Automated Security Association Management for Routing Protocols

draft-liang-karp-auto-sa-management-rp-00

IETF79 Beijing, China
November, 2010

Xiaoping Liang (Ellen)
ZTE Corporation
liang.xiaoping@zte.com.cn

Motivation

- SA provisioned to routing protocols is what we need to protect routing message essentially
- SAs of routing protocols are divers
- Automated management of SAs for routing protocols is desired and necessary
- Different keys management and their uses, and identity authentication, are involved in automated SA management system for routing protocols, and are indispensable parts of it

Goals

- Discuss automated security association (SA) management for routing protocols
- Discuss two candidate solutions of automated SA management that are based on IKEv2 and ISAKMP respectively

Prior Work

- RFC 4301 IPsec
- RFC 2408 ISAKMP
- RFC 4306, RFC 5996 IKEv2
- Draft-ietf-karp-framework-00
- Draft-ietf-karp-design-guide-01
- Draft-wei-karp-analysis-rp-sa-00

Draft Outline

- Automated SA management for routing protocols
- RP SA MGMT based on IKEv2 Extensions
- RP SA MGMT based on ISAKMP Extensions

* RP SA: Routing Protocol Security Association

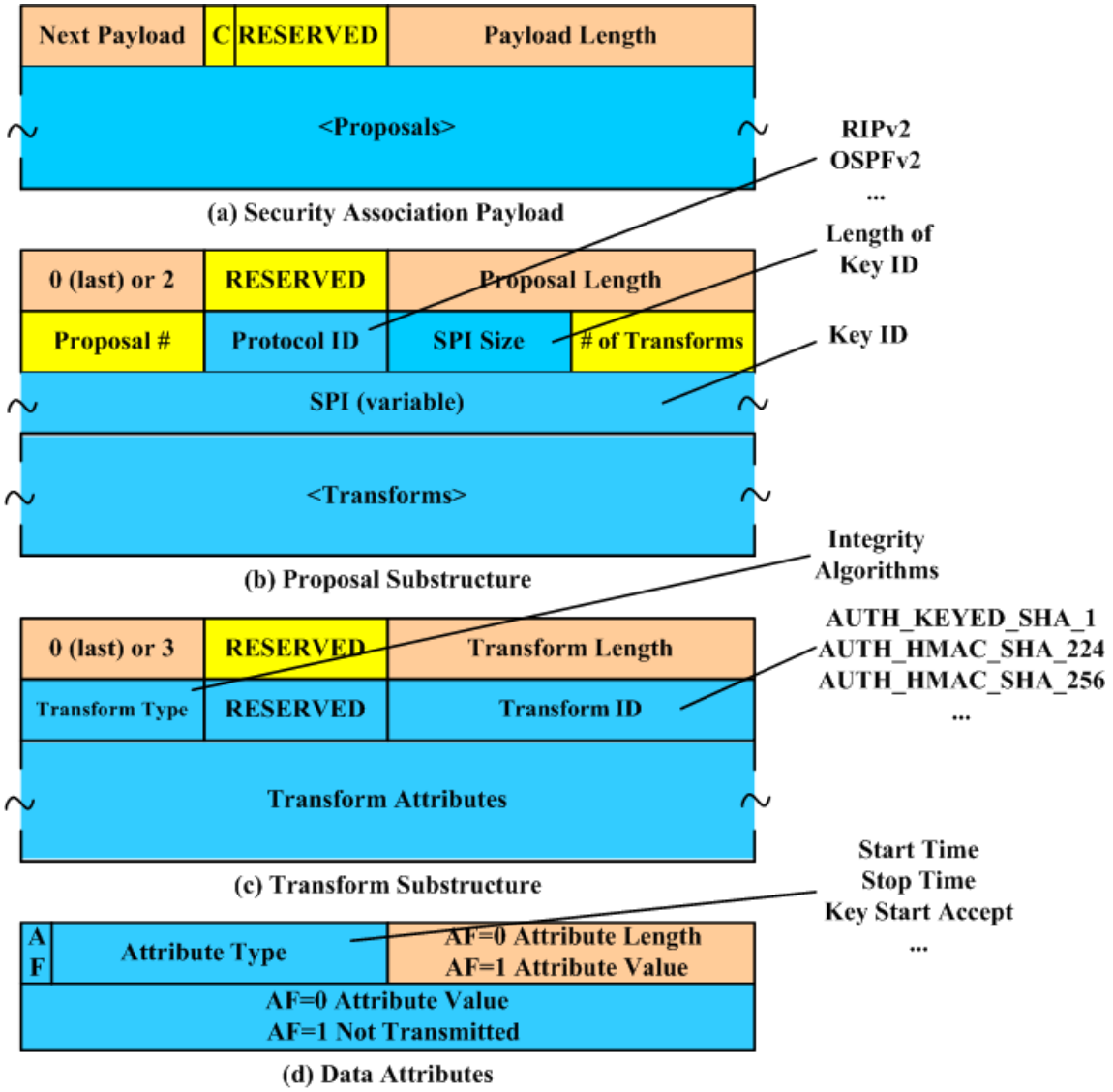
RP SA Establishment & Maintenance

