Security Analysis of IPv6 mobility

Kiran Isaac Abraham, Kushal Tayal and Siddhi Soman
IPv6 Mobility

• Allow mobile nodes to continue communication while moving from one location to another.
• If a node could maintain its IP address as it moves, then it can maintain its transport and higher layer link connections at its new location.
Terminology

- Internet
- Home Agent
- Mobile Node
- Home Address
Terminology

- Internet
- Home Agent
- Mobile Node
- Home Address
- Corresponding Node
- Correspondent Address
Basic Operation

Internet

Mobile Node

Home Agent

Home Address

Corresponding Node
Basic Operation

Internet

Home Agent

Home Address

Care of Address

Mobile Node

Corresponding Node
Return Routeability Procedure

<table>
<thead>
<tr>
<th>HoTi</th>
<th>Source</th>
<th>HA</th>
<th>Dest</th>
<th>CN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Home Init Cookie</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Internet

Home Agent

Corresponding Node

HoTi

Mobile Node

Care of Address

HoTi

Source

HA

Dest

CN
Return Routeability Procedure

<table>
<thead>
<tr>
<th>Source</th>
<th>CoA</th>
<th>Dest</th>
<th>CN</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoTi</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Home Agent

Internet

Corresponding Node

HoTi

CoTi

Care-of Init Cookie

Mobile Node

Care of Address
Return Routeability Procedure

<table>
<thead>
<tr>
<th>HoT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
</tr>
<tr>
<td>CN</td>
</tr>
<tr>
<td>Dest</td>
</tr>
<tr>
<td>HA</td>
</tr>
</tbody>
</table>

\[
K0 = \text{First (64, HMAC\_SHA1 (Kcn, (HA | nonce | 0 )))}
\]
Return Routeability Procedure

<table>
<thead>
<tr>
<th>CoT</th>
<th>Source</th>
<th>CN</th>
<th>Dest</th>
<th>CoA</th>
</tr>
</thead>
<tbody>
<tr>
<td>K1</td>
<td>First(64, HMAC_SHA1 (Kcn, (CoA</td>
<td>nonce</td>
<td>1 )))</td>
<td></td>
</tr>
</tbody>
</table>
Binding Update

<table>
<thead>
<tr>
<th>BU</th>
<th>Source</th>
<th>CoA</th>
<th>Dest</th>
<th>CN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HA, Seq No, H-NIdx, Co-NIdx,</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

First (96, HMAC_SHA1 (SHA1(K0|K1), (CoA |CN | BU )))
Attacks
Man in the Middle Attack

- Attacker sits between the two Home Agents

- Attacker then initializes return routeability procedure with MN pretending CN has moved and does the same with CN by informing it that MN has moved.
**Man in the Middle Attack**

- Attacker sits between the two Home Agents

- Attacker then initializes return routeability procedure with MN pretending CN has moved and does the same with CN by informing it that MN has moved.
Man in the Middle Attack

- Attacker sits between the two Home Agents
- Attacker then initializes return routeability procedure with MN pretending CN has moved and does the same with CN by informing it that MN has moved.
Man in the Middle Attack

- Attacker sits between the two Home Agents

- Attacker then initializes return routeability procedure with MN pretending CN has moved and does the same with CN by informing it that MN has moved.
Man in the Middle Attack

- Attacker sits between the two Home Agents
- Attacker then initializes return routeability procedure with MN pretending CN has moved and does the same with CN by informing it that MN has moved.
Man in the Middle Attack

- Attacker sits between the two Home Agents.
- Attacker then initializes return routeability procedure with MN pretending CN has moved and does the same with CN by informing it that MN has moved.
Man in the Middle Attack

- Attacker sits between the two Home Agents.
- Attacker then initializes return routeability procedure with MN pretending CN has moved and does the same with CN by informing it that MN has moved.
Man in the Middle Attack

- Attacker sits between the two Home Agents
- Attacker then initializes return routeability procedure with MN pretending CN has moved and does the same with CN by informing it that MN has moved.
Man in the Middle Attack

- Attacker sits between the two Home Agents
- Attacker then initializes return routeability procedure with MN pretending CN has moved and does the same with CN by informing it that MN has moved.
Man in the Middle Attack

- Attacker sits between the two Home Agents
- Attacker then initializes return routeability procedure with MN pretending CN has moved and does the same with CN by informing it that MN has moved.

