Randomness Improvements for Security Protocols

Nick Sullivan, Cas Cremers, Luke Garratt

draft-sullivan-randomness-improvements-00

Problem

- System-level randomness failures

- Ephemeral Diffie-Hellman protocols (TLS, IKE, more) could be vulnerable to broad-scale compromise

Previous Solutions

- Include a long-term secret as part of the randomness derivation
- NAXOS Trick (LaMacchia, Lauter, Mityagin)
  - Hash the private key into the RNG pool
  - Sometimes the private key is not available (PKCS#11)

Proposed Solution

- Given a long-term asymmetric key
- Sign (or encrypt) a static value with long-term key
- Mix result into RNG
- Example for how do use this in TLS in draft

Is this valuable?

Where should it live?

Randomness Improvements for Security Protocols

Nick Sullivan, Cas Cremers, Luke Garratt

draft-sullivan-randomness-improvements-00