get it wrong
  - Henry might defect

Naïve Solution II

- Alice can’t pick a good public key
  - Let Carol (CA) do it for her

- No
  - If anything happens, Alice will blame Carol.
  - Carol might get it wrong
  - Carol might defect

Proposal

- Alice generates a private key pair K_A
- Bob generates a private key pair K_B
- Bob passes both halves to Alice via a secret channel
- Bob calculates new key pair $K_{AB} = K_A \text{ ☺ } K_B$
  - K_{AB} is strong if either K_A or K_B is
  - Bob can defect if and only if Alice chose a weak key
  - Bob can improve the security of the key, but not weaken it.

In Diffie Hellman (non EC)

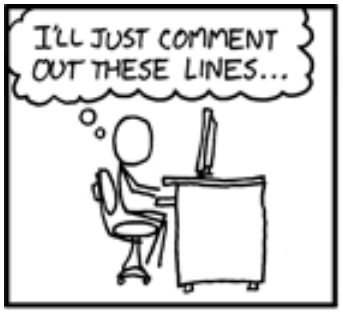
Create a Joint key from Left and Right

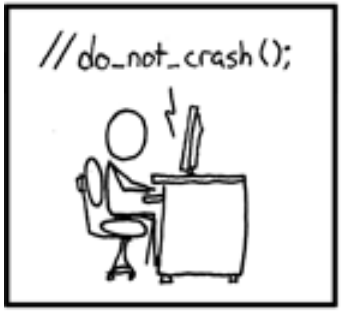
- KR = R, eR mod p
- KL = L, eL mod p
- KJ = J, eJ mod p
  - J = R + L
  - eJ mod p = eR+L mod p
    - = (eR mod p . eL mod p) mod p

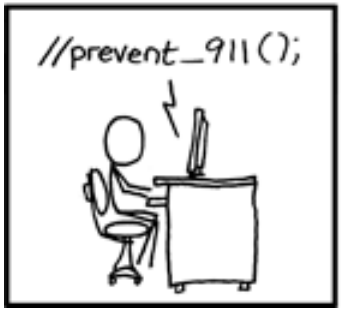
Conclusion

- We can and we should address the weak key problem
- The transition to EC is also a transition to DH
  - This may be the more interesting bit.

Next…







IN THE RUSH TO CLEAN UP THE DEBIAN-OPENSSL FIASCO, A NUMBER OF OTHER MAJOR SECURITY HOLES HAVE BEEN UNCOVERED:

AFFECTED SYSTEM	SECURITY PROBLEM
FEDORA CORE	VULNERABLE TO CERTAIN DECODER RINGS
XANDROS (EEE PC)	GIVES ROOT ACCESS IF ASKED IN STERN VOICE
GENTOO	VULNERABLE TO FLATTERY
OLPC OS	VULNERABLE TO JEFF GOLDBLUM'S POWERBOOK
SLACKWARE	GIVES ROOT ACCESS IF USER SAYS ELVISH WORD FOR "FRIEND
UBUNTU	TURNS OUT DISTRO IS ACTUALLY JUST WINDOWS VISTA WITH A FEW CUSTOM THEMES