Security Descriptions Extension for IPsec

draft-saito-mmusic-ipsec-negotiation-req-02
draft-saito-mmusic-sdes-ipsec-00

July 12, 2006

Makoto Saito (ma.saito@nttv6.jp)

Motivation

(draft-saito-mmusic-ipsec-negotiation-req-02)

- Using IPsec for Media Security
  - Desired by several vendors and ISPs for networked home appliance usage.
- Advantages
  - Many Vendors are already using IPsec.
  - Aggregation of a large number of media.

IPsec is a simple and comprehensive way in these cases.

Key-Exchange Methods

- IKE - Standard One
- Sdescriptions and Key-mgmt

  "Advantages of Using SDP"

  – Simple round-trip

  – Quick start of media after the SDP exchange

  – Other Advantages

    ✓Authentication of IPsec is consistent with that of SIP/SDP.

    ✓Synchronization with the state of media session (start, refresh, end)

Proposal: Security Descriptions Extension

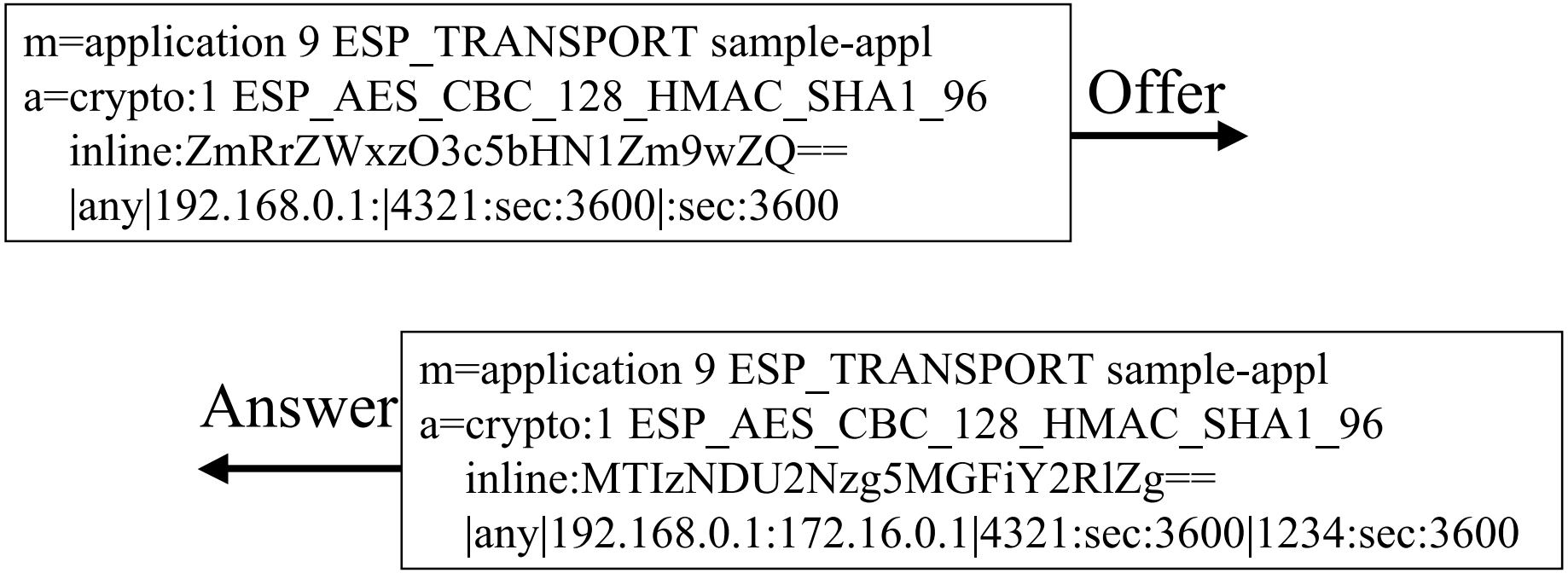
(draft-saito-mmusic-sdes-ipsec-00)

Security Descriptions

- General framework
- Only a profile of SRTP is defined for now
- Just adding a profile for IPsec (SA proposal) here

  i.e. key material, IP address, spi, life time, etc.

Example


m=application 9 ESP_TRANSPORT sample-appl
a=crypto:1 ESP_AES_CBC_128_HMAC_SHA1_96
inline:ZmRrZWxzO3c5bHN1Zm9wZQ==
|any|192.168.0.1:|4321:sec:3600|:sec:3600
Offer
Answer
m=application 9 ESP_TRANSPORT sample-appl
a=crypto:1 ESP_AES_CBC_128_HMAC_SHA1_96
inline:MTIzNDU2Nzg5MGFiY2RlZg==
|any|192.168.0.1:172.16.0.1|4321:sec:3600|1234:sec:3600

Next Step

- Several vendors already implemented it in a prototype format, and it's been working well.
- It seems like a good idea that the protocol format be specified in an IETF document.
- WG item or Individual submission for informational RFC?
- Any Comments?

Summary

- Requirements
  - Using IPsec for Media Security
  - Exchanging IPsec key in a simple and effective way: Using SDP
- Proposal
  - Security Descriptions Extension for IPsec
- Next Step
  - WG item or Individual submission for informational RFC?