TLS WG

Eric Rescorla
Network Resonance
ekr@networkresonance.com

Agenda

5	Chairs	Agenda Bashing
10	Chairs	Current WG Status
30	Eric Rescorla	draft-ietf-tls-rfc4346-bis-01.txt
10	Eric Rescorla	draft-ietf-tls-ctr-01.txt
15	Andrea Doherty	draft-linn-otp-tls-00.txt
15	Yngve N. Petterson	draft-pettersen-tls-interop-experience-00.txt
05	Uri Blumenthal	TLS-PSK with NULL
10	Michael Tüxen	DTLS PSK and key export

Document Status

TLS 1.1	RFC 4346 (PS)	Published
Extensions (revised)	RFC 4346 (PS)	Published
Datagram Transport Layer Security	RFC 4347 (PS)	Published
ECC Cipher Suites	RFC 4492 (PS)	Published
Transport Layer Security (TLS) Session Resumption without Server-Side State	RFC 4505 (PS)	Published
TLS User Mapping Extension	draft-santesson-tls-ume-07	RFC Ed Queue
TLS Handshake Message for Supplemental Data	draft-santesson-tls-supp-02	RFC Ed Queue
Transport Layer Security (TLS) Authorization Extensions	draft-housley-tls-authz-extns-07	RFC Ed Queue
Using OpenPGP keys for TLS authentication	draft-ietf-tls-openpgp-keys-10	Last Call
Using SRP for TLS Authentication	draft-ietf-tls-srp-12	AD Review
AES Counter Mode Cipher Suites for TLS and DTLS	draft-ietf-tls-ctr-01.txt	Ready for last call?
The TLS Protocol Version 1.2	draft-ietf-tls-rfc4346-bis-01.txt	Working...

Oops!

Dear IANA & RFC4492 authors,

It seems that the recently published RFC 4492, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)" had a slightly incorrect IANA considerations section: The text included only the new registries created in this document, but not the assignments from existing registries. The final draft-ietf-tls-ecc-12 did include all the assignments, but only in a note to the RFC editor, which was removed before publication (and presumably before IANA got the document).

(I noticed this while updating my own totally unofficial list of TLS-related numbers at http://people.nokia.net/~pasi/tls-numbers.txt)

How should we proceed to correct this issue? I've compiled a list of the missing assignments (at the end of this message), but obviously that should be carefully checked that it actually matches RFC4492...

Best regards, Pasi

TLS 1.2 Status

Eric Rescorla
Network Resonance
ekr@networkresonance.com

New Draft

- New draft (-01)
- Minor changes
  - Server-indicated hash function negotiation
  - Fixed protocol numbers (still missing one)
  - Harmonized $application\_data$ priority with 4346
  - Hashtype IANA section
  - Editorial

How to negotiate new PRF

- Via an extension
  - Aren't we starting to move the protocol into extensions?
- Tied to cipher suites (+ Protocol Version?)
  - Combinatoric explosion?
  - But new PRFs probably mean new cipher suites
    - Does this discourage mix-and-match?
- **Proposal**
  - All PRFs must match the current "API"
  - All current cipher suites get a PRF using SHA-1
  - Future hash-based cipher suites by default get PRF with their hash
  - Future cipher suites can define new PRFs

$verify\_data$

- Currently $PRF(MD5(handshake\_messages) + SHA1(handshake\_messages))$
  - Rationale for this construction is to save memory
    - 2-5 K?
  - Shouldn't be tied to some hash function, right?
  - Move somehow to PRF?
- **Proposal**
  - $PRF(handshake\_messages)$

SHA-384

- Not currently there
  - Should we put it in?
- **Proposal**
  - No.

Alerts

- We've got a 1-byte field
  - It's about 15% consumed (thanks Pasi)
  - You need Standards Track document to get a code point
    - People are asking for code points in non-PS documents
- Expand the field?
  - Make it 16 bits? Add a freeform text field? (insane, right?)
- Allow Specification Required?
- **Proposal 1**
  - Expand the field to 16 bits
  - Allow Specification Required
- **Proposal 2**
  - Do nothing.

Version Numbers in Records

- What version goes in the $client\_hello$ record header
  - The spec appears to say lowest version
  - And clients are inconsistent
  - And servers get confused
- We need more data
- **Rough Proposal**
  - Decide what you SHOULD put in
    - Either lowest or highest, presumably
  - Server mostly ignores it—at least the low byte