An example of mobile user

Mobile device (IP_A) connects to Base station via PPPoE access (Circuit X). Frequently update IP address Anchors.

IP address | Anchors
---|---
IP_A | Circuit X

Base station also provides E1 access (Circuit Y) to SAVI device. Another table:

IP address | Anchors
---|---
IP_A | Circuit Y
Problems with L2 Anchors

- Mobile user may access to the network from different L2 anchors, e.g. circuit ID, which may change frequently
- Circuit ID may vary greatly in different access networks
  - MAC
  - Ethernet Port
  - VLAN
  - E1 Time slot
  - ...
- User with dual uplinks to a SAVI device
  - What anchor will be bound when the two uplinks has different circuit ID?
- **Shared key can be used as a common anchor**
Shared Key SAVI Highlight

- Each host shares a key with SAVI device
- Dynamic negotiation mechanism may be used for a host to acquire a shared key
- A user is identified by its IP address
- What is used for calculating signature is only IP address but not the whole IP packet
- Signature is carried by ICV (Integrity Check Value) field in IP Authentication Header

- Validate source addresses by shared keys
SKey SAVI Data structures

- IP address entry
  - IP source address
  - shared key
  - shared key lifetime
  - hash algorithm
Processing on Host

- Host Calculate its signature from its shared key and IP address with selected HASH algorithm
- The signature is inserted in to AH's ICV field
- Sequence Number Field may be used as nonce to prevent replay attack
AH with Signature in IPv4/v6

<table>
<thead>
<tr>
<th>IP Header</th>
<th>AH (ICV=Signature)</th>
<th>Upper Layer Header &amp; Data</th>
</tr>
</thead>
</table>

SKey signature in IPv4 packet

<table>
<thead>
<tr>
<th>IP Header</th>
<th>hop-by-hop, routing, fragment.</th>
<th>AH (ICV=Signature)</th>
<th>Dest. option</th>
<th>Upper Layer Header &amp; Data</th>
</tr>
</thead>
</table>

SKey signature in IPv6 packet

- SKey SAVI is applicable to both IPv4 and IPv6
- In IPv6 context, AH is viewed as an end-to-end payload, and thus should appear after hop-by-hop, routing, and fragmentation extension headers.
Processing on SAVI Device

- SKey SAVI computes a signature in a similar way as host.
- If the two signatures match, we can assert that the IP packet was sent from the legal owner of the IP address.

1. Packets received
2. Retrieve signature and User ID(S. IP@)
3. Obtain share key & HASH algorithm by User ID(S. IP@)
4. Calculate signature with SKey and S. IP@
5. Compare signatures
   - different
     - Illegal packet filtered or redirected
   - same
     - Legal packet forwarded
Advantages of SKey SAVI

- Link layer and physical layer info independent
- Applicable to both IPv4 and IPv6
- More efficient than IPsec
- SKey is more secure than L2 anchors
Next Steps?