Analysis of Security Association for Current Routing Protocol

draft-wei-karp-analysis-rp-sa-00

IETF78, Maastricht, Netherlands
July, 2010

Yinxing Wei, ZTE Corporation
wei.yinxing@zte.com.cn

Motivation

- Goal of KARP WG
  - KARP aims to improve the communication security of the packets on the wire used by the routing protocols

- Current State
  - Security Association (SA) is the basis for protecting the packet of routing protocol, e.g., message authentication, integrity protection
  - Many routing protocols have already defined their own SAs

➢ This document analyzes the SA of several routing protocols, i.e., RIPv2, OSPFv2, ISIS, BFD, and BGP

Our Work

- Briefly overview of existing SAs of routing protocols
- Compare typical fields of those SAs
- Identify potential issue and discuss possible approaches

Overview of SA fields

	Key Identifier	Algorithms	Key	Life Time	Sequence Number	KDF
RIPv2	√	√	√	√	√	
OSPFv2	√	√	√	√	√	
ISIS	√	√	√			
BFD	√	√	√		√	
BGP	√	√	√		√	√

Table 1 – Key identifier

Routing Protocol	Name of Key ID	Length of Key ID
RIPv2	Key Identifier	8 bits
OSPFv2	Key Identifier	8 bits
ISIS	Key Identifier	2 octets
BFD	Authentication Key Identifier	2 octets
BGP	KeyID	8 bits

Table 2 – Algorithms and Key Length

Routing Protocol	Algorithms	Key Length
RIPv2	KEYED-MD5, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	variable
OSPFv2	Keyed-MD5, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	variable
ISIS	HMAC-MD5, HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	variable
BFD	Keyed MD5, Keyed SHA-1, HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	variable
BGP	Keyed MD5, HMAC-SHA-1-96, AES-128-CMAC-96	variable

Table 3 – Life Time

Routing Protocol	Fields
RIPv2	Start Time, Stop Time
OSPFv2	Key Start Accept, Key Start Generate, Key Stop Generate, Key Stop Accept
ISIS	None
BFD	None
BGP	None

Table 4 – Sequence number

Routing Protocol	Length of Sequence number
RIPv2	32bits
OSPFv2	32bits
ISIS	None
BFD	32bits
BGP	32bits

Issues and Approaches

- Issues
  - The diversity of routing protocol SA
  - May impact on the design of KARP framework or KMP protocol
- Possible Approaches - generic SA (gSA)?
  - Pros
    - A bridge between manual configuration or KMP protocol and routing protocol
    - A unified interface to manual configuration or KMP protocol
    - Decouple KMP with routing protocol
    - KMP and routing protocol can be evolved independently
    - The complexity of the design of KMP is greatly reduced
  - Cons
    - A new layer is added , which produces extra cost

Next Step

- Take IPsec SA into account
- Adopted as a WG draft?