MSEC Meeting

IETF 71st – Philadelphia, March 2008

Vincent Roca

TESLA for ALC/NORM status

- basically
  - new -04 version of the I-D (Feb. 18th, 2008)
  - IMHO the specifications are now stable
  - we implemented most of it to cross-check the specification...
    - **seems to work...**
    - **... but we did not test it thoroughly yet**

Modifications to the I-D

- new bootstrap information message format
  - contains a “key chain commitment” rather than disclosing a key
    - ⇒ **in line with some authentication tags that commit to a new key chain + avoids some tricky situations at session startup**
- added “crypto function type” for digit. signatures
  - new IANA registry and new bootstrap info msg field
  - says: this RSASSA-PKCS1-v1_5 is based on SHA-1
  - is it appropriate? Opinion?

Modifications to the I-D (cont')

- clarified the use of multiple key chains
  - now require that the periods during which we disclose the last key of previous KC (LKofPKC) and the period during which we send commitments to the new KC (CtoNKC) must not overlap
    - **motivations:**
      - **(1) a receiver knows upon receiving a new KC commitment that he will no longer be able to authenticate packets of previous chain if any;**
      - **(2) faked packets that disclose the LKofPKC or send CtoNKC at wrong time MAY be immediately dropped**

Modifications to the I-D (cont')

- explain when a receiver can flush packets of a previous KC waiting to be authenticated
  - direct consequence of previous point...
- finished description of the processing steps of incoming packets at a receiver
  - several points were missing
  - it's critical
    - **one can easily design bogus TESLA receivers (or implementations that are subject to DoS) if not specified carefully...**

Modifications to the I-D (cont')

- editiorial work
  - text/sections moved...
  - and clarifications added
- ready for WGLC?