Requirements for IPsec Negotiation in the SIP Framework

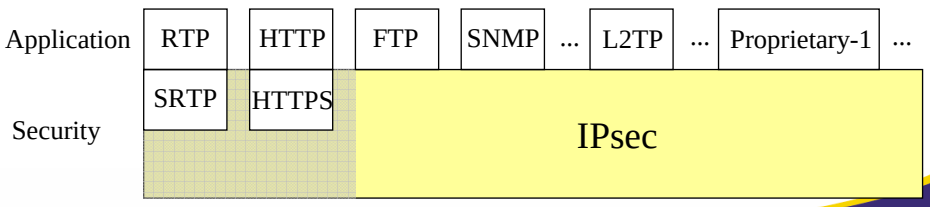
draft-saito-mmusic-ipsec-negotiation-req-00.txt

August 1, 2005

Makoto Saito (ma.saito@ntt.com)
Shingo Fujimoto (shingo_fujimoto@jp.fujitsu.com)

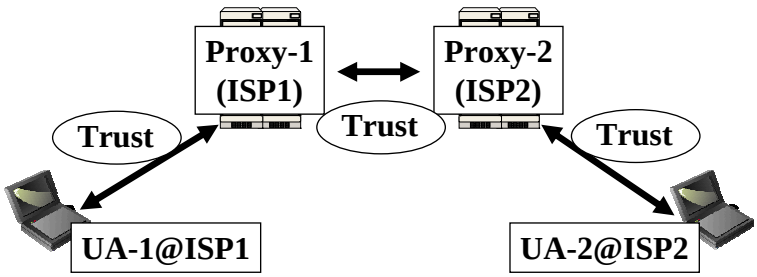
Motivation

- To secure communication between **SIP-enabled home appliances**.
  - Applicable to Proprietary Media Protocols
  - One Generic Security Protocol
- Proposal: IPsec!!
  - But, no standard key-exchange mechanism for IPsec within SIP/SDP.



Where and how can it be used?

- Assumptions
  - Trusted 3rd Party Model
    - ISPs' SIP proxies assure identification of UAs
  - Mutual Trust between Domains (ISPs?)

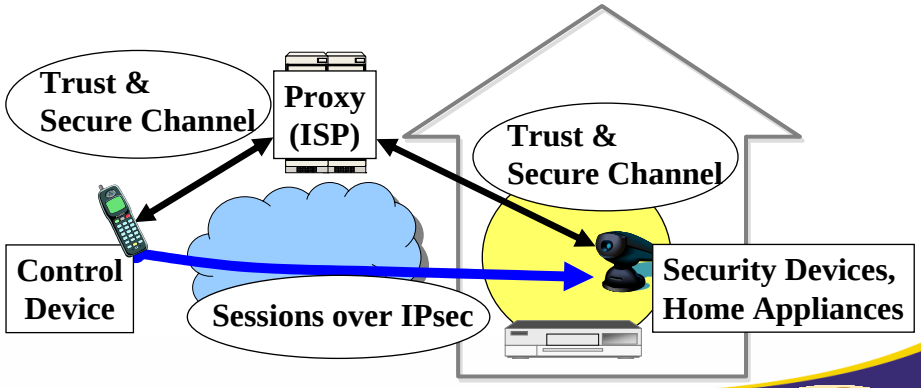


3

Use Case 1: Remote Device Control

- Home Security Service

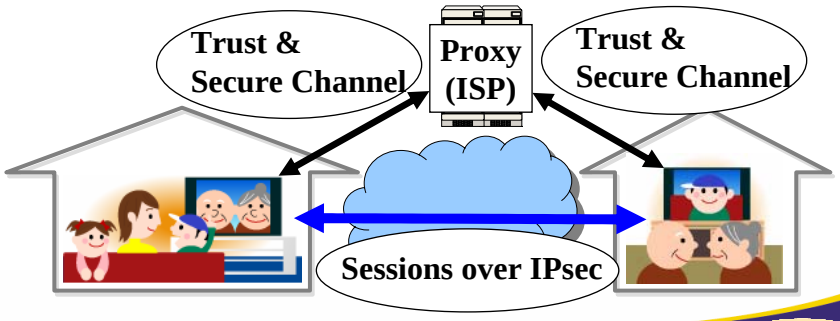
  Controlling Sensors, Cameras, etc.
- Secure Access via the Internet



4

Use Case 2: Visual Communication

- P2P Communication between Users
  Proprietary protocols are often used.
  (Not always RTP)
- Secure Access via the Internet



5

Requirements for Security Protocol

- Security
- Reduction of Resources
  - Transaction Load
  - Implementation Cost
- Connectivity
  - Protocol Interoperability, Scalability
- Generic Use
  - Independent of Applications

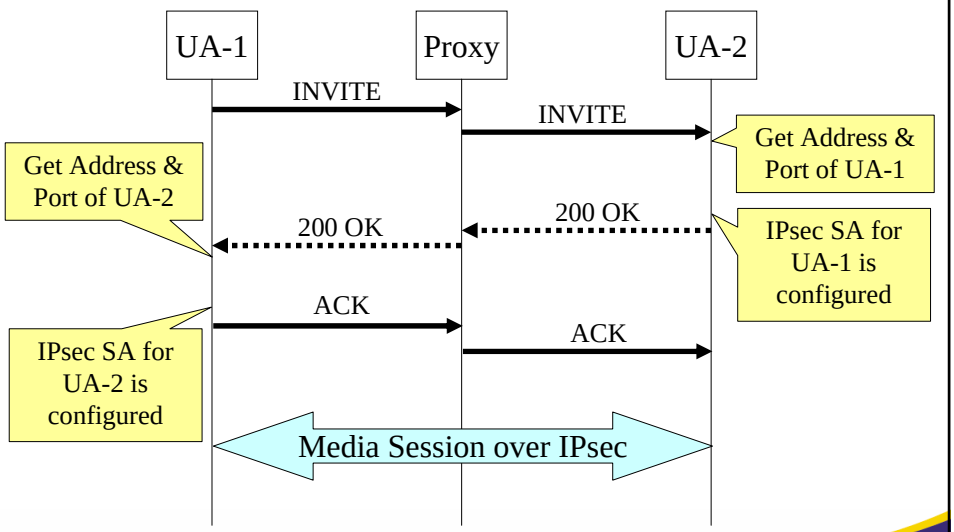
→ IPsec meets these requirements

6

Possible Key-Exchange Solutions

	Conformance with SDP	Implementation	Calculation Load
IKE (RFC2409)	No	Full IKE needed	High
KINK (work in progress)	No	External Kerberos system needed	Low
MIKEY with kmgmt	Yes	in SDP	High
Security Descriptions	Yes	in SDP	Low *SDP must be secured.

IPsec Negotiation in SIP



Summary

- Home appliances need security with their resources reduced. ----- IPsec is proposed.
- Standard mechanism to configure IPsec based on SDP information is needed.
- Concept of Security Descriptions may be a better solution.

Discussions in MMUSIC ML

- Why SIP to configure IPsec?
  - IP addresses of devices (necessary for IPsec configuration) are not static. They are determined during SDP negotiation.
- Why not IKE for key-exchange?
  - It is still necessary to transmit the information from SDP to IKE. It's efficient to exchange IPsec keys during SDP negotiation.

Next Steps

- Suggestions?
- Discussions?
- MMUSIC WG item?