Update on TLS-pwd

Dan Harkins

IETF 84

Vancouver, BC, Canada

What is it?

- Certificate-less TLS ciphersuites
- Mutual authentication using a password/phrase
  - Not susceptible to dictionary attack
  - Misuse resistant!
- Advantages over SRP
  - Supports ECC
  - Domain parameter set is not fixed
  - More crypto-agile
- Being specified for use in smart grid by Wi-Fi Alliance
- Useful with EST: parlay a short, simple string into a certificate.
  - You don't need a certificate to get a certificate.

Minutes from IETF-83

Eric polls the group:

1. do people think its valuable to have a new cred mechanism that has advantages over SRP?
2. What would it take to convince ourselves that this would be the right mechanism?

Only positive hums for the first one so Eric wants to ping David McGrew afterwards to take up with CFRG for second question

(emphasis mine)

So then what happened?

- Presentation at CFRG meeting at IETF-83
- Asked for review on the CFRG list
  - Small amount of discussion
  - Nothing definitive
- Request from chairmen of CFRG to produce an I-D that describes the exchange (not tied to a particular protocol)
  - Similar to RFC 2631 (Diffie-Hellman key exchange)
  - Informational track RFC since that’s all IRTF can produce
- How does the WG interpret this? Positively, I hope.

Requests

- Please adopt the draft as a WG item
  - Produce a Standards Track RFC
  - Get code points for the ciphersuites
- Interoperate with me!
  - I have an implementation (not all of the ciphersuites in the draft though)
  - I can make the server-side code available on a publicly accessible computer to test your client
  - I'd like to test my client-side code against your server