- RP SA Attributes identified and unified Format
  - Key ID, authentication algorithm, authentication key, life time, sequence number, etc.; the direction
  - Interoperation; header format and payload format
- Secure Channel
  - Established before RP SA is transferred; encryption and message authentication and anti-replay
- RP SA Negotiation, Creation, and Distribution and Delivery
  - Motivation, procedure, payloads, what to negotiate
  - How to create
- RP SA Deletion, Update, and Rekey
  - Life time, life cycle
  - Adjacencies bouncing problem

IKEv2 Extensions 1/5

- Why using IKEv2
  - Existing mechanism for key management evolving along time, and is deploying by industry
  - Flexible and extensible naturally to support RP SA MGMT
- Extending SA Payload to support RP SA
- Adding New Payload to support RP SA
- Adding New Exchange Type to support RP SA negotiation

IKEv2 Extensions 2/5
-- Extending SA Payload



IKEv2 Extensions 3/5
-- Extending SA Payload

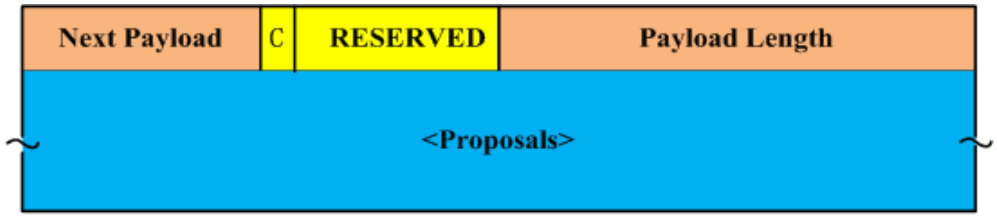
- IKE_SA_INIT exchange, secure channel established (IKE_SA)

```
     Initiator                    Responder
-----------------------------------------------------
   HDR, SAi, KEi, Ni -->

                        <--  HDR, SAr, KEr, Nr, [CERTREQ]
```

