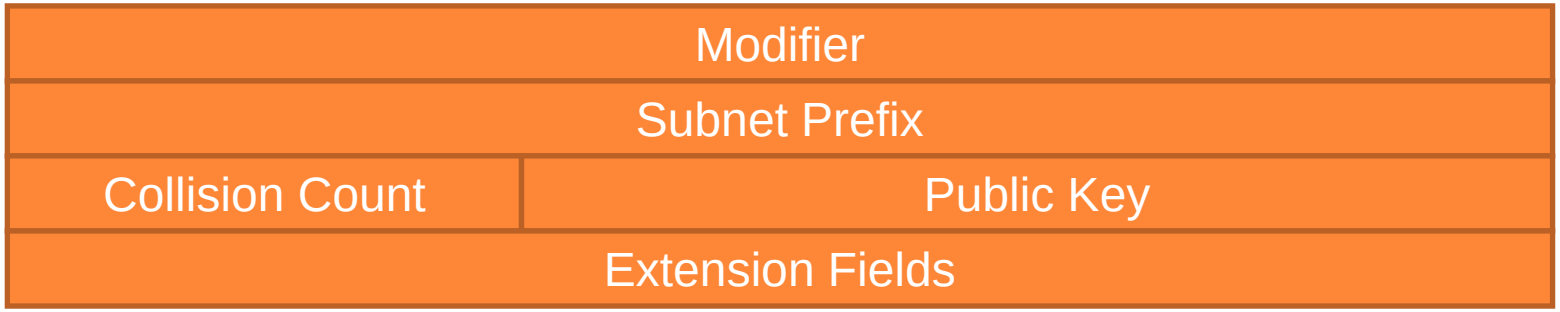
IKEv2 with CGA

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



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

IKEv2 quick overview

- IKE_SA_INIT

```
 Initiator                          Responder
-----------                        -----------
 HDR, SAi1, KEi, Ni    -->

                       <--    HDR, SAr1, KEr, Nr, [CERTREQ]
```

