CFRG discussion on ChaCha20

mcgrew@cisco.com

TLS Working Group @ IETF 89

Background

- TLS chairs asked CFRG chairs to provide an update on ChaCha and Poly1305 (2/23)
  - CFRG chairs offered input on new ECC
- CFRG agenda included questions

  http://www.ietf.org/proceedings/89/slides/slides-89-cfrg-0.pptx
- We suggest that the request from TLS to CFRG be formalized
  - To what questions should we seek answers?

ChaCha20 and Poly1305

- Points made in CFRG
  - ChaCha20 should not be used as a stream cipher
  - AEAD construction is preferable
    - draft-nir-cfrg-chacha20-poly1305-00 should be advanced and reviewed more
  - The composition of ChaCha and Poly1305 is novel and needs review
    - Let's seek input from Dan Bernstein
- Hum on "do you think this function is adequately secure to be used in TLS ciphersuites?"
  - Few agreed, 1 or 2 disagreed, many felt unsuited to respond
  - Note that the room has a lower proportion of cryptanalysts than list
- Suggestion:
  - Proceed with draft-nir-cfrg-chacha20-poly1305-00, expecting tweaks, with a one month period to review draft-nir-cfrg-chacha20-poly1305-00 in CFRG

New ECC

- Curve25519
  - draft-josefsson-tls-curve25519-01
  - Montgomery form
  - Not suitable for signatures
- draft-ladd-safecurves-01
  - Montgomery and Edwards form
  - DJB: safecurves not all equally well performing

CFRG Conclusion on New ECC

- Focus on doing **one** new curve family
- Aim for reusability beyond TLS (SSH, IKE, …)
- CFRG should have an interim meeting dedicated to the discussion of New ECC
  - Teleconference will be accessible to more CFRG members
  - 20+ interested in participating
  - Early April (one month to prepare)
  - Identify goals in advance
  - Solicit written input and presentations

What questions should we ask CFRG?

- Should be specific to drafts when possible
- Should be written down
  - Email sent to CFRG and TLS list
  - Could be debated on list and finalized by chairs
- Should have a cutoff date (~3 months)
- Should consider general suitability, and not just security
- Should provide goals, or accept input on goals