500 bits – Implementor’s Lament

Lyrics: Daniel J. Bernstein, Tanja Lange

Performance: Daniel J. Bernstein, Geoffroy Couteau, Carl Ellison, Rémi Géraud (guitar), Becca Kreuter, Tanja Lange, Kristin Lauter, Christof Paar, Tom Roeder, Mike Rosulek (guitar)

Original by: Hedy West
If you implement a stack that allows downgrade attacks, Eve will roll your key size back to 40 bits.
If you implement a stack that allows downgrade attacks, Eve will roll your key size back to 40 bits.

40 bits, 40 bits, 40 bits, 40 bits, RC4 with 40 bits is all you get.
If your client check is weak then you’re vulnerable to FREAK say Hello to RSA 500 bits.
If your client check is weak then you’re vulnerable to FREAK say Hello to RSA 500 bits. 500 bits, 500 bits, 500 bits, 500 bits, RSA 500 bits is all you get.
Unauthenticated acks give cross-protocol attacks. LogJam breaks 500 bits of DHE.
Unauthenticated acks give cross-protocol attacks. LogJam breaks 500 bits of DHE.

500 bits, 500 bits, 500 bits, 500 bits, DHE 500 bits is all you get.
If you implement a stack that allows downgrade attacks, Eve will roll your software back to export suites.