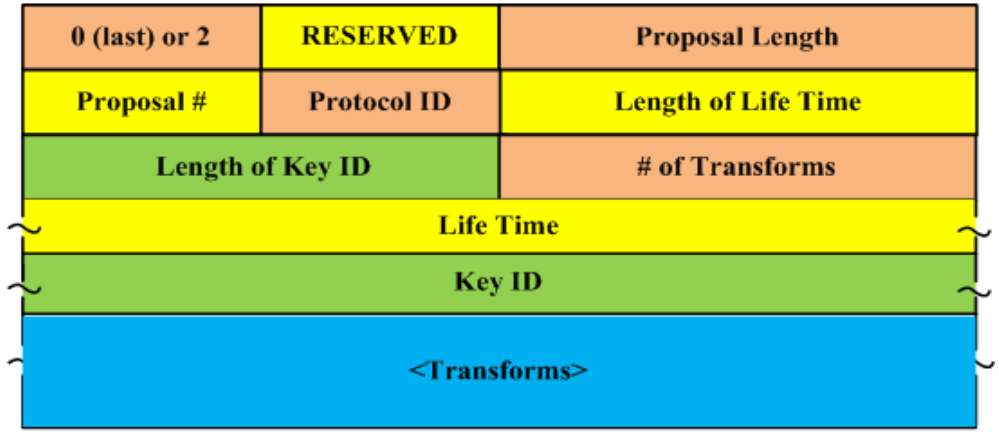
- IKE_AUTH exchange, RP SA negotiation

```
    Initiator                          Responder
-----------------------------------------------------------
 HDR, SK {IDi, [CERT,] [CERTREQ,]
   [IDr,] AUTH, SAe, TSi, TSr}  -->

                          <--  HDR, SK {IDr, [CERT,]
                               AUTH, SAe, TSi, TSr}
```

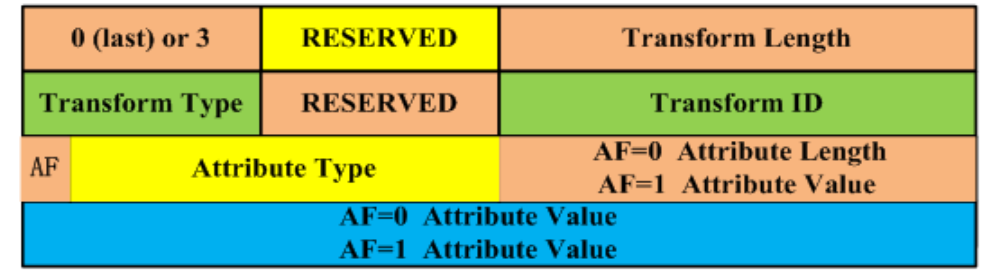
IKEv2 Extensions 4/5
-- Adding New Payload



（a）Security Association Payload for Routing Protocol (SARP)



