École Nationale Supérieure
des Télécommunications de Bretagne

ENST Bretagne

IKEv2 Address Management

Francis.Dupont@enst-bretagne.fr

www.enst-bretagne.fr

Groupe des écoles
des télécommunications

Terminology

- Peer addresses:
  - Term from an old PKI for IPsec document
  - The addresses IKE runs over
  - Endpoint addresses of IPsec tunnel SAs
  - Loose (in IKEv2) relationship with IP address ID payload

draft-dupont-ikev2-addrmgmt-04.txt

- Goals:
  - Multi-homing (multiple peer addresses)
  - Mobility (peer address changes)
  - New transport protocols (SCTP, ...)
  - Security, flexibility, simplicity
- No goals:
  - NAT traversal
- Devices:
  - Peer addresses as IKE SA parameters
  - Special handling/clarification of transport mode
  - Peer address sets (new notification)
  - Explicit peer address update (new payload)

Peer addresses (security)

- Security aspects
  - No 3rd party bombing (aka. reflection attack)
  - Change in transit (transient pseudo-NAT attack)
  - Return routability check
  - Binding with certificates, ...

Peer addresses (sets)

- Address sets:
  - Initiated in the second exchange
  - Validated against authentication
  - Can be changed at any time
  - Ordering can carry some meaning?

Transport mode

- Proxy mode:
  - When the Traffic Selector doesn't match the peer address, follow the Traffic Selector
  - Security issue: proper authorization **is** needed
    - Proposal: accept it when the Traffic Selector is in the address set
- Peer address changes:
  - Transport mode SAs are not concerned

Peer address update

- Change the endpoint addresses of IPsec or IKE SAs
- List of SAs to update, but
- An “all SAs” flag
- Possible return routability check
- New payload

Conclusion

- Three items:
  - Requirements
  - Mechanisms
  - Policies
- Nothing about header compression