Requirements for IPsec Negotiation in the SIP Framework

draft-saito-mmusic-ipsec-negotiation-req-01.txt

November 9, 2005

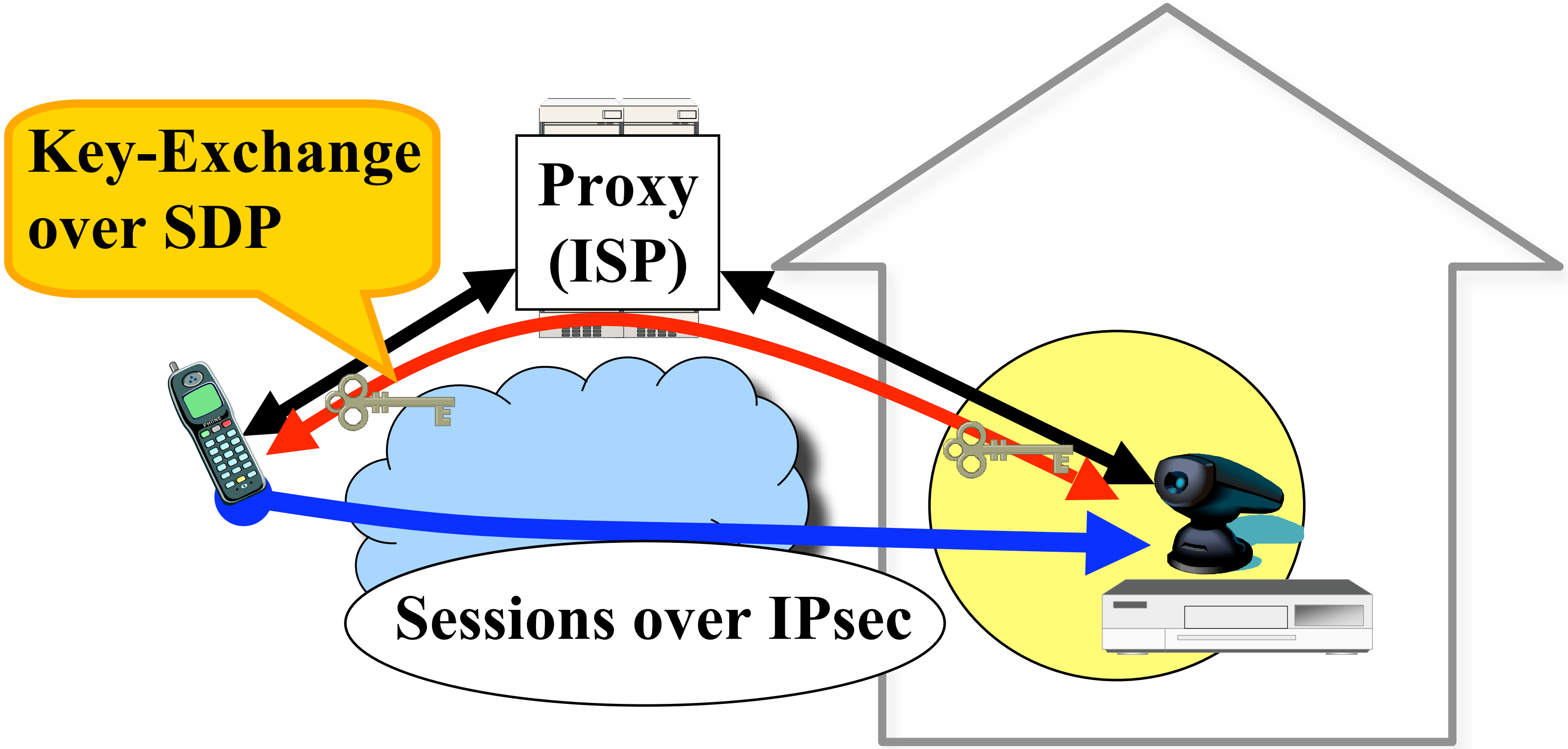
Makoto Saito (ma.saito@ntt.com)
Shingo Fujimoto (shingo_fujimoto@jp.fujitsu.com)

Motivation

- A lot of people are using Internet mindless of their security.
- Security risks (such as forgery, eavesdropping, and so on) are increasing.
- One option of countermeasures is using IPsec (independent of applications).
- Make IPsec easy to use for general people.

