IPv6 Security

IPv6 Security Seminar,
23 March, 2005

Ray Hunt, Associate Professor
Dept. of Computer Science and Software Engineering
University of Canterbury
New Zealand

Contents

- IPv6 security features
- IPSec AH/ESP Tunnel/Transport security services
- IPv6 Threats
- IPv6 Unauthorised Access
- IPv6 Routing Extension Header
- IPv6 Tunneling
- IPv6 Flow Label Vulnerability
- IPv6 Multicast Vulnerability
- IPv6 Neighbour Discovery Vulnerability
- Security consideration for an IPv6 firewall
- Mobile IPv6 security

IPv6 Security Features

- Many similar security problems existing in IPv6 as IPv4 viz:
  - Spoof IP address
  - Modify packet contents
  - Replay
  - Sniff packet in transit

IPSec (AH & ESP)

- IPSec provides security services for IPv6
  - Access Control
  - Connectionless Integrity
  - Data origin authentication
  - Anti-replay
  - Confidentiality (via encryption)
  - Traffic flow confidentiality

IPSec AH and ESP Security Services

<table>
<thead>
<tr>
<th>Security Service</th>
<th>AH</th>
<th>ESP (Encryption)</th>
<th>ESP (Encryption + Authentication)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Connectionless integrity</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data origin authentication</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Anti-replay</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Traffic flow confidentiality</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

IP Security (IPSec) Roadmap (RFC 2411)

Specific algorithms defined as required
IP Security (IPSec) RFCs

- RFC 2401 — Security Architecture for the Internet Protocol
- RFC 2402 — IP Authentication Header
- RFC 2406 — IP Encapsulating Security Payload
- RFC 2409 — The Internet Key Exchange (IKE)
- RFC 1828 — IP Authentication using Keyed MD5
- RFC 1829 — The ESP DES-CBC Transform

IP Authentication Header (AH)

- Supports data origin authentication and data integrity on a per-packet basis
- Optional replay protection
- Protects the integrity of the ENTIRE Packet
  - Header (except for mutable fields - e.g., IPv4/IPv6 TTL, TOS, checksum)
  - Payload (still cleartext, not encrypted)

IPSec Encapsulating Security Payload (ESP)

- Provides data origin authentication, integrity protection, confidentiality (encryption) and optional replay protection on per-packet basis
- Protects either payload (transport) or original header+payload (tunnel)

IPSec Transport and Tunnel Mode

- IPsec - AH Tunnel (R/FW-R/FW)
- IPsec - ESP Transport (client-server)

IPv6 IPSec Transport Mode

1. After applying AH
   - IPv6 Header
2. After applying ESP
   - IPv6 Header
3. After applying ESP-AH
   - IPv6 Header

IPv6 IPSec Tunnel Mode

1. After applying AH
   - IPv6 Header
2. After applying ESP
   - IPv6 Header
3. After applying ESP-AH
   - IPv6 Header

Ext Header* — Destination Options for the final destination can be positioned after AH or ESP.
IPSec Security Association (SA)

- SAs are fundamental to IPSec operation
- Set of parameters - protocol, tunnel/transport mode, crypto algorithm, key life-time etc define the security association between two entities
- SA = (SPI, DA, AH/ESP)
- SPI - Security Parameter Index
- Unfortunately in mobile IP networks DA can change and this can cause firewalls to break connections
- Full implementation of IPv6 (routers, firewalls..) can rectify this
- Reference: RFC2409 The Internet Key Exchange (IKE)

IPv6 Threats - Summary

- IPv6 Unauthorised Access
- IPv6 Routing Extension Header
- IPv6 Tunneling
- IPv6 Flow Label Vulnerability
- IPv6 Multicast Vulnerability
- IPv6 Neighbour Discovery Vulnerability

IPv6 Threats

- IPv6 Unauthorised Access
  - IPv6 Access control mechanism similar to IPv4 except:
    - IPv6 Address - IPv6 interface can have more than one IPv6 address, eg link-local address (FE80::/10), site-local addresses, global unicast and anycast addresses
    - IPv6 firewall needs to be carefully configured to control access for these three types of IPv6 addresses
    - IPv6 multicast addresses have defined scope, eg link-local multicast must not be forwarded
    - IPv6 firewall must define site-local address boundary
    - IPv6 firewalls need to drop packets with a multicast source address

IPv6 Threats

- IPv6 Unauthorised Access
  - ICMPv6
    - All types of ICMPv4 packets can be blocked at firewall as IPv4 uses different mechanisms for:
      - Layer 2/3 address resolution - ARP in IPv4, Route discovery in IPv6
      - IPv6 multicast receivers use Multicast Listener Discovery (MLD) with ICMPv6 in an IPv6 packet
      - IPv4 uses Internet Group Management Protocol (IGMP, which is identical to MLD) with IGMP in an IPv4 packet

IPv6 Threats

- IPv6 Unauthorised Access
  - Even though ICMPv6 messages depend on security policy, the following are important for correct IPv6 operation:
    - ICMPv6 Type 2 (Packet Too Big):
    - ICMPv6 Type 133, 134 (Router Solicitation and Router Advertisement)
    - ICMPv6 Type 135, 136 (Neighbour Solicitation and Neighbour Advertisement)
    - ICMPv6 Type 130-132, 143 (Multicast Listener Query/Report/Done/Version 2 Report)
IPv6 Threats

- IPv6 Routing Extension Header
  - Although IPv6 routing extension header resembles IPv4 source routing...
  - An IPv4 firewall cannot process an IPv6 routing extension header as it looks at destination address only
  - In diagram web server may then pass packets on to victim
  - In IPv4 source routing, IP address in options field while in IPv6 they are part of the header
  - Thus IPv6 firewalls need specific rules to handle this


