Blog Export: c0t0d0s0.org, http://www.c0t0d0s0.org/

Friday, September 6. 2013

Broken cryptography

There was once a comment stating "If privacy is outlawed, only outlaws will have privacy". I would change that "If privacy is broken to catch terrorists, only terrorists will have privacy". I have my doubts that any interesting data transmitted by terrorists will be transmitted by communication means that are breakable. There are unbreakable means of encrypting and decrypting data, you can even look them up in Wikipedia: One-time pad. Perhaps using a Lady Gaga CD as a key ... that music sound pretty random to me And i assume that terrorists can read wikipedia as well as the normal people. So where are we now: The cryptography used by normal people as defined by standards is broken by agencies, however cryptography unbreakable is still available to not-so-smart-bombs with semtex underwear respectively the people sending them ...

Posted by Joerg Moellenkamp in English, Privacy at 10:21

Time to change the kssl default from RC4 to AES I'd say…

Some -c examples in the manpage would be nice as well.
Anonymous on Sep 6 2013, 21:23