Scope of Requirements

- Using IPsec for Media Session
- Light-Weighted IPsec Key-Exchange over SDP



Key-Exchange over SDP

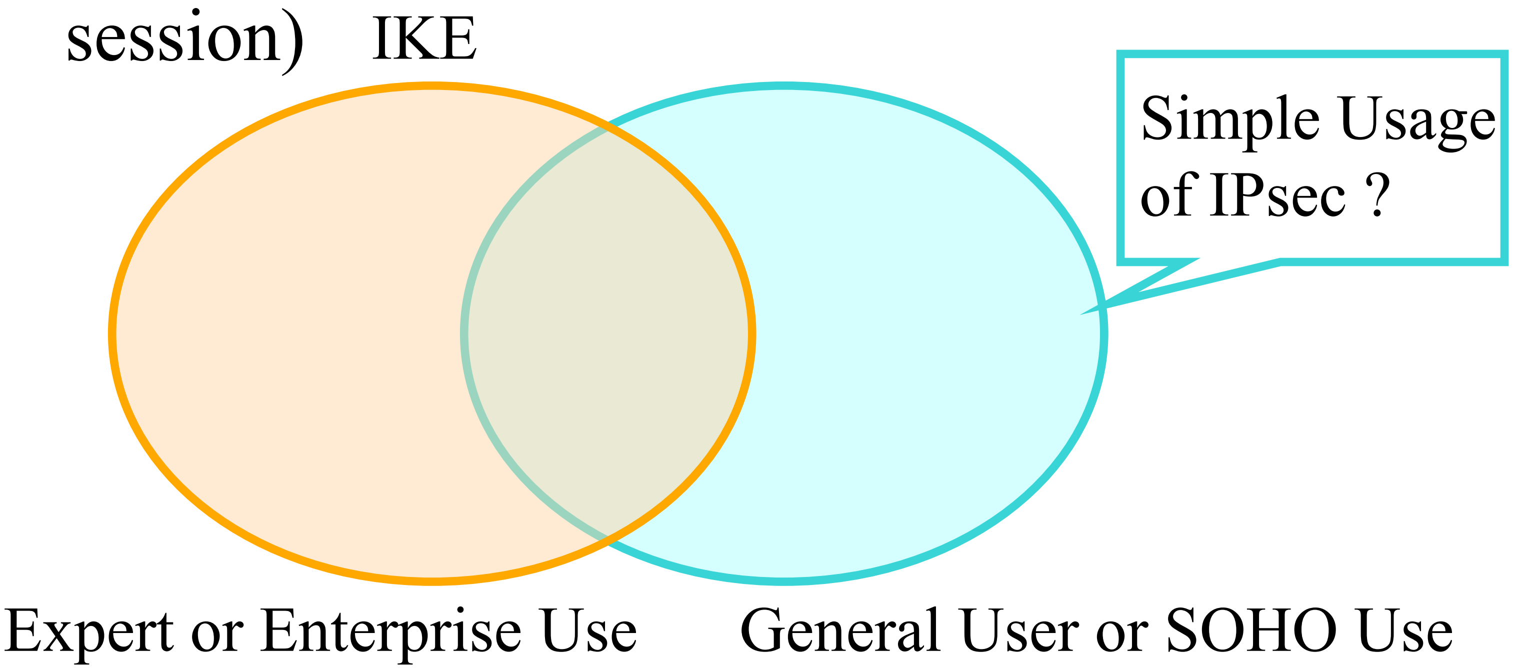
Proxy (ISP)

Sessions over IPsec

Why not use IKE?

- IKE would be a standard method.
  - We need a not-so-complicated option, too.
  - It’s quite efficient to make use of SDP.

    (ex: overhead at the beginning of media session)



Next Steps

Our Idea

- Framework such as sdescriptions or key-mgmt is suitable for this kind of usage.
- We hope for a guideline of extension for the protocols other than SRTP.

Any Comments or Questions ?
Interested in this requirement ?