IPv6 Threats

- IPv6 Routing Extension Header
  - Type 2 routing header used specifically for mobile IPv6 networks
  - IPv6 nodes that process Type 2 Routing header must verify that address contained in Type 2 Routing header is node’s home address in order to prevent packets from being forwarded outside the node
  - IPv6 specifies that upper-layer protocol should not respond with a packet, which has a Routing header that is automatically derived by reversing the received Routing header; unless integrity/authenticity of source address and Routing header have been verified (e.g., via an Authentication header in received packet)

IPv6 Threats - IPv6 Tunneling

- During IPv6 transition period, many sites will use IPv6 tunnels over IPv4 infrastructure (static or automatic). Generic concerns about tunneling:
  - May be easier to avoid ingress filtering checks
  - Possible to send packets having link-local addresses and Hop Limit = 255, which can be used to attack subnet hosts from remote node
  - Automatic tunneling mechanisms are typically dangerous as other end-point is unspecified
IPv6 Threats - IPv6 Tunneling

- This attack (diagram) can be used to accomplish a DoS on destination host.
- If destination host generates replies (TCP SYN ACK, TCP RST, ICMPv6 Echo Reply, ICMPv6 Destination Unreachable, etc.) to spoofed source, the victim host is used as a reflector for attacking another victim (the spoofed source).
- Distributed Reflection DoS can be performed if large number of nodes are involved in sending spoofed traffic with same IPv6 source address.


IPv6 Threats

- IPv6 Flow Label Vulnerability
  - IPv6 Flow Label header has security issues such as denial-of-service and theft-of-service by unauthorised traffic.
  - Flows are identified by 3-tuple of (Flow Label, SA, DA) in IPv6 header. Risk of theft or DoS introduced by Flow Label is closely related to risk of theft or DoS by address spoofing.
  - Adversary who can forge an address is also likely to be able to forge a label.
  - Theft of service can become DoS, eg altering flow labels on intermediate routers.


IPv6 Threats

- IPv6 Multicast Vulnerability
  - A multicast group address has prefix format of FF00::/8. A single host can send data to logically 2**120 multicast groups. The multicast network would be responsible for maintaining this state. To handle this, multicast network needs to limit number of multicast source and group states.
  - To protect against this receiver-based attack, all routers should limit the packet rate of MLD (Multicast Listener Discovery) messages.

IPv6 Threats

- IPv6 Neighbour Discovery Vulnerability
  - Malicious node can generate various attacks using vulnerabilities in Neighbour Discovery, Router Discovery and Address Autoconfiguration.
  - Many of the attacks involve preventing communication between victim node and all other nodes or a router.
  - Redirecting other hosts’ traffic to a victim node and creating a flood at the victim node.

Security Consideration for an IPv6 Firewall

- Firewall architectures currently applied in IPv4 are generally applicable to IPv6.
- Packet examining in IPv6 firewalls is similar to that used for IPv4 networks.
- IPv6 header format has changed but is still similar to IPv4 header.
- However, IPv6 introduces new operations viz:
  - Address Autoconfiguration and Path MTU Discovery.
  - Support for new features such as IPSec, mobility, multicast, Quality-of-Service.

IPv6 firewall must consider following security issues:

- Address filtering
- IPv4 attacks
- ICMPv6 filtering
- Extension header
- ICMPv6 error message for packet drop
- QoS support
- Multicast support
- Mobile IPv6 support
- IPSec support

Mobile IPv6 Security

- Key components of mobile IPv6:
  - Mobile Node (MN)
  - Home Agent (HA)
  - Correspondent Node (CN)
  - Home address (HoA)
  - Care-of-address (CoA)
  - Home link
  - Foreign link

Mobile IPv6 Security - communication scenarios

1. Home Registration
2. Communication through a tunnel
3. Correspondent Registration
4. Direct Communication

1. Home Agent
2. Correspondent Node
3. Mobile Node

Mobile IPv6 Security - home address option and firewall
Mobile IPv6 Security

- Security issues with IPv6 Routing Headers
  - Type 2 Routing header is introduced in order to distinguish between IPv6 source routing and Mobile IPv6
  - IPv6 Routing extension header potentially has security problems, and firewalls would restrict packets with a Routing extension header
  - Type 2 Routing header is safer because mobile node verifies that address is same as its home address in order to prevent packets from being forwarded outside of node

Mobile IPv6 Security - attacking correspondent node

- Mobile IPv6 uses binding to redirect traffic from one address (home address) to another (care-of address)
- Binding between mobile node and its home agent, or between mobile node and correspondent node, is used to modify handling of incoming or outgoing packets
- This leads to security risks such as man-in-the-middle attacks, hijacking, eavesdropping, impersonation, and DoS attacks.
- See following slide …..


Mobile IPv6 Security - home registration

- Correspondent Node
  - IPv6 Header
    - Source Address: CoA
    - Destination Address: HA
  - Destination Options Header
  - Home Address Option: HoA
  - ESP Header (Transport Mode)
  - Mobility Header
  - Binding Update Message (with Alternate Care-of Address CoA)

- Mobile Node
  - IPv6 Header
    - Source Address: HA
    - Destination Address: CoA
  - Type 2 Routing Header
    - Home Address: HoA
  - ESP Header (Transport Mode)
  - Mobility Header
  - Binding Acknowledgement

HaA – 2000::1
CoA – 2345::1
Summary

- IPv6 addresses and solves many of the security issues associated with IPv4
- Vulnerabilities exist in use of IPv6 as some mechanisms differ from IPv4 (e.g. use of ICMPv6)
- Mixed (v4 and v6) networks are problematic (e.g. automatically tunneling)
- Careful IPv6 firewall design is essential