Diagram:
- Mobile Node
- Home Agent 1
- Home Agent 2
- Corresponding Node
- Internet
- Attacker
- HoTi
- CoTi
- HoT
- CoT
- CN
- MN
- BU
- Hurray!
DDoS Attack

- 2 types
  - MN malicious
  - HA-MN both malicious

- Malicious Mobile node does a binding update with target node’s address as its own Care-of-Address and forwards traffic to target node.
DDoS Attack

- 2 types
  - MN malicious
  - HA-MN both malicious

Malicious Mobile node does a binding update with target node’s address as its own Care-of-Address and forwards traffic to target node.
DDoS Attack

- 2 types
  - MN malicious
  - HA-MN both malicious

- Malicious Mobile node does a binding update with target node’s address as its own Care-of-Address and forwards traffic to target node.
DOS attack

- The attacker can compromise one of the HA-CN or CN-MN paths to block Binding Update procedure.

- Results in non-optimized routing of data and a Denial of Service attack at the HA node.
Minor Attacks

Security Association Attack
  • Use IPSec Security Association with HA to start BU for another MN under the same HA.

Fake HoTi-CoTi packets
  • An attacker node can spam CN with fake packets for the return routeability procedure and overload the CN by forcing it to generate HoT and CoT packets.

Fake Binding Update packets
  • As per the RFC, if CN receives excessive number of false BU packets, it blocks further BU packets.

Block and Replay BU
  • An attacker can block final BU packet and hold until MN moves to new location, then replay the BU packet to CN, thereby establishing connection with some arbitrary node at that CoA.
Defenses
Defense for MiTM attack

• Need of 2-way authentication as MN and CN do not know each other.
• Can use certificates to authenticate each other.
• Need of a trusted Certificate Authority for this purpose.
• Two ways –
  • manual authentication
  • establishing shared secret key
• Another method that can be used is latency examination but it assumes correct packet delivery, no packet loss, etc.
Defense for DDoS and DoS

DDoS:
• MN needs to identify itself to the CN.
• CN then can query the HA on foreign network to verify the identity of MN.

DoS:
• We can set a threshold at the HA on the capacity of the network flow being utilized and force the return routeability procedure.
• It will help reduce latency issues and chances of DoS attack.
Other Defenses

• We can have one-to-one security association between HA and MN which will prevent MN misusing its authorization with HA.
• Web trust of Home Agents.
• Proper configuration is very important e.g. setting parameters like nonce lifetime, number of messages after which binding update request might be rejected by CN etc. properly.
• Proper implementation of nonce and nonce index etc.
• Good configuration of ICMP packets and the procedures to handle ICMP packets can help prevent some attacks.
Murphi – Message Types

MessageType : enum {

  M_MN_HA_HOTI, -- 1. MN->HA: \{Nhoti\}Kha
  M_HA_CN_HOTI, -- 2. HA->CN: Nhoti
  M_MN_CN_COTI, -- 3. MN->CN: Ncoti
  M_CN_HA_HOT, -- 4. CN->HA: \{Nhoti,KeygenHome, nonceIndex\}
  M_HA_MN_HOT, -- 5. HA->MN: \{Nhoti,KeygenHome, nonceIndex\}Kmn
  M_CN_MN_COT, -- 6. CN->MN: \{Ncoti, KeygenCare, NonceIndex\}
  M_FINAL,
  M_SUCCESS,
  M_FAIL
};
Murphi - States

MobileNodeStates : enum {
  I_NO_MOBILITY,
  I_NOT_STARTED,  -- state after initialization
  I_STARTED,
  I_WAIT,        -- waiting for response from responder
  I_RECD1,
  I_RECD2,
  I_FINAL_WAIT,
  I_SUCCESS,
  I_FAIL
};
Murphi - Invariant

MN[MN[mob_node1].CorrespondingNode].CareOf =
  MN[mob_node1].cacheCorrespondingNode
&
MN[MN[mob_node2].CorrespondingNode].CareOf =
  MN[mob_node2].cacheCorrespondingNode
Conclusion

• IPv6 mobility – very effective and simplistic design.
• It introduces a lot of subtle variations making it difficult for an attacker to attack the system and reduces the possibility of an attack to a great extent.
• However attacks are still possible on the system.
• The different security measures which we proposed can be made optional depending on the requirements of the network.
• The specification provides decent security and has limited the attacks to very specific scenarios. Further analysis and inclusion of security measures depends on the tradeoff between security v/s usability and cost.