TLS WG

Eric Rescorla
Network Resonance
ekr@networkresonance.com
# Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Name</th>
<th>Topic/Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Chairs</td>
<td>Agenda Bashing</td>
</tr>
<tr>
<td>10</td>
<td>Chairs</td>
<td>Current WG Status</td>
</tr>
<tr>
<td>30</td>
<td>Eric Rescorla</td>
<td>draft-ietf-tls-rfc4346-bis-01.txt</td>
</tr>
<tr>
<td>10</td>
<td>Eric Rescorla</td>
<td>draft-ietf-tls-ctr-01.txt</td>
</tr>
<tr>
<td>15</td>
<td>Andrea Doherty</td>
<td>draft-linn-otp-tls-00.txt</td>
</tr>
<tr>
<td>15</td>
<td>Yngve N. Petterson</td>
<td>draft-pettersen-tls-interop-experience-00.txt</td>
</tr>
<tr>
<td>05</td>
<td>Uri Blumenthal</td>
<td>TLS-PSK with NULL</td>
</tr>
<tr>
<td>10</td>
<td>Michael Tüxen</td>
<td>DTLS PSK and key export</td>
</tr>
</tbody>
</table>
## Document Status

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