- IKE_AUTH

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

                                    <--    HDR, SK {IDr, [CERT,] AUTH,
                                                 SAr2, TSi, TSr}
```

IKEv2+CGA (1/2)

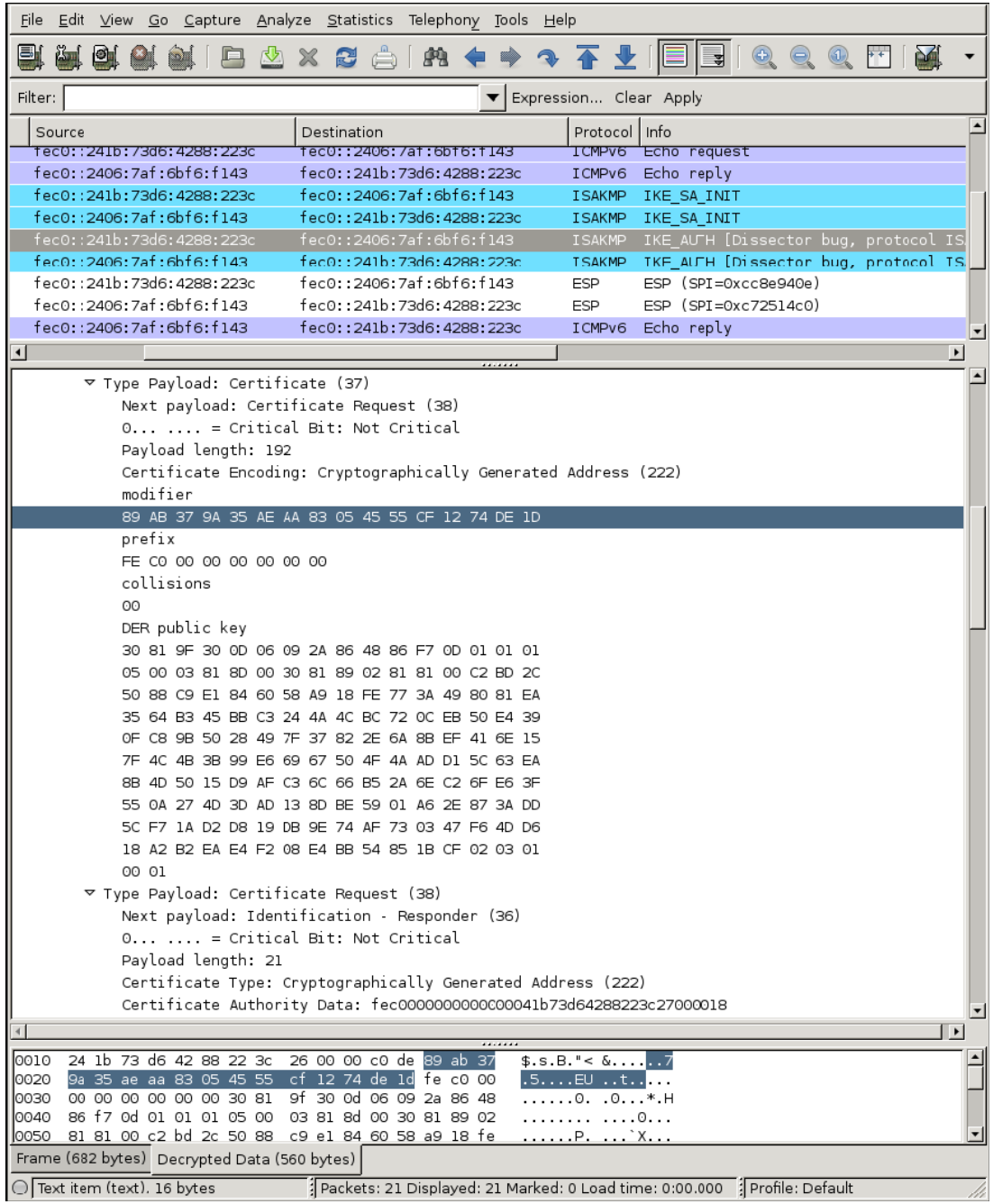
- Based on draft-laganier-ike-ipv6-cga-02 (expired)
- CGA used as an alternative credential in IKE_AUTH

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


File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
Source Destination Protocol Info
fec0::241b:73d6:4288:223c fec0::2406:7af:6bf6:f143 ICMPv6 Echo request
fec0::2406:7af:6bf6:f143 fec0::241b:73d6:4288:223c ICMPv6 Echo reply
fec0::241b:73d6:4288:223c fec0::2406:7af:6bf6:f143 ISAKMP IKE_SA_INIT
fec0::2406:7af:6bf6:f143 fec0::241b:73d6:4288:223c ISAKMP IKE_SA_INIT
fec0::241b:73d6:4288:223c fec0::2406:7af:6bf6:f143 ISAKMP IKE_AUTH [Dissector bug, protocol IS
fec0::241b:73d6:4288:223c fec0::2406:7af:6bf6:f143 ESP ESP (SPI=0xcc8e940e)
fec0::2406:7af:6bf6:f143 fec0::241b:73d6:4288:223c ESP ESP (SPI=0xc72514c0)
fec0::2406:7af:6bf6:f143 fec0::241b:73d6:4288:223c ICMPv6 Echo reply
Type Payload: Certificate (37)
Next payload: Certificate Request (38)
0... .... = Critical Bit: Not Critical
Payload length: 192
Certificate Encoding: Cryptographically Generated Address (222)
modifier
89 AB 37 9A 35 AE AA 83 05 45 55 CF 12 74 DE 1D
prefix
FE C0 00 00 00 00 00 00
collisions
00
DER public key
30 81 9F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01
05 00 03 81 8D 00 30 81 89 02 81 81 00 C2 BD 2C
50 88 C9 E1 84 60 58 A9 18 FE 77 3A 49 80 81 EA
35 64 B3 45 BB C3 24 4A 4C BC 72 0C EB 50 E4 39
0F C8 9B 50 28 49 7F 37 82 2E 6A 8B EF 41 6E 15
7F 4C 4B 3B 99 E6 69 67 50 4F 4A AD D1 5C 63 EA
8B 4D 50 15 D9 AF C3 6C 66 B5 2A 6E C2 6F E6 3F
55 0A 27 4D 3D AD 13 8D BE 59 01 A6 2E 87 3A DD
5C F7 1A D2 D8 19 DB 9E 74 AF 73 03 47 F6 4D D6
18 A2 B2 EA E4 F2 08 E4 BB 54 85 1B CF 02 03 01
00 01
Type Payload: Certificate Request (38)
Next payload: Identification - Responder (36)
0... .... = Critical Bit: Not Critical
Payload length: 21
Certificate Type: Cryptographically Generated Address (222)
Certificate Authority Data: fec0000000000c00041b73d64288223c27000018
0010 24 1b 73 d6 42 88 22 3c 26 00 00 c0 de 89 ab 37 $.s.B."< &.....7
0020 9a 35 ae aa 83 05 45 55 cf 12 74 de 1d fe c0 00 .5....EU ..t.....
0030 00 00 00 00 00 00 30 81 9f 30 0d 06 09 2a 86 48 ......0. .0...*.H
0040 86 f7 0d 01 01 01 05 00 03 81 8d 00 30 81 89 02 ....0...
0050 81 81 00 c2 bd 2c 50 88 c9 e1 84 60 58 a9 18 fe ......P. ...`X...
Frame (682 bytes)
Decrypted Data (560 bytes)
Text item (text). 16 bytes
Packets: 21 Displayed: 21 Marked: 0 Load time: 0:00.000
Profile: Default

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?