



TESLA for ALC/NORM I-D <draf-faurite-rmt-tesla-for-alcnorm-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
 Omentioned 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." O<draft-ietf-msec-srtp-tesla-03.txt> (Feb. 2005) "The use of TESLA in SRTP" O<draft-ietf-msec-bootstrapping-tesla-01.txt> (May) 2005) "Bootstrapping TESLA"S Oold 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
 - Owhereas ALC/NORM can use in-band signaling through the header extension mechanism
 - \Rightarrow 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

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





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

Key chain switching is not addressed

OALC sessions can be very long (e.g. in on-demand mode) and may require several key chains

- \Rightarrow specify how to do that reliably and efficiently
- Information payload formats are missing
 - Ono bootstrapping information format in draft-ietfmsec-bootstrapping-tesla (MIKEY)
 - Oonly available in the dead TESLA Spec I-D
 - \Rightarrow 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
 Oseparate control packet because of header ext. size
 only sent at the beginning (push) or periodically (ondemand)
- 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

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





What's next?

Split our I-D or not?

- **O** 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

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





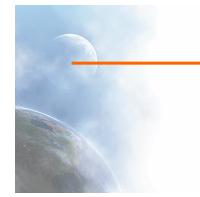
What's next? (cont')

We implemented all these features (except secure NTP)

○based on A.Perrig/B. Whillock 's code (thanks ☺)○will be public soon







That's all!



