Network Performance Measurement for IPsec

draft-bi-ippm-ipsec-01

Yang Cui , Emily Bi, Kostas Pentikousis (Ed.)

IETF 86

Orlando, Florida, USA

Background

- OWAMP [RFC 4656], TWAMP [RFC 5357]
  - Discussion on security protection in the past
  - Decision to develop a dedicated security mechanism and give up on TLS, DTLS, IPsec
  - Unauthenticated, authenticated, and encrypted modes
- Today: interested in stats about the actual deployment of the authenticated and encrypted modes in practice
  - Cf. IKEv2/IPsec deployment

Proposed Enhancement

- Today: O/TWAMP security mechanism
  - Based on shared secret, does not support credential or certificates
  - Four (4) keys for integrity and encryption protection
    - AES keys: OWAMP-Control, OWAMP-Test
    - HMAC keys: OWAMP-Control, OWAMP-Test
- Proposal: Use IKEv2/IPsec to feed the key to O/TWAMP
  - Well-known and well-designed security mechanism
  - Enhance security protection, key negotiation
  - Support certificate based key exchange
  - Extend to automatic key management

Proposal Advantages

- Use of well-understood, widely-implemented IKEv2/IPsec to replace a specialized security mechanism
  - Enhance O/TWAMP security
- Support cert-based key exchange
  - More flexible in practice and more efficient
- Ease key management in shared secret model
  - The use of IKEv2/IPsec makes it easier to extend automatic key management.
- Community Document: please contribute!

