TLS Extractor Status

Eric Rescorla
RTFM, Inc.
ekr@networkresonance.com

Document Currently in Last Call

- Last call ends Dec 4, 2008
- Comments from Pasi Eronen, Alfred Hïnes, Hugo Krawczyk
- Mostly editorial
- One typo in the definition of context_value
- Terminology issue from Hugo

Terminology Issue

I have a single "objection" to this document, namely, the use of the word "extractor". Let me explain.

In the context of key derivation functions the notion of extraction refers to a first phase where one starts with a somewhat weak source of randomness (such as an imperfect RNG, a Diffie-Hellman value, etc) and extracts a first cryptographically strong key K.

In a second phase, often called key expansion, one derives multiple keys out of this K using a PRF exactly as the current document specifies. Since master_secret is assumed to already be a cryptographically strong key, then this specification is sound and correct (especially that it includes the essential context information).

Proposed New Names

- Exporter
- Deriver
- Your name here