TLS WG

Eric Rescorla

Network Resonance

ekr@networkresonance.com

Agenda

1. Agenda bashing (5 minutes) - chairs
   - Bluesheets
   - Agenda changes
   - Scribe for minutes
   - Jabber scribe
2. Document status (5 minutes) - chairs
   - Progress since last IETF
3. TLS 1.2 (60 minutes) - Eric Rescorla
4. TLS GCM (10 minutes) - Abhijit Choudbury
5. EAP Authentication (10 minutes) - Yaron Sheffer
6. GSS-API Authentication (10 minutes) - Stefan Santesson
7. Discussion of GSS/EAP (20) - All
8. TLS Extractors (10) - Eric Rescorla

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	RFC 4681	**Published**
TLS Handshake Message for Supplemental Data	RFC 4680	**Published**
Transport Layer Security (TLS) Authorization Extensions	draft-housley-tls-authz-extns-07	Re-last-called
Using OpenPGP keys for TLS authentication	draft-ietf-tls-openpgp-keys-10	**RFC Ed Queue**
Using SRP for TLS Authentication	draft-ietf-tls-srp-12	Editors revising
Pre-Shared Key Cipher Suites with NULL Encryption for Transport Layer Security (TLS)	RFC 4785	Published
AES Counter Mode Cipher Suites for TLS and DTLS	draft-ietf-tls-ctr-01.txt	Working... (missed for this meeting)
The TLS Protocol Version 1.2	draft-ietf-tls-rfc4346-bis-03.txt	Working...

TLS 1.2 Status

Eric Rescorla
Network Resonance
ekr@networkresonance.com

“Major” Changes

- Require Bleichenbacher and timing attack protection [issues 17 and 12].
- Made maximum fragment size a MUST [issue 9]
- Remove ephemeral RSA [issue 3]
- Stripped out discussion of how to generate the IV and replaced it with a randomness/unpredictability requirement [issue 7]
- Stripped out discussion of how to generate the IV and replaced it with a randomness/unpredictability requirement [issue 7]
- Removed extension definitions and merged the ExtendedHello definitions [issues 31 and 32]
- Cleaned up backward compatibility text [issue 25]

Open Issues: DigestInfo Parameters

- Should we include NULL parameter in encodings?
- My read of PKCS#1 v2.1 is that NULL is encouraged for PKCS#1 1.5
- Proposal: MUST use NULL; MUST accept either NULL or no parameters.

Open Issue: Hash Agility for Signatures

- TLS 1.0,1 did not let you specify which hash you used
  - Mandated SHA-1 for DSA, MD5/SHA-1 for RSA
- Current draft allows you to specify allowable hashes
- ...but places two objectionable reqts
  - Must use SHA-1 with DSA (what about long keys?)
  - Must use same algorithm as your certificate has
- Minimal proposal
  - Either side can sign with *any* hash offered by peer
  - List offered in preference order(?)
  - DSA/ECDSA MUST be used with acceptable variant of SHA (defined elsewhere?)
- Should we move the server's indication to an extn.?

Open Issue: Alerts

- Which alerts MUST be fatal?
- Which alerts MUST be sent?
- Concern about requiring too many alerts (cf. Bleichenbacher)
- Proposal:
  - agree on what alerts are fatal
  - MUST send them
- NIST's proposal for new fatal alerts:
  - bad_certificate, unsupported_certificate, and certificate_revoked

draft-rescorla-tls-suiteb

Eric Rescorla
Network Resonance
ekr@networkresonance.com

Background: NSA Suite B

- NSA profile for COTS security algorithms

Encryption	AES 128/256
Digital Signature	ECDSA 256/384 (prime)
Key Exchange	ECDH or ECMQV 256/384
Hashing	SHA-256/384

What is this document?

- Adds SHA-256/SHA-384 cipher suites to TLS-ECC
- Adds ECC + GCM cipher suites (with SHA-256)
- Profile for specific curves for SuiteB compliance
  - P256 for 256-bit suites
  - P384 for 384-bit suites
  - Can ignore this if don't want SuiteB

What to do?

- Reasonable comments received from Pasi
- Should this be a WG doc?
- What about specifying longer hashes for non-ECC cipher suites?

draft-rescorla-tls-extractor

Eric Rescorla
Network Resonance
ekr@networkresonance.com

Motivation

- More call to use TLS as a key management framework for other protocols
- Paradigmatic example: DTLS-SRTP
  - Negotiate DTLS in RTP media plane
  - Extension indicates “use SRTP for framing”
  - Need to extract keys to feed to SRTP
- Other cases suggested: TCP-AUTH, SCTP-AUTH
- Purpose of draft is to offer a single secure way to do this

General mechanism

- Use $PRF(master\_secret, ''EXTRACTOR'' + label)$
  - Labels need to be registered with IANA
- Advantages
  - Provides safe keying material (can't be reversed)
  - Prevents collisions between external users

Comments from Pasi

- Must be signalled by some TLS extension
  - So both sides agree
- Remove “EXTRACTOR” — let IANA guarantee uniqueness
  - Pro: Compatibility with EAP
  - More care required to avoid clashes with TLS internal uses
- Change IANA policy to IETF Consensus

What to do?

- Should this be a WG doc?

Whither SRP

- Document basically done
- Question of status: Informational/Experimental or Proposed
- Some sentiment during WGLC for Proposed
- General issue: IPR status of ZKPPs
- No IPR disclosures on this document—this can't be right
- But overall status unclear
- Other WGs have been inconsistent on this
- Discussion?