Update on draft-irtf-cfrg-dragonfly

Dan Harkins, Aruba Networks

IETF 87 Berlin

What is this draft again?

- Defines the *dragonfly* key exchange in a generic fashion (much in the same way that RFC 2631 defined Diffie-Hellman)
  - Authentication using only a password
  - Resistant to dictionary attack
  - A true peer-to-peer protocol– either side can initiate and both sides can initiate simultaneously

Where the draft is now

- Version -00 was somewhat rushed:
  - Acknowledgements section: “This template was derived from an initial version written by Pekka Savola and contributed by him to the xml2rfc project.”
  - A few typos
  - Did not mention requirement to validate received public keys
- Version -01 is current draft, addresses errors and omissions above

Where the draft should go

- Rene Struik has commented on -01
  - Another typo
  - Need a section describing salted passwords, if applicable
- IEEE 802.15.9 expressed interest in using this key exchange in the framework they are defining
  - Need to ensure the draft is defined in a way that can be useful to that group
  - Should mention inclusion of nonces in the mix, if the protocol has a way of exchanging them
- A version -02 is definitely needed!
  - Perhaps that version will be ready for WGLC