Network Performance Measurement for IPsec

draft-bi-ippm-ipsec-00

Emily Bi, Kostas Pentikousis, Yang Cui
IETF 85@Atlanta, 2012-11-06

Problem Statement

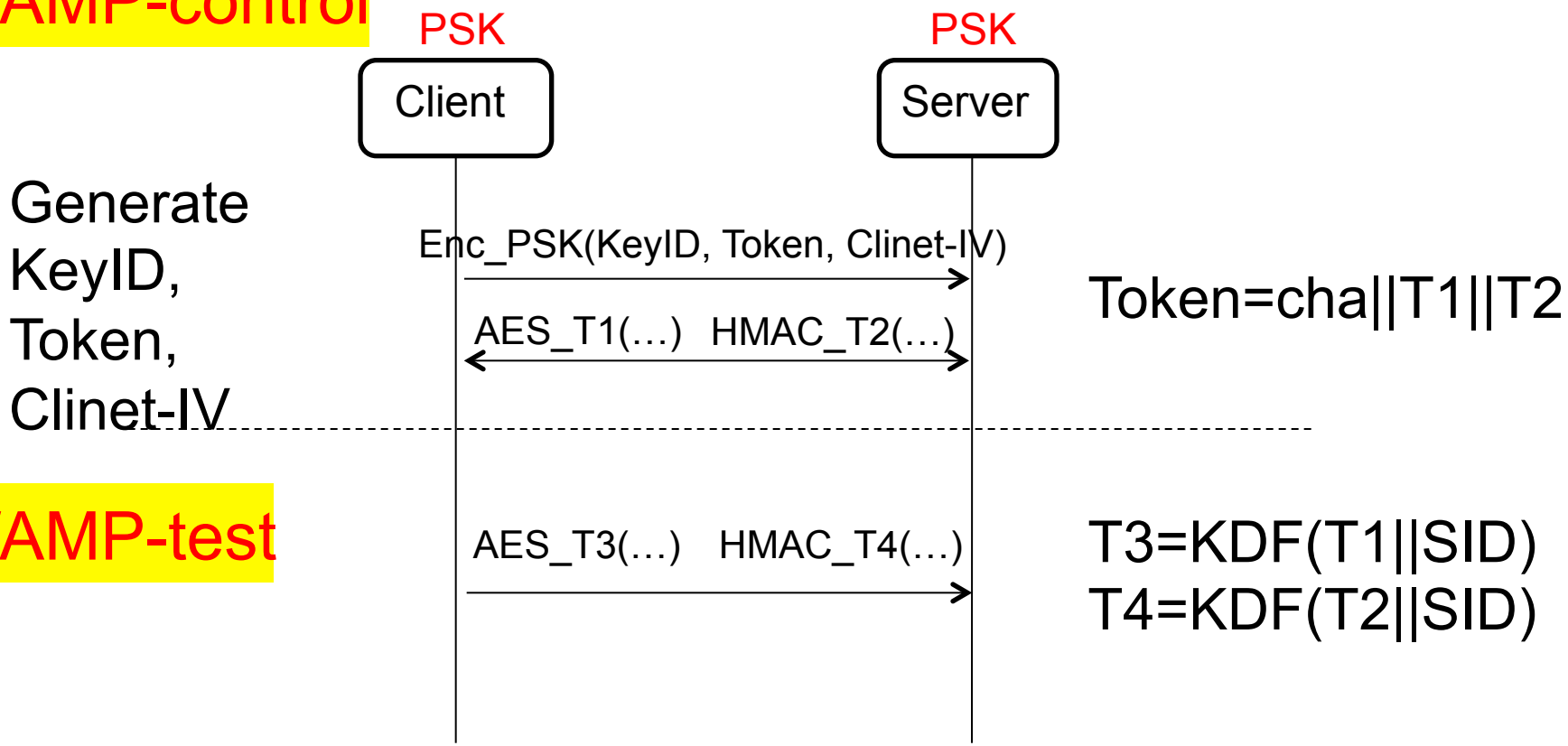
- Question: What about using IPsec to protect OWAMP?
- Answer: According to [RFC4656] (ca. 2000-2006)
  - IPsec cannot be used for partial authentication of a packet. The authenticated mode of IPPM would not be possible.
  - IPsec is not widely deployed, and OWAMP should not depend on Ipsec deployment .
  - Most lightweight embedded devices, such as, Ethernet switches, DSL "modems", and other such devices mostly do not support IPsec.
  - The API for manipulating IPsec from an application is *currently* poorly understood.

