CFRG reporting back to TLS WG

IETF 90, Toronto

Kenny Paterson, CFRG co-chair

State of Play

- CFRG list announcement July 15th relaying request for new curve recommendations from TLS WG chairs.

- CFRG chairs announced 2-part process:
  - Reach rough consensus on requirements (2 wks).
  - Reach rough consensus on curves (4 wks).
  - Finalise recommendations (2 wks).
  - Roughly 40 e-mails on list since.

State of Play

- CFRG@IETF90:
  - Wednesday 1300-1500
  - Roughly 90 minutes presentation + discussion on new ECC.
  - Overview talk on ECC old and new from Tanja Lange (TU Eindhoven).
  - Talk on NUMS curves from Brian LaMacchia and Craig Costello (Microsoft).
  - Talk on Curve25519 and friends from Dan Bernstein (UIC/TU Eindhoven).
  - Lively Q&A/discussion, continued at ISRG dinner.

Emerging Areas of Consensus on Requirements

- Protection against side-channel attacks strongly desired.
- Basic elements of curve selection – defined over prime field; prime or near-prime order; twist security.
  - Not always needed, but we can achieve these at no real cost.
- Need to support existing algorithms.
  - Strong steer from TLS WG.
  - ECDHE, EC-DSA, and maybe ECDH.
  - Interop with existing wire formats desirable, not essential.
  - Versus potential perf. gains from adopting new algs
- Need for *rigidity* in curve generation process.
  - Trustable curve generation process is important.
  - It's a primary motivation for this work.
  - How much rigidity is enough to satisfy public opinion?

Emerging Areas of Consensus on Curve Form

- Switch from Weierstrass-only form to alternative forms (Montgomery/Edwards/twisted Edwards)
  - Deployability of new W.-only form curves not significantly easier, even though there's a large deployed code base for W.-only form curves.
  - Much easier side-channel protection without perf. sacrifice using alt. forms.
  - Co-factor > 1 for alt. forms has potential for implementation errors.
  - Overall, *tenatively,* alt. forms seem to be the way to go.

- Growing realisation amongst non-experts.
  - It's complicated!

Current Areas of Debate

- Specific implementation detail at 128-bit security level:
  - (Montgomery + twisted Edwards for ECDHE + point conversions) versus just twisted Edwards for ECDHE?
  - Related implications for wire format.
- What does *ephemeral* mean?
  - Server-side: every key exchange or every 10s or every hour?
  - Has implications for selection of curve form (costs of fixed base versus variable base computations).
- Actual choice of specific curves.

Summary (personal view)

- In terms of perf+security, there's not much to choose between the competing alt. (i.e. non-W.-only) curve proposals at each security level.
- We're making progress; *rough* consensus on requirements should be possible.
- Getting consensus on selection of curves will require some give and take from competing proposers.