Deprecating RC4 and 3DES for Kerberos

Ben Kaduk <kaduk@mit.edu>

IETF 92, Dallas, TX, USA

Kitten WG

draft-kaduk-kitten-des-des-des-die-die-die

- Well, maybe it should have been draft-kaduk-kitten-arcfour-please-go-away (credit: ghudson)
- But, maybe not: can the NSA decrypt RC4 in real-time?

Why both?

The last two non-CFX enctypes:

- Non-CFX enctypes do not use acceptor subkeys
- Almost lets us move RFC 1964 to historic
  - But not quite, since it defines the string form of principal names (anything else?)
- No context deletion tokens
- But really, both are getting to be weak(-ish)

Why RC4?

- string2key is really bad
  - One rainbow table for all users, anyway, from md4
- Keystream biases
  - No published way to get may repeated encryptions (?)
- Other attacks against the cipher (persistent rumors)
- Cross-protocol NT hash issues
  - I don’t know the full scope of the issues

Why will eliminating RC4 be hard?

- Windows XP, Server 2003
    - Going EoL real soon now
- Cross-realm keys are still hard to update
- ???

Why triple-DES?

- String2key is n-fold-based; untrusted
- 64-bit block size, so ciphertext collisions expected (birthday attack) after 2^{32} encryptions
- Slow
- Not actually much else
- (But anything recent that implements 3DES also does AES)

Thoughts?

- Should we deprecate both of them now?