Current Keys Usage

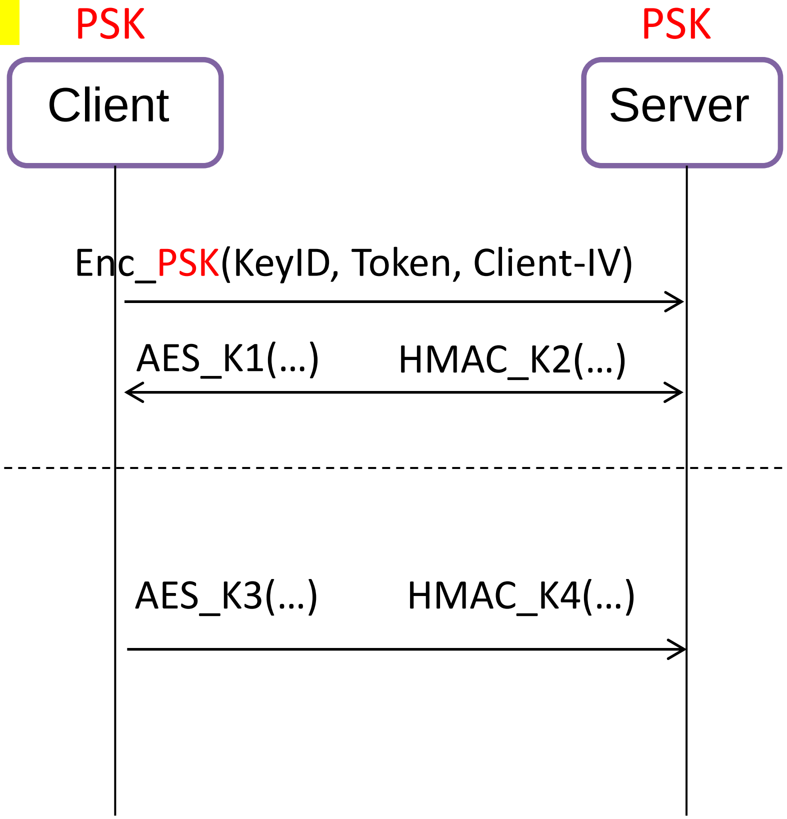
OWAMP-control

Generate

✓KeyID,

✓Token,

✓Client-IV



Token=cha||K1||K2

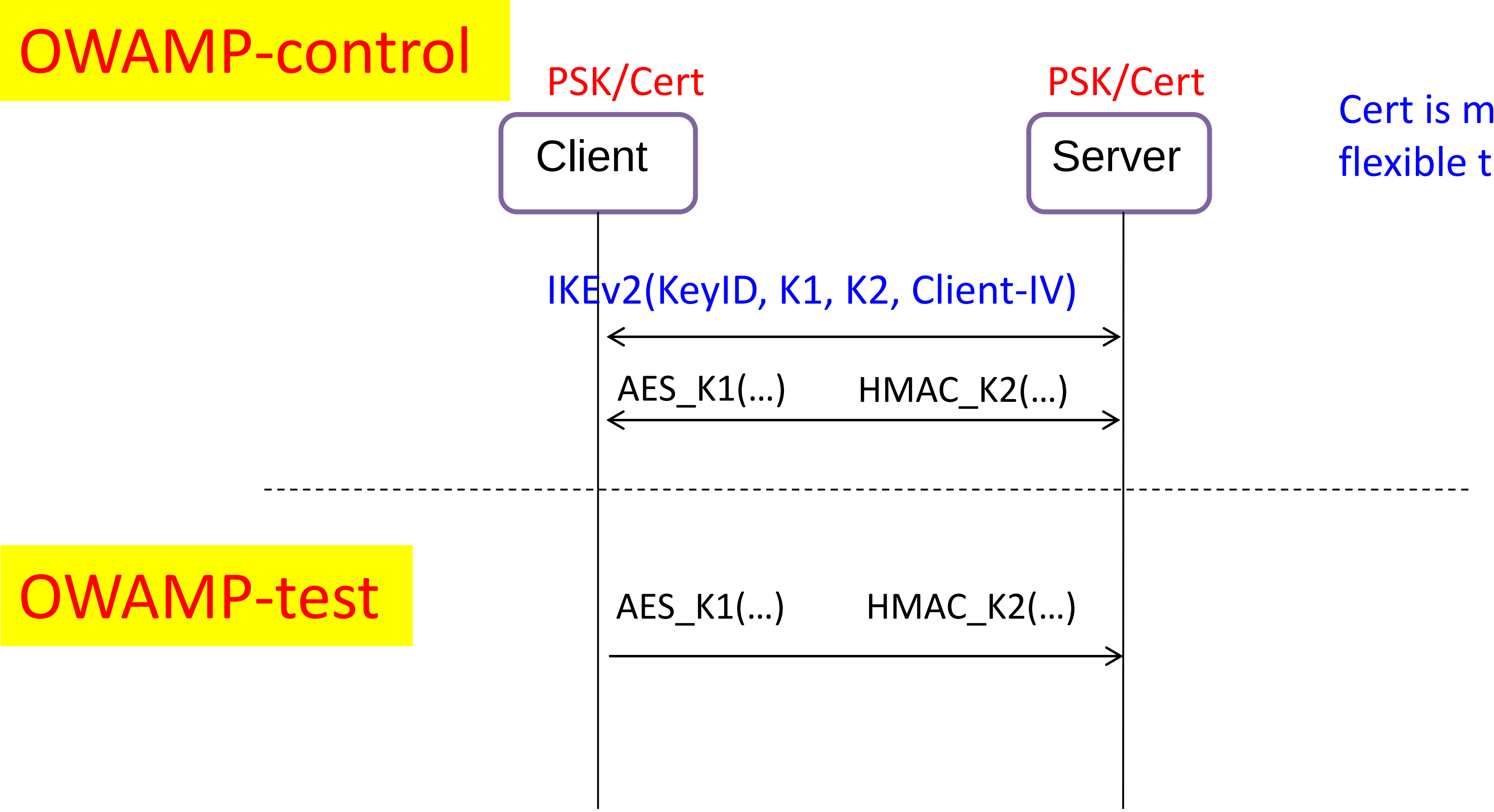
OWAMP-test

K3=KDF(K1||SID)

K4=KDF(K2||SID)

Finally, share 4 keys for enc and auth

New Keys Usage



OWAMP-control

PSK/Cert

Client

PSK/Cert

Server

IKEv2(KeyID, K1, K2, Client-IV)

AES_K1(…) HMAC_K2(…)

OWAMP-test

AES_K1(…) HMAC_K2(…)

Cert is more flexible to use

Keys exchanged by IKEv2, encryption by AES, integrity by HMAC, others simply follow O/TWAMP

Way Forward

- Request to add network performance measurement for IPsec in the new charter
- Consider this draft for work group adoption