SRv6 Path Verification

draft-yang-spring-srv6-verification-04

Feng Yang(China Mobile)

Changwang Lin(New H3C Technologies)

Han Zhang(Tsinghua University)

IETF 125

History

This draft is targeted to address the SRv6 path modification or insertion in draft-ietf-spring-srv6-security, both on-path or off-path attack.

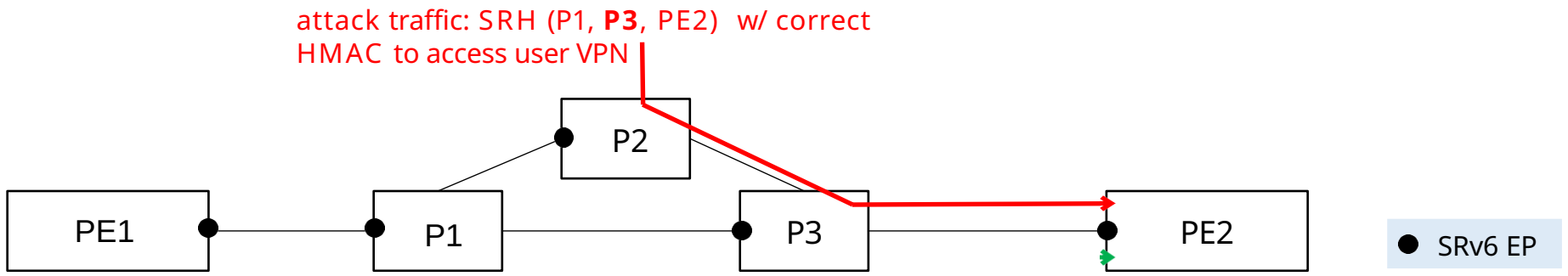
- This proposal was first presented in 122 meeting in SPRING WG.
  - linear combination of hop-by-hop authentication, auth(n)=alg(SID1) +.....+ alg(SIDn)
- Updated per mail discussion, and presented in 123 meeting.
  - Change linear combination of hop-by-hop authentication to recursive HMAC, auth(n)=alg_n(auth(n-1)) + alg_n(SIDn)
- Updated per comments of 123 meeting.
  - Add SRv6 SD-WAN and enterprise deployment cases, which is vulnerable to path manipulation.

Problem & Solution Recap

When running SRv6 in enterprise networks, path manipulation regard “Modification Attack” and “Packet Insertion” specified in draft-ietf-spring-srv6-security are relevant.

Problem

HMAC mechanism in RFC 8754 does not verify if the real forwarding path against SID list in packet



Solution

Recursive HMAC

```
auth=empty    auth=alg_1(auth)+alg_1(DA)   auth=alg_2(auth)+alg_2(DA)   auth=alg_3(auth)+alg_3(DA)

auth: Path verification TLV value in SRH
alg_n: hmac algorithm, alg_n(x) = hmac(k_n, x), k_n is the key on node n
DA: destination address of IPv6 packet
```

Benefits

Forwarding path will be strictly verified against SID list on tail node.

Constant auth code length in packet, regardless of length of SID list.

The amount of computation is just on DA (128 bits) and last hop authentication code (128 bits).

Next Step

If no objection, we would like to request WG adoption