（b）Proposal Substructure



（c）Transform Substructure

IKEv2 Extensions 5/5
-- Adding New Exchange Type

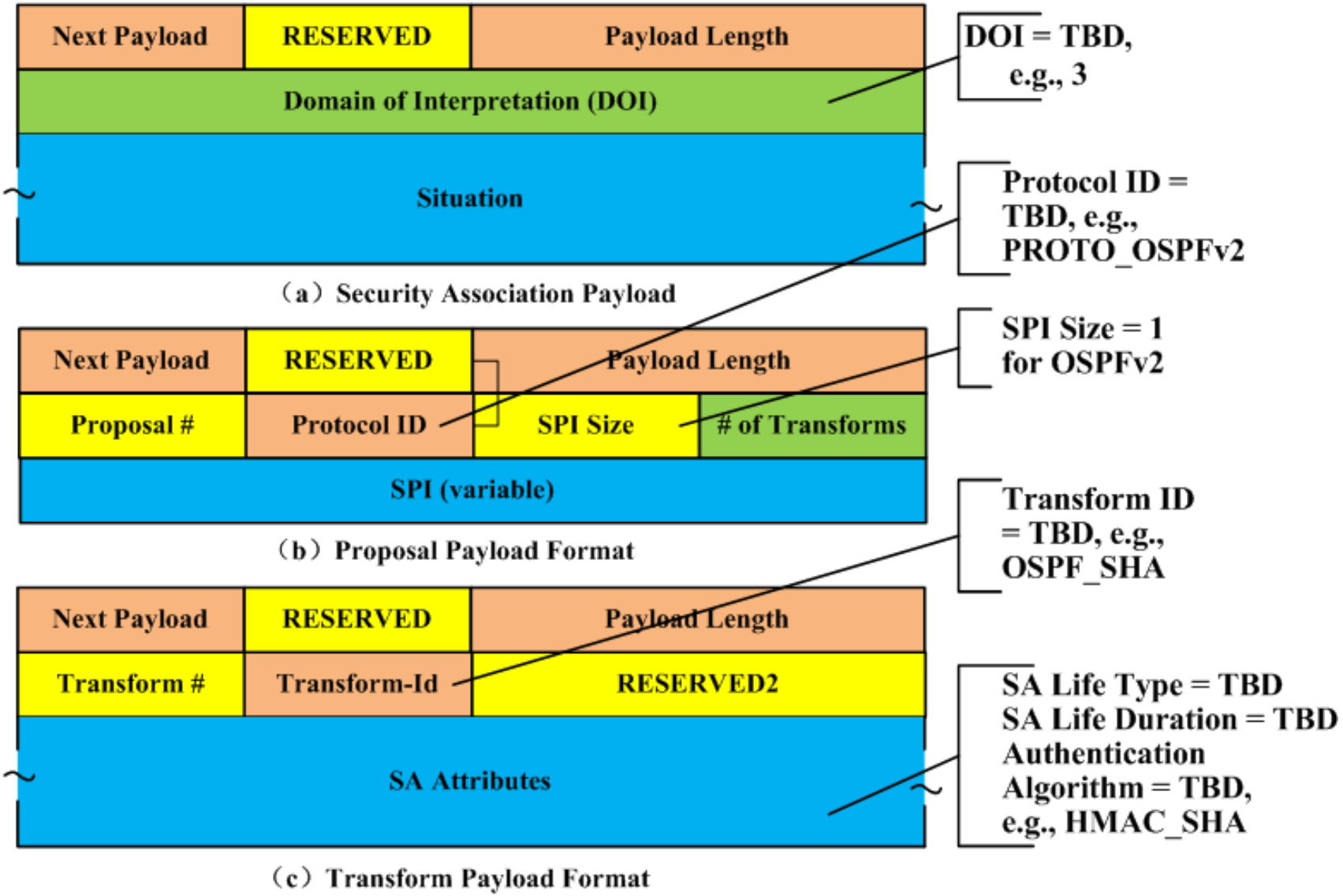
```
Initiator                                   Responder
-------------------------------------------------------------------
HDR, SK {SAei,Ni,[KEi,][...]}  -->

                        <--  HDR, SK {SAer,Nr,[KEr,][...]}
```

```
Initiator                                   Responder
-------------------------------------------------------------------
HDR, SK {SARPi, Ni, [KEi,][...]} -->

                        <-- HDR, SK {SARPr, Nr, [KEr,][...]}
```

