IKE Context Transfer in an IPv6 Mobility Environment

Fabien Allard (FT R&D)
Jean-Marie Bonnin (Télécom Bretagne)
Jean-Michel Combes (FT R&D)
Julien Bournelle (FT R&D)

MobiArch'08 - Seattle (WA) – 22/08/08
Summary

- Context Transfer use case: IPsec / IKEv2
- Solution against SPI collision: a MOBIKE extension
- Implementation of CXTP for IPsec / IKE in a IPv6 mobility environment
- Conclusion & Future work
Context Transfer use case: IPsec / IKEv2

- **Issue:**
  - Security provisioning is a major requirement in an all-IP-based network architecture providing multimedia services.
  - In a mobility context, security between mobile nodes and network access equipments must be set up from scratch after each HandOver (HO) and for each customer.
  - In the case where an **IPsec tunnel** is dynamically set up between a Mobile Node (MN) and a Security Gateway (SG) using IKE:
    - **IPsec and IKE contexts** are created in the MN and the SG.
  - IKE signalisation
    - lot of message exchanges (specially when EAP is used)
    - cryptographic computation time for keys generation
  
=> takes a significant amount of time, crucially affecting the handoff performance

- **Proposed solution to re-establish the security parameters:**
  - **Transfer of IPsec / IKE contexts between SG using CXTP** (RFC 4067)
Context Transfer use case: IPsec / IKEv2

pSG = previous Security Gateway
nSG = new Security Gateway
Context Transfer use case: IPsec / IKEv2

**IPsec context** = \((SAD^1 + SPD^2 + PAD^3)\) contexts + IKE\(^4\) context

1. **Security Association Database**
   - Consulted in order to know how to process each packet (AH/ESP)
     - **SPI**, **Source/Destination IP addresses**, IPsec protocol (AH/ESP)
     - Sequence counter number, anti-replay window
     - AH/ESP algorithms and keys
     - IPsec mode (tunnel or transport)
     - Path MTU
     - IPsec SA lifetime

2. **Security Policy Database**
   - Defines the security policy to apply to each packet (IPSEC/BYPASS/DISCARD)
     - **Inner source/destination IP addresses**
     - Upper protocol
     - Security policy
Context Transfer use case: IPsec / IKEv2

3. **Peer Authentication Database**
   - Identifies the peers that are authorized to communicate with the SG
     - Identifier
     - Authentication protocol and method
     - Pre-shared key or X.509 certificate

4. **Internet Key Exchange**
   - Sets up the IPsec SAs dynamically between two network equipments.
     - Initiator and responder **SPI**
     - Initiator and responder Nonces
     - Cryptographic algorithms
     - SKEYSEED (from which all keys are derived)
     - Lifetime
Solution against SPI collision: a MOBIKE extension

- SPI (Security Parameter Index)
  - Uniquely identifies the initiator or responder of a SA
  - SPI for IKE SA and SPI for IPsec SA

- Issue:
  - After a Context Transfer, SPIs may need to be updated if they are already in use in the nSG
  - SPI collision
  - In this case, new SPIs must be negotiated between the MN and the nSG

- Proposed solution:
  - Definition of a MOBIKE extension (UPDATE_SPI message type) in order to handle the SPI negotiation between the MN and the nSG

- What is MOBIKE?
  - IKEv2 Mobility and Multihoming Protocol
  - Allows to update IP addresses of an IPsec tunnel created with IKEv2

MobiArch'08 – Seattle (WA)
Solution against SPI collision: a MOBIKE extension

- IKE_INIT_SA
- IKE_AUTH(MOBIKE_SUPPORTED)
- CREATE_CHILD_SA

Previous IPsec tunnel (pCoA – pRA)

IKEv2 exchanges

CTAR (IPsec)
CT-Req (IPsec)
CTD (SPD + PAD + SAD + IKEv2 Ctxt)

L2 / L3 HO => new CoA

Previous IPsec tunnel transferred (pCoA – pRA)

(nAR -> nCoA) HDR, SK{N(UPDATE_SA_ADDRESSES), N(UPDATE_SPI), ...}
(nCoA -> nAR) HDR, SK{N(UPDATE_SPI), ...}
(nAR -> nCoA) HDR, SK{N(UPDATE_SPI)}

Updated IPsec tunnel (nCoA – nRA)
Implementation of CXTP for IPsec / IKE in a IPv6 mobility environment - Testbed

- Local platform
  - FreeBSD
  - KAME snap for IPv6 mobility support
  - Racoon for IKEv1 negociation
Implementation of CXTP for IPsec / IKE in a IPv6 mobility environment - Results

- UDP traffic generator with 50ms delay between each packet.
- Mobile IPv6 HO delay is not take into account.
- Only focused on the security set up delay
  - during this time, all UDP packets are lost

<table>
<thead>
<tr>
<th>IKEv1 mode</th>
<th>Average delay (in ms)</th>
<th>Number of messages</th>
<th>Total size of messages (in Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKEv1 main mode</td>
<td>1500</td>
<td>11</td>
<td>2182</td>
</tr>
<tr>
<td>IKEv1 aggressive mode</td>
<td>1300</td>
<td>8</td>
<td>1896</td>
</tr>
<tr>
<td>IKEv1 with context transfer optimisation</td>
<td>20</td>
<td>1</td>
<td>106</td>
</tr>
</tbody>
</table>
Conclusion & Future work

- Paper set out
  - an application of the context transfer for IPsec/IKE
  - a solution against the SPI collision using a MOBIKE extension
  - a set of practical results showing that CT for IPsec can drastically reduce the time needed to re-establish an IPsec tunnel after a HO.

- Main gains of context transfer for security
  - Performance improvements for IPv6 mobility environment
  - Less security signalisation in the core network

- Future work
  - CXTP for IKEv2 implementation
    - Comparison results with and without using CT optimisation
Questions ?
Implementation of CXTP for IPsec / IKE in a IPv6 mobility environment - Results

- $\alpha$
  - HO delay
- $\beta$
  - IKEv1 with CT optimisation delay to re-establish the IPsec tunnel
- $\gamma$
  - IKEv1 in aggressive mode delay to re-establish the IPsec tunnel
- $\delta$
  - IKEv1 in main mode delay to re-establish the IPsec tunnel

---

*MobiArch’08 – Seattle (WA)*
Implementation of CXTP for IPsec / IKE in a IPv6 mobility environment - Testbed

- **CXTP module**
  > follows RFC4067

- **IPsec CXTP module**
  > PF_KEYv2 API
  > links CXTP module with FreeBSD kernel’s databases (SAD + SPD contexts)
  > links CXTP module with Racoon (IKEv1 context)

- Communication through a shared memory