IKEv2 with CGA

Jean-Michel Combes
<jeanmichel.combes@orange-ftgroup.com>

Aurélien Wailly
<aurelien.wailly@orange-ftgroup.com>
• CGA design
• IKEv2 quick overview
• IKEv2+CGA
• Implementation
• IKEv2+CGA and DNSSEC
CGA design

- Cryptographically Generated Addresses [RFC3972]
- Public/private key pair
- CGA Parameters

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Subnet Prefix</th>
<th>Collision Count</th>
<th>Public Key</th>
<th>Extension Fields</th>
</tr>
</thead>
</table>

- IPv6 address: Prefix (64 bits) || Interface ID (64 bits)
- Interface ID = First64(Hash(CGA Parameters))
IKEv2 quick overview

- **IKE_SA_INIT**

  Initiator
  ---------------
  HDR, SAi1, KEi, Ni

  Responder
  ---------------

              -->

  <-- HDR, SAR1, KER, Nr, [CERTREQ]

- **IKE_AUTH**

  Initiator
  ---------------
  HDR, SK {IDi, [CERT], [CERTREQ], [ CERTREQ], [ IDr,]
  AUTH, SAi2, TSi, TSr}

  Responder
  ---------------

              -->

              <-- HDR, SK {IDr, [CERT], AUTH,
  SAR2, TSi, TSr}
IKEv2+CGA (1/2)

- Based on draft-laganier-ike-ipv6-cga-02 (expired)
- CGA used as an alternative credential in IKE_AUTH
IKEv2+CGA (2/2)

- IDi, IDr
  - ID_IPV6_ADDR == CGA
- CERT
  - New type: 222
  - Includes CGA parameters
  - Format looks like a self-signed certificate
- CERTREQ
  - New type: 222
- AUTH
  - Signature based on the private key associated to the CGA public one
- Peer Authorization Database (PAD)
  - ID_IPV6_ADDR associated with CGA authentication method
First conclusions

• Implementation
  – Based on **StrongSwan**

• Advantages
  – Infrastructureless
    • Less entities than a classical trust infrastructure (e.g. PKI)
    • Less attack vectors than on certification path

• Drawbacks
  – Identity
    • CGA, hard to remember for a human
    • IPsec security policy only based on IP addresses
  – "Hard-coded" cryptographic algorithms
    • SHA1 mandatory
    • RSA (minimum key length is 384 bits)
  – Revocation
    • Not possible
IKEv2+CGA and DNSSEC

• Use of DNS
  – To set up IPsec security policy with FQDN
  – Potentially, to solve revocation issue

• Use of DNSSEC
  – To keep the same security level

• Implementation
  – Based on BIND
  – Partially implemented (issue with StrongSwan design)
Questions?