IPsec security for packet based synchronization

draft-xu-tictoc-ipsec-security-for-synchronization-02

Yang Cui
On Behalf of Yixian Xu
Huawei
Nov. 13-18, 2011 @Taipei, IETF#82

Current Status

- Current version attracted a long thread of discussions in Mailing lists (tictoc and IPsec) for comments
- Thanks for all comments and suggestions to the draft
  - In particular, *Danny Mayer, Kevin Gross, Nico Williams, David L. Mills, Paul_Koning, Tim Frost, Manav Bhatia, Michael Richardson, Stephen Kent, Leonid Goldin, Yaakov Stein, Karen O'Donoghue (Chronological Order)…*
- A new version is being prepared accordingly

Questions Raised in Mailing Lists

Question 1.

- Do we need Encryption of Timing Packets?

Question 2.

- Do we need to equip Encrypted Timing Packets w/t certain Identifier?
  - In other words, to distinguish the timing packets right away, but not after decrypting all traffic

Others.

- editorial and a few technical problems

Q1: Security of Timing Packets

- For timing message, even though *Integrity* is further essential than *Confidentiality*, there exists use cases in which both of them are provided
  - 3GPP Femtocell published standard, [3GPP TS 33.320], "Femtocell SHALL support receiving time synchronization messages over the secure backhaul link between Femtocell and the Security GW, and Femtocell SHALL use IKEv2 protocol to set up at least one IPsec tunnel to protect the traffic with Security GW.
  - Some scenarios where confidentiality and integrity is mandatory

Q2: IPsec Security for Packet based Synchronization

- Solutions:
  - IEEE 1588v2: An experimental Annex is described, only useful for ESP-NULL, i.e. integrity only protection
  - IPsec: no solutions are known, except that trivially timestamp all (packets) and decrypt all
    - Note that it is highly costly to put timestamps on all packets. For example, a hardware implementation [ISPCS'10]: Frame check sequence, UDP check sum, and HMAC need to be computed for timestamp, where HMAC is quite costly to do for all packets!
- This Proposal:
  - To equip encrypted timing packets w/t Identifier based on slightly extended WESP[RFC5840]
  - So that, timing packets could be recognized immediately w/o decryption

On Blocking Identified Timing Packets

- Comment:
  - If encrypted timing packets could be identified easily, then it is more convenient for attackers to block?
- Response:
  - Can't agree. Timing packets in plain text could be blocked in a similar way.
- Identifying timing packets does not change the security against the *Blocking attack*.

Next Step

- Re-submit the draft for re-evaluation,
  - Answer Q1 and Q2
  - By now, proposed mechanism is the most efficient to IPsec synchronization.
  - Or, any other efficient mechanism?
  - Editorial problems

Thank you!