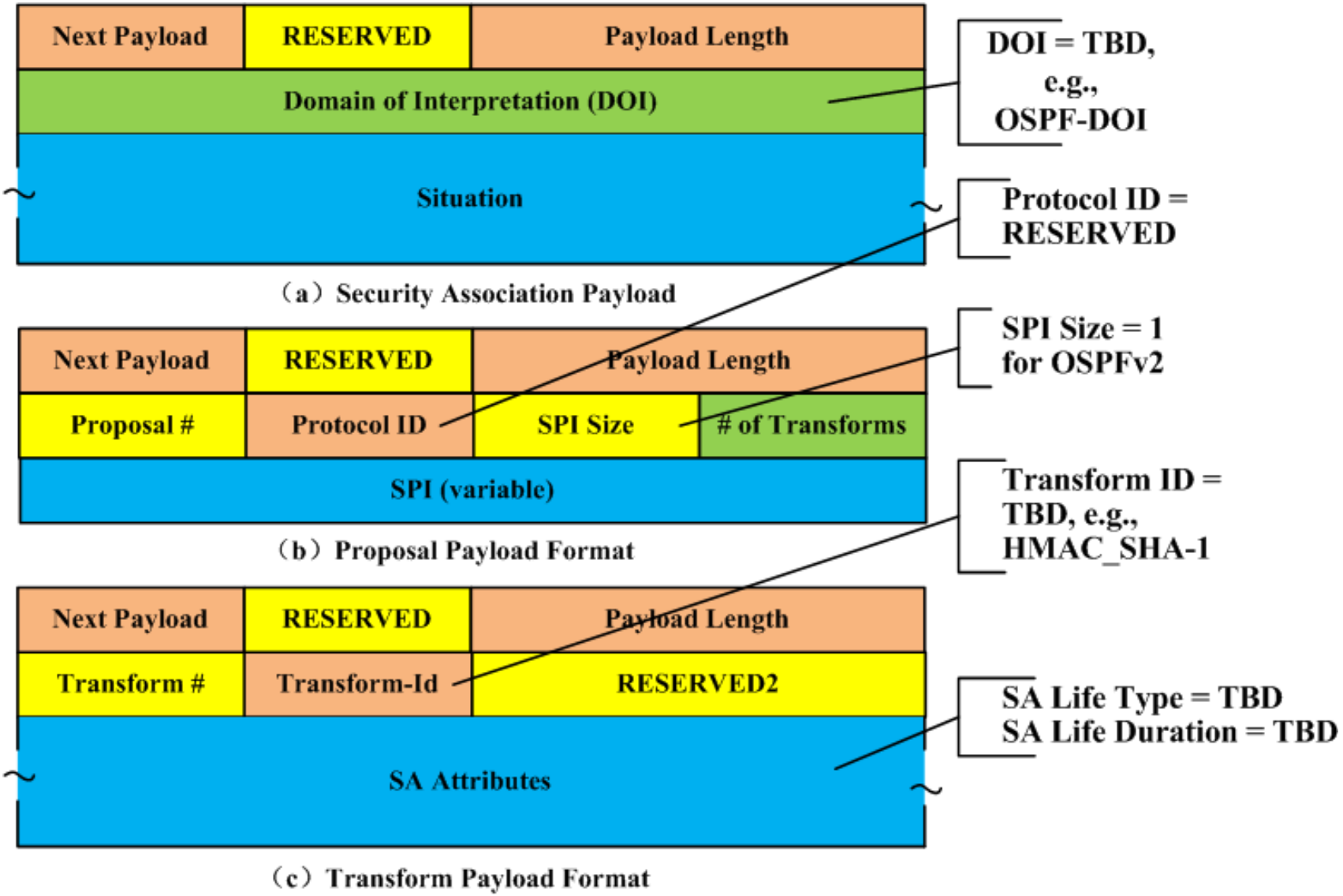
ISAKMP Extensions 1/3

- Why using ISAKMP
  - Intended to support the negotiation of SAs for security protocols at all layers of the network stack
  - Provides a framework but not define mechanisms
- Extension method:
  - Extend DOI of SA payload to indicate the subsequent payloads are used to negotiate RP SA
  - Extend Security Protocol Identifiers of proposal for RP SA
  - Match SPI field in proposal substructure to Key ID of RP SA, and extend SPI Size (in octet) field to indicate the length of Key ID of RP SA
  - Extend Transform Identifiers to define transform for routing protocol
  - Extend Attribute Type to support attributes of RP SA
- Alternatively, extend DOI field of SA payload to indicate the subsequent payloads will be used to negotiate RP SA for specific routing protocol

ISAKMP Extensions 2/3



ISAKMP Extensions 3/3



Summary of the Extensions

Options	Pros	Cons
Extend SA of IKEv2	Reuse IKEv2 at maximum	Extend IKEv2
Add new payload in IKEv2	Speed up RP SA payload processing	Extend IKEv2 one more step
Add new exchange in IKEv2	Speed up RP SA exchange	Extend IKEv2 two more steps
Extend payload in ISAKMP (1)	Reuse ISAKMP at maximum	Extend ISAKMP
Extend payload in ISAKMP (2)	More dedicated to specific RP	Extend ISAKMP By defining more DOI

We show one approach/direction to KMP for routing protocols!

Future Work

- Identity proof/authentication
- Group key management
- Inter-domain authentication
- …

WE NEED YOU!!!

Please review and consider taking this on as working group document

Q&A