IPv6 Security

Malta 6DISS workshop

4-6 april 2006

Jerome.Durand@renater.fr

Copy ...Rights

- *This slide set is the ownership of the 6DISS project via its partners*
- *The Powerpoint version of this material may be reused and modified only with written authorization*
- *Using part of this material must mention 6DISS courtesy*
- *PDF files are available from www.6diss.org*

Contributions

- Main authors
  - János Mohácsi, NIIF/HUNGARNET - Hungary
  - Laurent Toutain, ENST-Bretagne – IRISA, France
- Contributors
  - Bernard Tuy, Renater, France
  - Jérôme Durand, Renater, France

Threats

Scanning and addresses

Scanning in IPv6

- Subnet Size is much larger
  - Default subnets in IPv6 have 2^64 addresses (approx. 18x10^18). Exhaustive scan on every address on a subnet is no longer reasonable (if 1 000 000 address per second then > 500 000 year to scan)
  - NMAP doesn't even support for IPv6 network scanning (for now...)

Scanning in IPv6 /2

- IPv6 Scanning methods are likely to change
  - Public servers will still need to be DNS reachable giving attacker some hosts to attack – this is not new!
  - Administrators may adopt easy to remember addresses (::1,::2,::53, or simply IPv4 last octet)
  - EUI-64 has “fixed part”
  - Ethernet card vendors guess
  - New techniques to harvest addresses – e.g. from DNS zones, logs
    - Deny DNS zone transfer
  - By compromising routers at key transit points in a network, an attacker can learn new addresses to scan

Scanning in IPv6 / 3

- New attack vectors “All node/router …. addresses”
- New Multicast Addresses - IPv6 supports new multicast addresses that can enable an attacker to identify key resources on a network and attack them
- For example, all nodes (FF02::1), all routers (FF05::2) and all DHCP servers (FF05::5)
- These addresses must be filtered at the border in order to make them unreachable from the outside – this is the default if no IPv6 multicasting enabled.

Security of IPv6 addresses

- Privacy enhanced addresses as defined RFC 3041
  - prevents device/user tracking from
  - makes accountability harder
- New privacy extended IPv6 addresses generated CGA (crytographically generated addresses)
  - maintains privacy
  - accountability possible by link administrators

Threats

Unauthorized Access

Unauthorized Access control in IPv6

- Policy implementation in IPv6 with Layer 3 and Layer 4 is still done in firewalls
- Some design considerations! – see next slides also
  - Filter site-scoped multicast addresses at site boundaries
  - Filter IPv4 mapped IPv6 addresses on the wire
  - Multiple addresses per interfaces

Action	Src	Dst	Src port	Dst port
permit	a:b:c:d::e	x:y:z:w::v	any	ssh
deny	any	any		

Unauthorized Access control in IPv6

- non-routable + bogon address filtering slightly different
  - in IPv4 easier deny non-routable + bogon
  - in IPv6 easier to permit legitimate (almost)

Action	Src	Dst	Src port	Dst port
deny	2001:db8::/32	host/net		
permit	2001::/16	host/net	any	service
permit	2002::/16	host/net	any	service
permit	2003::/16	host/net	any	service
permit	3ffe::/16	host/net	any	service
deny	any	any		

IANA allocations in March 2006

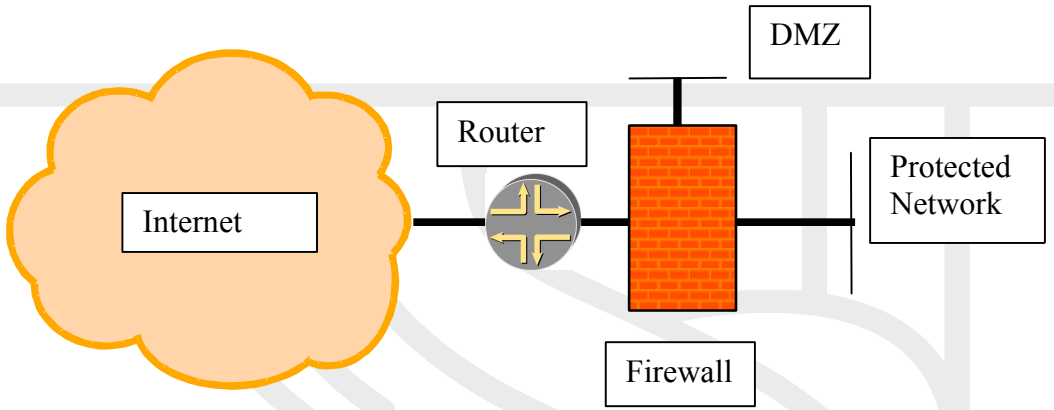
- http://www.iana.org/assignments/ipv6-unicast-address-assignments

