Security Architectures for Mobile IPv6

Euro6IX/ 6NET Workshop, Limerick, Ireland
Wednesday June 5th 2002

Thomas Scheffler
T-Systems Nova GmbH
Berkom
thomas.scheffler@t-systems.com
Overview

- Work in the 6WINIT Project
- Security Analysis of Mobile IPv6
- Possible Security Architecture
- Implementation
- Outlook
Validate introduction of Wireless Internet in Europe

- Based on IPv6 + GPRS and UMTS/3GPP
- Both personal and terminal mobility
- Full range of IPv6 Facilities
- Procedures for IPv6-2-3G Nets
  - Including IPv4/IPv6 network and application integration
- Investigate problems providing a trans-national wireless delivery service
- Early IPv6-ready applications testing
- Implement handsets and edge devices

Validate the feasibility of running real applications
Mobile Scenarios are designed to provide freedom for the user to roam about - they are susceptible to by their very design

- distinguishing between legitimate and illegitimate use
- authentication, authorisation and accounting of use across administrative domains
- denial of service
- creating, distributing and enforcing policies
- eavesdropping
Security Analysis of Mobile IPv6

<table>
<thead>
<tr>
<th>Tread</th>
<th>Possible Solution</th>
<th>Abbr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Man in the Middle</td>
<td>Authentication of Control Messages</td>
<td>MITM</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>Line Encryption</td>
<td>S</td>
</tr>
<tr>
<td>Manipulation of Binding Cache (DoS)</td>
<td>Authentication of Control Messages</td>
<td>DOS</td>
</tr>
<tr>
<td>ICMP Attack</td>
<td>Access Lists for ICMP Requests on Router</td>
<td>DOS</td>
</tr>
<tr>
<td>Unauthorised Access</td>
<td>User Authentication, Access Lists, AAA</td>
<td>UZ</td>
</tr>
<tr>
<td>Session Stealing</td>
<td>Authentication of Control Messages</td>
<td>MN-SS  CN-SS</td>
</tr>
<tr>
<td>Profiling</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Security Analysis of Mobile IPv6

Currently most MIPv6 Implementations do not support secure control messages.

- A number of security issues is left to other protocols
- Scalability issues due to lack of ‘Global PKI’

<table>
<thead>
<tr>
<th>Company / Project</th>
<th>Open Source</th>
<th>Draft Status</th>
<th>Security</th>
<th>Platform</th>
<th>Further Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ericsson/Telebit</td>
<td>No</td>
<td>13</td>
<td>No</td>
<td>Telebit Router</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft</td>
<td>No</td>
<td>12</td>
<td>Status not clear</td>
<td>Windows</td>
<td>Yes</td>
</tr>
<tr>
<td>MIPL</td>
<td>Yes</td>
<td>15</td>
<td>Yes</td>
<td>Linux</td>
<td>Yes</td>
</tr>
<tr>
<td>Lancaster</td>
<td>Yes</td>
<td>5</td>
<td>No</td>
<td>Linux</td>
<td>No</td>
</tr>
<tr>
<td>Monarch</td>
<td>Yes</td>
<td>3</td>
<td>No</td>
<td>BSD</td>
<td>No</td>
</tr>
<tr>
<td>NEC</td>
<td>Yes</td>
<td>13</td>
<td>Yes</td>
<td>BSD</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>First version planned for 4/2002</td>
</tr>
</tbody>
</table>
Proposed Architecture for ‘Closed Systems’

What is a closed system
- One administrative domain
- Users/machines are known in advance
- Single use policy
- Dedicated software environment

Characteristics of an closed system
- Authentication of users can used predefined tokens (MAC,...)
- Firewalling keeps out the rest
- Threads from within
  - Illegitimate use
  - Playful users
- No need to be 100 per cent standards compliant
Proposed Architecture for ‘Closed Systems’

- **Home Agent**
- **Correspondent Node**
- **Mobile Node (Care of address - Autoconfiguration)**
- **IPSec Tunnel**
- **Company Headquarter**
- **Branch Office A**
- **Branch Office B**
Lab Setup and Findings

Security Gateways:
- FreeSWAN (IABG)
- Mobile IPv6:
  - MIPL
Lab Setup and Findings

Findings:

- Authentication of Binding Updates not yet possible (MIPL freezes)
- No implementations for Draft 16/17 (Reverse Routability)
- Solution for small installations
- Critical components are missing
  - PKI
  - AAA
  - Policy Server
- All hosts need to support Mobile IP!
Outlook

Things to do:
- Interworking (eg. FreeSWAN/MIPL, 6WIND Edge Device)
- Status of standardisation (New Drafts)
- Integration of MIP and IPsec Gateway on one Machine
- Thorough testing and validation of security
- Integration with AAA and PKI
- Securing Open Mobile IPv6 Installations
Thank you for your interest!

Thomas Scheffler

T-Systems Nova GmbH
Berkom
Next Generation Networks
Goslarer Ufer 35
10589 Berlin

Tel. +49 30 3497 2274
Fax +49 30 3497 2275
thomas.scheffler@t-systems.com