MOBIKEv2: MOBIKE extension for Transport mode

draft-mglt-ipsecme-mobikev2-00.txt

D. Migault, D. Palomares

07/25/2014 extitle- IETF90- Toronto

Motivations & Goals

Extends MOBIKE for IPsec transport mode

Why do we want using MOBIKE and the transport mode:

- Avoid an unecessary IP header
- Transport is used for E2E communication (offloading DNS...)

Design Principle:

- Re-use MOBIKE signaling
- Agree you support MOBIKE for transport mode

MOBIKE Version Negociation

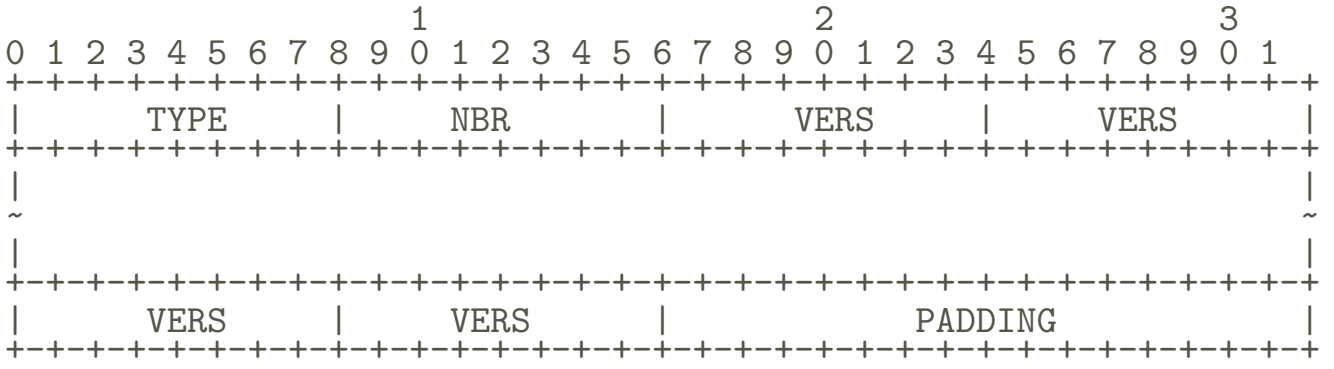
```
Initiator                   Responder
------                    ------
1) (IP_I1:500 -> IP_R1:500)
   HDR, SAi1, KEi, Ni ->
        N(NAT_DETECTION_SOURCE_IP),
        N(NAT_DETECTION_DESTINATION_IP)  ->

                        <-  (IP_R1:500 -> IP_I1:500)
                             HDR, SAr1, KEr, Nr,
                                  N(NAT_DETECTION_SOURCE_IP),
                                  N(NAT_DETECTION_DESTINATION_IP)

2) (IP_I1:4500 -> IP_R1:4500)
   HDR, SK { IDi, CERT, AUTH,
             CP(CFG_REQUEST),
             SAi2, TSi, TSr,
             N(MOBIKE_SUPPORTED, V1, V2}
                      ->

                       <-  (IP_R1:4500 -> IP_I1:4500)
                             HDR, SK { IDr, CERT, AUTH,
                                       CP(CFG_REPLY),
                                       SAr2, TSi, TSr,
                                       N(MOBIKE_SUPPORTED, V2}
```

Version Parameter Payload



MOBIKEv2 and IANA

```
Registry:
Value         NOTIFY PARAMETER - MOBIKEv2    Reference
------  --------------  -----
0             Reserved
1             Version
2-255         Reserved to IANA
```

```
Name                                  Value    Reference
--                                  ---    -----
MOBIKE_UNSUPPORTED_VERSION            8192
```

Notify Message - error type - Private values

IPsec DataBase Impact

The main difference between transport mode and tunnel mode, is:

- Updated IP address is a Traffic Selector

Impact on SPD:

- SPD is not modified
- Only SPD-cache is updated

Impact SAD:

- TS are modifed

Impact on the PAD:

- PAD match MUST be performed before performing the update

Next

Conclusion:

- MOBIKEv2 is a way to perform Mobility with the IPsec transport mode.
- MOBIKEv2 is compatible with MOBIKE
- Requires very few modifications to MOBIKE
- We have implemented this extention on Strongswan

Position toward BEET mode:

- BEET mode prevents transporting the tunnel header
- Upgrading IKEv2 is easier than upgrading IPsec

Thank you for your attention