draft-irtf-cfrg-pake-reqs-00

Jörn-Marc Schmidt
Dan Harkins

What? Why? When?

- Draft to ultimately express consensus of RG on requirements for PAKEs submitted to CFRG
- To add some structure to an anticipated discussion when we get around to discussing PAKEs– oh, and the chairmen asked too
- To be submitted *Real Soon Now*– hopefully within a month

What's it Look Like?

- A discussion of different types of PAKEs
  - password storage and augmented versus balanced
  - transmitting encrypted public keys versus unencrypted pubic keys
- A brief note about password authenticated key *distribution* being separate from key *establishment*
- Mention of multiparty PAKEs
- A discussion of the threat environment and what it means for a PAKE to be secure
- A list of (hopefully) non-controversial requirements

Requirements?

- A PAKE scheme MUST clearly state its features– e.g regarding balanced versus augmented
- A PAKE scheme SHOULD come with a security proof and clearly state its assumptions and models
- It SHOULD be possible to implement the PAKE scheme in constant time
- For a PAKE using ECC, the scheme SHOULD address mapping of bitstrings to field elements and back, where appropriate
- Optimizations to improve performance MAY be mentioned