KSP Update (2)

A distributed fault-tolerant group key selection protocol

Mick Seaman
mick_seaman@ieee.org

Background

http://www.ieee802.org/1/files/public/docs2006/af-seaman-key-selection-protocol-0506-05.pdf

http://www.ieee802.org/1/files/public/docs2004/af-seaman-key-selection-protocol-1204-04.pdf

http://www.ieee802.org/1/files/public/docs2004/AF-seaman-secure-multicast-transport-01.pdf

http://www.ieee802.org/1/files/public/docs2004/af-seaman-ksp-update-01.pdf

Summary

Background

Changes

Proofs

Changes (1)

CMAC protection of KSPDUs

- Following Brian Weis' analysis of earlier proposal
- Replaces GMAC (mis)use—but see later
  - Loses full line rate protection against DoS attacks
- AES-CMAC-128 using K=AES-ECB(CAK, 0x01)

Proposes definite keyed prf for SAK calculation

- SAK = AES-CMAC(K,M,128)
  - K = AES-ECB(CAK,0x02)
  - M = KCn,....KC1

Changes (2)

Extension to allow key selection by server and distn.

- KC calculated ‘key’ serves as proof of freshness of distributed key
  - removes any single PDU limitations
  - allows distribution of a group CAK by a point-to-point KSP dialogue that uses CAK=PMK

Proofs

SAK freshness and security

- does not depend at all on KSPDU integrity
- purely a function of CMAC(KC list)