Security Services on IPv6 Networks: PKIv6 and IPv6-VPNs

Antonio F. Gómez Skarmeta
<skarmeta@dif.um.es>

University of Murcia
SPAIN
1 Year Subactivity Description

- Mobility on IPv6 networks
  - Going to be coordinated with 6Net
- Security on IPv6:
  - Static VPNs with IPv6 and PKIv6
  - Collaboration with 6Net via UCL test on VPNs
- Multihoming and Renumbering
- QoS over IPv6
- Mobility and VPNs using MPLS
UM-IPV6 2001:0720:1710::/48

Network Design

Internal Univ. Connection
IPv6 network design

- Native connection to Euro6IX
- IPv6 tunnel

UCL-UMU

IPv6 Services

VPNv6 testbed

IPv6 Mobility testbed

IPv6 Multicast testbed

Router IPv6

UCL

Euro6IX

UMU
The UMU-PKIv6 Service
UMU-PKIv6 Description

- Main Objective ... to establish a high security infrastructure for distributed systems

- Main Features:
  - PKI supporting the IPv6 protocol
  - Developed in Java → multiplatform
  - Issue, renew and revoke certificates for every entity (person or process) belonging to one organization
  - Either RAs or Web browsers to make their own
UMU-PKIv6 Description (II)

Main Features: (II)

- LDAPv6 directory support
- Use of smart cards (file system, RSA or Java Cards) ... allowing user mobility and increasing security
- PKI Certification Policy support
- VPN devices certification support (using the SCEP protocol)
- Support for the OCSP protocol and Time Stamp
- Web administration
- Used in both Euro6IX and 6NET projects (cross-certification)
UMU-PKIv6 Advanced Services

- TSP Message
- OCSP Message
- TimeStamping Authority
- TimeStamp Server (associated with a NTP server)
- SCEP Server (for requesting certificates from an IPsec device)
- SCEP Client
- OCSP Server (for on-line revocation support)
- OCSP Client
- IPsec device
- Certification Authority
- Certificate

Diagram showing relationships between various components and services.
UMU-PKIPv6 RA Snapshot

Requesting a certificate

Validating a certificate
UMU-PKIPv6 Final User Operation Snapshot
PKIv6

- PKIv6 running in both sites, UCL and UMU.
  - UMU:
    - IPv6-only: https://pki.ipv6.um.es
    - IPv4: https://pki.dif.um.es
  - UCL (test site, not production PKI):
    - IPv6-only: https://persephone.ip6.cs.ucl.ac.uk
    - IPv4: https://persephone.cs.ucl.ac.uk

- Interoperability tests between both of them.
  - certification, revocation and renewal request, etc.
Test suite (Current Work)

- ISABELv6,
- AGWSv6, and
- The UCL-CS Secure Conference Store

- Others (with IPv6 Support)

For a Joint Euro6IX-6NET Demo
Static VPNs with IPv6
Main objectives of this Service

- Evaluation of currently available open-source and some commercial IPv6 IPsec/IKE solutions
- Design and deployment of a static IPv6 VPN service according to the Euro6IX testbed or related-applications requirements
- Establish Joint IPv6 VPN(s) between some (interested) Euro6IX and 6NET partners
IPsec/IKE solutions being currently analyzed

- One-year activity in Euro6IX (until Dec. 2002)
- Open-Source Solutions
  - FreeS/WAN IPv6 (Linux)
  - USAGI Project (Linux)
  - KAME Project (FreeBSD)
- Commercial Solutions
  - Microsoft IPv6 (Windows XP)
  - Solaris 9
  - 6WIND
  - Others with IPv6 support
Designed evaluation plan

- Background: TAHI Project
  - http://www.tahi.org

- Interoperability tests
  - Test scenarios
  - Test suite
  - Final reports
    - Configuration and installations guides
    - Test reports
Basic IPsec scenarios

Security Association

IPv6 Router  IPv6 Router
IPv6 Host
Insecure IPv6 Network
IPv6 Host

Security Association

IPv6 Host  IPv6 Secure Gateway  IPv6 Secure Gateway  IPv6 Host
Insecure IPv6 Network

Security Association

IPv6 Router  IPv6 Router
IPv6 Host
Insecure IPv6 Network
IPv6 Host

Security Association

IPv6 Host  IPv6 Secure Gateway  IPv6 Secure Gateway  IPv6 Host
Insecure IPv6 Network
# Defined Test Scenarios

