TESLA for ALC and NORM
draft-ietf-msec-tesla-for-alc-norm-06

IETF 73 – Minneapolis, November 2008

Vincent Roca (INRIA)
Status

- MSEC WGLC, with CC to RMT

- issued in Sept. 19th-Oct. 3rd for -05 version

- received detailed comments:
  - Brian Weis (MSEC co-chair)
  - Ramu Panayappan (security group, CMU)

- no serious problem has been found

- new -06 version that addresses most comments submitted on Oct. 24th

http://www.ietf.org/internet-drafts/draft-ietf-msec-tesla-for-alc-norm-06.txt
How we addressed the comments…

- (BW) “weak group MAC” is a bit pejorative
  - we now use “Group MAC”.

- (BW) add a scope section rather than saying so often it’s out of scope
  - good idea, added

- (BW) whether or not NTP is required isn’t clear
  - secure time synchronization is a MUST, how to do that is left to the developer
  - clarified that some fields use an NTP format independently of whether or not NTP is used
How we addressed the comments... (cont’)

● (BW) I-D does not consider the auth of feedback packets, which is a bit limitative...
  ○ it’s addressed by the companion I-D (“simple auth schemes for ALC and NORM”)
  ○ clarified in section “1.2 Scope”

● (BW) should default to SHA-256, not SHA-1
  ○ agreed, SHA-1 was assumed to be safe till 2011 [IETF plenary, Nov 2005], which is now close...
How we addressed the comments… (cont’)

○ **impacts:**
  - packet authentication tag (based on HMAC-SHA*)
  - digital signatures (even if RFC4359 says that SHA1 MUST be used!)

○ **TODO:** -06 only partially implements the change (e.g., examples are not updated). Will be done in -07.

○ **(BW) what happens if a receiver “guesses” the value of “i” (interval index) wrong?**

○ **background:**

  with compact forms of TESLA HE, only 1 or 3 bytes of the original 32-bit “i” value is carried in the packet ⇒ the receiver guesses the remaining byte(s)
How we addressed the comments… (cont’)

- excellent point, insufficiently addressed in previous I-D
  - added section “4.3.1. Wrong Guess of the i Parameter”

- a wrong guess is caused by:
  - a very long transmission delay (> 256*T_int milliseconds, with T_int in the order of the RTT) => does not happen normally
  - a deliberate attack

- error will be captured:
  - by the safe packet test (step 2), or
  - by the new key index test (step 4a) or key verification test (step 4b) if this packet discloses a key, or
  - by the authentication test (step 7), when the key corresponding to this wrong interval index is disclosed.

- it’s safe, the packet is ALWAYS discarded 😊
How we addressed the comments… (cont’)

● (BW/Ramu) anti-replay: does NORM seq. # check happen before TESLA processing?
  ○ good practice is to check before…. But checking after does not compromise TESLA. Clarified.

● (BW) does IANA need to create a repository?
  ○ oups, we missed the point!
  ○ there’s already a TESLA registry (from RFC4442):
    • let’s take advantage of it…

  http://www.iana.org/assignments/tesla-parameters/

  ○ TODO: will be done in -07.
How we addressed the comments… (cont’)

- (Ramu) GPS is not 100% safe
  - Right, it’s not a fully secured time sync… Clarified

- (Ramu) why does the Group MAC include the digital signature? It prevents parallelism
  - It enables a receiver to identify corrupted signatures during the (cheap) Group MAC verif. (mitigates DoS)

- (Ramu) with Group MAC periodical rekeying, there’s a risk of not using the correct key
  - Yes, if GKMP is not sufficiently real-time. Anyway, it’s out-of-scope, and accepting old keys would be strange!
Additional modifications

- in addition, we made 3 corrections:
  - corrected a small ambiguity in description of the authentication of incoming packets
    - (step 4a/4b): storing all intermediate keys is more natural. Corrected
  - clarified that in the auth tags, the MAC($K'_i$, $M$) is truncated
    - it was only mentioned in section 1.2.1 and implicitly in the IANA section ⇒ it was misleading...
Additional modifications… (cont’)

- added “4.2.2 Discarding unnecessary packets earlier”
  - only an optimization, that specifies when incoming packets can be safely discarded, prior to TESLA auth.
  - example:
    - pure data ALC packet (no signaling) for an object not desired by the application (or already decoded)
  - can dramatically reduce the processing load under normal conditions 😊
Next steps

1. we update the I-D
   - finish SHA-1 to SHA-256 migration (examples)
   - clarify IANA registration

2. continue with IESG review?

Above all, we are grateful to Brian and Ramu for their detailed and very useful review!