OWAMP Security

- [RFC4656] uses a specific security mechanism
- OWAMP needs client and server to have a pre-shared key (a passphrase), to
  - encrypt the session key for OWAMP-control encryption and authentication, and
  - further generate keys for OWAMP-test encryption and authentication
- Use different keys for OWAMP-control and OWAMP-test (4 keys, AES/HMAC) to avoid reflection attack**
  - May be error-prone for engineers who are not familiar with security

OWAMP Key Generation and Transport

OWAMP-control



OWAMP-test

T3=KDF(T1||SID)
T4=KDF(T2||SID)

Finally, share 4 keys for enc and auth

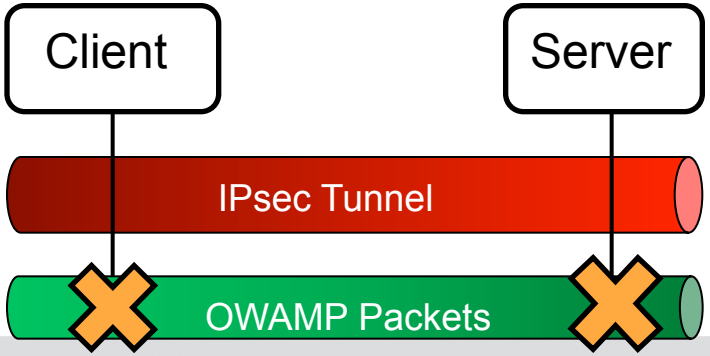
Some Observations

- Since [RFC4656] was published, IPsec has been widely deployed
  - In case that IPsec is already deployed and actively used, there is a collision between partial authentication of O/TWAMP and IPsec. Limits the applicability and use of O/TWAMP in networks using Ipsec *already*
  - In several currently-deployed types of networks, IPsec is widely used to protect the data and signaling planes
  - A large number of limited-resource and low-cost devices support of IPsec
  - In practice, most competent technical personnel and programmers have no problems using IPsec.

So, why not consider IPsec or TLS etc. to protect O/TWAMP?

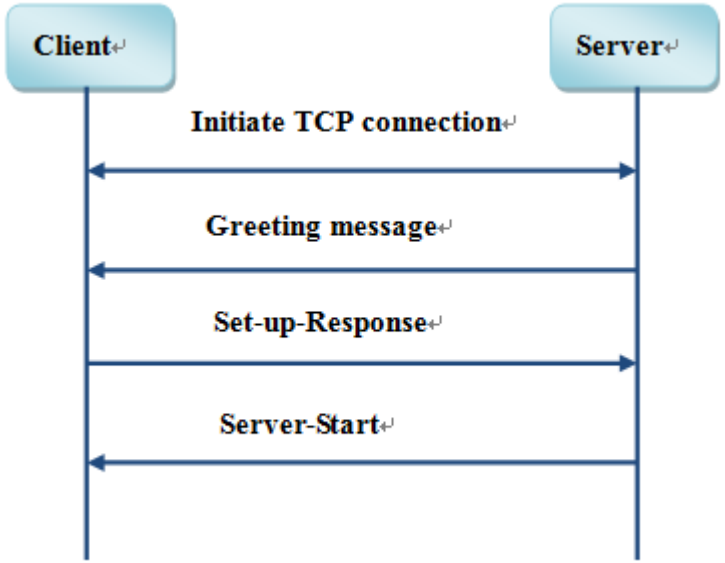
Performance Measurement with IPsec

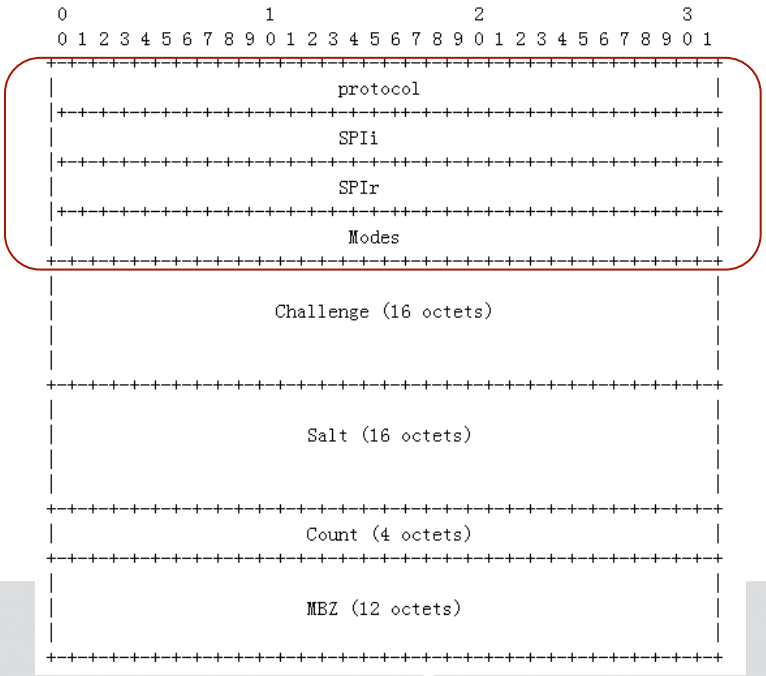
- In case that client and server supporting IPsec, use IKEv2 to negotiate the session keys for encryption and authentication for OWAMP-control and OWAMP-test
  - Enhance the security by using popular protocol to replace specific one
  - May reduce keys to 2, AES/HMAC (not included in the draft), since the IKEv2 instead is deployed.
  - May not rely on the pre-shared key, but on certificates/credential, thus enhance the flexibility
- In case that there is an existing IPsec tunnel between client and server, only unauthenticated mode should be used. In other words, use IPsec tunnel to protect the OWAMP



A Proposed Solution

- A method of binding IPPM and IKEv2 is proposed in the draft, have a look and send your comments!
- The shared key used in the security of O/TWAMP is derived from IPsec.
  - Shared secret key=PRF{ KEYMAT, Session ID}





Thank you