<table>
<thead>
<tr>
<th>No.</th>
<th>Category</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>Transport mode AH</td>
<td>Host</td>
</tr>
<tr>
<td>(1)</td>
<td>Transport mode ESP</td>
<td>Host</td>
</tr>
<tr>
<td>(3)</td>
<td>Transport mode AH &amp; ESP</td>
<td>Host</td>
</tr>
<tr>
<td>(4)</td>
<td>Tunnel mode AH</td>
<td>Host</td>
</tr>
<tr>
<td>(5)</td>
<td>Tunnel mode ESP</td>
<td>Host</td>
</tr>
<tr>
<td>(6)</td>
<td>Transport mode AH &amp; tunnel mode ESP</td>
<td>Host</td>
</tr>
<tr>
<td>(7)</td>
<td>Transport mode &amp; tunnel mode</td>
<td>Host</td>
</tr>
<tr>
<td>(8)</td>
<td>Tunnel mode AH</td>
<td>Host</td>
</tr>
<tr>
<td>(9)</td>
<td>Tunnel mode ESP</td>
<td>Host</td>
</tr>
<tr>
<td>(10)</td>
<td>IPSec Tunnel mode with HOST</td>
<td>Router</td>
</tr>
<tr>
<td>(11)</td>
<td>IPSec Tunnel to IPSec Tunnel mode</td>
<td>Router</td>
</tr>
<tr>
<td>(12)</td>
<td>IPSec Tunnel to IPSec Tunnel mode with HOST</td>
<td>Router</td>
</tr>
<tr>
<td>(13)</td>
<td>AH Transport to ESP Tunnel mode</td>
<td>Router</td>
</tr>
</tbody>
</table>

AH: Authentication Header

ESP: Encapsulating Security Payload
Example of test scenario: Transport mode AH (Host)
AH Transport to ESP Tunnel mode:
two secure gateways get a SA using tunnel mode ESP and after get a new SA using transport mode AH.
Defined Test Suite

- Basic applications
  - Ping6 (ICMPv6)
  - Telnet6 (TCP)
  - Host6 (UDP)
- Another IPv6 applications within the project
VPNv6

- Scenario UCL-UMU:
  - Tunnel ESP
  - IKE with certificates of PKIv6

- Implementation: KAME integrated in FreeBSD 4.5 release.

- CISCO 2600 actually just IPv4 waiting for releases
VPNv6 - Scenario UCL-UMU

UCL
- IPv6 Router
- PC router
  - snickers.cs.ucl.ac.uk

Tunnel ESP
- IPv6 Network

UMU
- PC router Secure Gateway
  - rohan.ipv6.um.es

IPv6 Host
  - gimly.ipv6.um.es
  - gloin.ipv6.um.es
Next/Current work

- Evaluation of the IPsec/IKE solutions
  - Running interoperability tests
  - Test Reports
- Design of a Dynamic VPN Service (based on the concept of Security Policy defined by the IETF/DMTF)
- Attribute certificate support for VPN and authorization procedures
- Definition of AAA scenarios to relate mobility testbed and PKIv6
Security Policies for VPMPs (I)

Policy Definition Process Schema

- **Administrator**
- **Policy Repository**
- **LDAP**
- **Policy Management Tool** (Parser XML/LDAP)
- **CIM-XML**
- **CIM Client**
- **CIM Object Manager**
Security Policies for VPNs (II)

Policy Recovery Process Schema

- LDAP
- PDP
- COPS (PIB)
- SPD/SAD
- PEP

Scene 1
- Non-COPS IPSec Node
- retrieve from SPD/SAD

Scene 2
- Non-COPS IPSec Node (Agent SNMP)
- retrieve from COPS (MIB)

Scene 3
- COPS IPSec Node
- application of policy from PEP
- PDP retrieve from LDAP

Policy Repository
AAAa6

- To define a chain of AAA servers managed by AAA protocol (DIAMETER) over IPv6 between both Universities
- To use established VPNs to secure communications between AAA servers
- Future MIPv6 and AAA tests
Planned AAAv6 testbed
Security Services on IPv6 Networks: PKIv6 and IPv6-VPNs

Antonio F. Gómez Skarmeta
<skarmeta@dif.um.es>

University of Murcia
SPAIN