
TESLA for ALC/NORM I-D
<draf-faurite-rmt-tesla-for-alc-
norm-00.txt>

IETF 63rd- Paris meeting

Sébastien Faurite, Aurélien Francillon, Vincent
Roca (INRIA)

August 2nd, 2005

Motivations for this I-D

- TESLA identified a long time ago in RMT docs
 - mentioned in ALC, LCT, FLUTE and NORM RFCs
- A lot of good work on TESLA in MSEC
 - RFC 4082 (June 2005)
“TESLA: multicast source auth. transform intro.”
 - <draft-ietf-msec-srtp-tesla-03.txt> (Feb. 2005)
“The use of TESLA in SRTP”
 - <draft-ietf-msec-bootstrapping-tesla-01.txt> (May 2005) *“Bootstrapping TESLA”S*
 - old I-D <draft-ietf-msec-tesla-spec-00.txt> (Apr 2002)
“TESLA specification”
now ``dead``, but mostly useful... some parts of our I-D rely on it!

Missing features in current MSEC docs

But several features are still missing...

- Only MIKEY-based bootstrapping is considered
 - whereas ALC/NORM can use **in-band signaling** through the header extension mechanism
 - ⇒ **no need for an extra protocol**
 - whereas ALC sessions can require a periodic TESLA bootstrapping (e.g. in on-demand mode)
 - ⇒ **full control on when bootstrapping information is sent is needed**

Missing features in MSEC docs... (cont')

- Indirect synchronization is mentioned but not detailed
 - ALC sessions have **potentially no back channel**, so direct synchronization is not necessarily feasible
 - direct synchronization leads to scalability problems, while ALC sessions are **massively scalable**
 - ⇒ **indirect synchronization support is almost mandatory with ALC (less true with NORM)**
 - ⇒ **specify how to do that reliably**

Missing features in MSEC docs... (cont')

- Key chain switching is not addressed
 - ALC sessions can be **very long** (e.g. in on-demand mode) and may require several key chains
 - ⇒ **specify how to do that reliably and efficiently**
- Information payload formats are missing
 - no bootstrapping information format in draft-ietf-msec-bootstrapping-tesla (MIKEY)
 - only available in the dead TESLA Spec I-D
 - ⇒ **specify an updated format along this line**



The “TESLA for ALC/NORM” I-D

- Requires an initial bootstrap information message
 - sent in a **dedicated** ALC/NORM control packet containing only a **bootstrap info header extension**
 - **separate control packet because of header ext. size**
 - only sent at the beginning (push) or periodically (on-demand)
- Indirect time synchronization
 - ALC/NORM server sends list of possible NTP servers in the bootstrap info message
 - use secure NTP (server sends certificate)

The “TESLA for ALC/NORM” I-D... (cont’)

- Signature extension

- each ALC/NORM packet contains a signature header extension
- contains MAC + interval number + a key
 - the key depends on whether we are in a single chain or are switching between two chains

What's next?

1. Split our I-D or not?

- mailing list discussion initiated by M. Luby
- several TESLA protocol features could easily be moved to MSEC specific docs... or merged with existing MSEC docs
- keep a streamlined ALC/NORM instantiation document, avoiding duplications
- could increase the applicability or additional features in other contexts

2. Work on some technical aspects

- it's only a -00 version...

What's next? (cont')

- We implemented all these features (except secure NTP)
 - based on A.Perrig/B. Whillock 's code (thanks 😊)
 - will be public soon



That's all!