Protocol Proposal: draft-erb-lurk-rsalg

Rich Salz
Akamai Technologies

Terminology

- “All the good ones are taken”

Client ←→ Server ← → KeyOwner

- Don’t care; whatever the WG/BoF decides
- *But do decide early and stick to it.*

Our Goals

- Don’t be a signing oracle
- Stronger protection for session encryption keys
- Don’t lose PFS

Protocol Overview

- TLS presentation syntax
- Request/response
- Request ID repeated in response
  - Allows streaming, pipelining, etc
- Connections between Server and KeyOwner SHOULD (may be MUST) mutual-auth TLS with strong cipher-suite

Static RSA Details

- It’s kinda like DH ☺
- Server picks N, uses SHA256(N) as its random and sends N to KeyOwner
- KeyOwner uses SHA256(N) in generating PRF
- … future access to KeyOwner protects traffic since adversary needs N, not SHA256(N)

Session Encryption Key Details

- Add SHA(private-key) into KDF
  - Protects owner-A from attacks by owner-B
- Server sends salt
  - Server can ensure unique sessions

Next Steps

- If WG creates and WG adopts, then …
  - Adding ECC variants makes sense
  - Adding TLS 1.3 makes sense
  - What else makes sense?
- We filed an IPR declaration for what is currently documented (RF with cross-license)
- We have other IP in this area; IPR TBD