Operational Concerns for Implementations of TLS

Paul Hoffman

WPKOPS, IETF 88

Introduction

- This will be a draft in the future, and the WG might want to adopt it
- Operational concerns when implementing TLS
- Mostly about TLS handshake, some about application data

Purpose of the new draft

- As with any protocol in wide deployment, bugs and varying interpretations of the standard have resulted in an implementation ecosystem which contains many potholes
- We can document recommendations (not requirements) that will help avoid the potholes

Relationship to WPKOPS

- A few of the recommendations apply to PKI, but many don’t
- Could split these into two documents, but so few implementers know about them it might be better to have them all together here
- Another way to think about this: if the handshake doesn’t happen, the web PKI doesn’t even get a chance to work

Handshake recommendations

- Certificates payload brings up many PKIX and related issues
- ClientHello particularly rife with issues
- Extensions, ServerHello, and ServerKeyExchange have some pitfalls too
- Security issues with fallback to less capable versions of TLS
- Application data issues: ciphersuites, record sizes, AES-GCM nonces

Next steps

- Authors will create a real draft (very soon)
- WG can consider if this has enough to do with WPKOPS to keep it in the charter