SRP transport problems

Ted Lemon <elemon@apple.com>

SRP is (almost) published, but...

We've run into some issues

- First big customer of SRP is Thread, which is a constrained network
- SRP packets are pretty big, and are sent over UDP (oops)
  - This means they can't be segmented, and large packets are way less reliable
- IoT networks are steady state: SRP registrations often happen because something changed
  - Synchronization events produce thundering herds of SRP registrations
  - This leads to immediate congestion collapse, which takes a while to recover from

How to improve things

- Packet size
  - 6lowpan-style compression: get rid of redundant data, make fields smaller.
  - Assume registrar has key when that's likely
  - Can we send partial HMAC hashes?
- Transport
  - Send an initial very small probe with hashes of intended registrations
  - SRP registrar can reply with a schedule: don't respond for N milliseconds
  - SRP registrar can indicate whether any of its hashes match hashes sent by requester

Status of this work

- Lots of hot air
- No implementations yet