2001:0000::/23 IANA 01 Jul 99 [1] [7]
2001:0200::/23 APNIC 01 Jul 99
2001:0400::/23 ARIN 01 Jul 99
2001:0600::/23 RIPE NCC 01 Jul 99
2001:0800::/23 RIPE NCC 01 May 02
2001:0A00::/23 RIPE NCC 02 Nov 02
2001:0C00::/23 APNIC 01 May 02 [2]
2001:0E00::/23 APNIC 01 Jan 03
2001:1200::/23 LACNIC 01 Nov 02
2001:1400::/23 RIPE NCC 01 Feb 03
2001:1600::/23 RIPE NCC 01 Jul 03
2001:1800::/23 ARIN 01 Apr 03
2001:1A00::/23 RIPE NCC 01 Jan 04
2001:1C00::/22 RIPE NCC 01 May 04
2001:2000::/20 RIPE NCC 01 May 04
2001:3000::/21 RIPE NCC 01 May 04
2001:3800::/22 RIPE NCC 01 May 04 2001:3C00::/22 RESERVED 11 Jun 04
[3] 2001:4000::/23 RIPE NCC 11 Jun 04
2001:4200::/23 AfriNIC 01 Jun 04
2001:4400::/23 APNIC 11 Jun 04
2001:4600::/23 RIPE NCC 17 Aug 04
2001:4800::/23 ARIN 24 Aug 04
2001:4A00::/23 RIPE NCC 15 Oct 04
2001:4C00::/23 RIPE NCC 17 Dec 04
2001:5000::/20 RIPE NCC 10 Sep 04
2001:8000::/19 APNIC 30 Nov 04
2001:A000::/20 APNIC 30 Nov 04
2001:B000::/20 APNIC 08 Mar 06
2002:0000::/16 6to4 01 Feb 01 [4]
2003:0000::/18 RIPE NCC 12 Jan 05
2400:0000::/19 APNIC 20 May 05
2400:2000::/19 APNIC 08 Jul 05
2400:4000::/21 APNIC 08 Aug 05 2404:0000::/23 APNIC 19 Jan 06
2600:0000::/22 ARIN 19 Apr 05
2604:0000::/22 ARIN 19 Apr 05
2608:0000::/22 ARIN 19 Apr 05
260C:0000::/22 ARIN 19 Apr 05
2610:0000::/23 ARIN 17 Nov 05
2800:0000::/23 LACNIC 17 Nov 05
2A00:0000::/21 RIPE NCC 19 Apr 05
2A01:0000::/16 RIPE NCC 15 Dec 05 [6]
3FFE:0000::/16 6BONE 01 Dec 98 [5]

IPv6 Firewalls

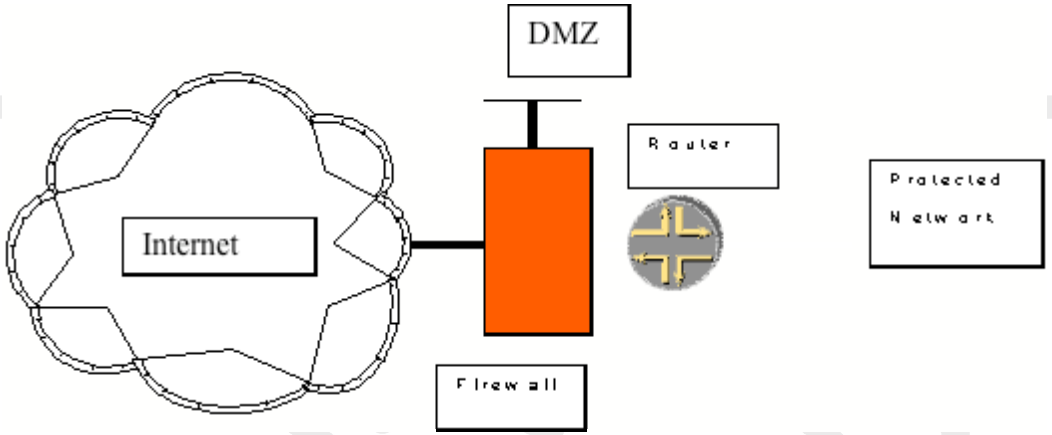
- IPv6 architecture and firewall - requirements
  - No need to NAT – same level of security with IPv6 possible as with IPv4 (security and privacy) – even better: e2e security with IPSec
  - Weaknesses of the packet filtering cannot be made hidden by NAT
  - Support for IPv6 header chaining
  - Support for IPv4/IPv6 transition and coexistence
  - Not breaking IPv4 security

IPv6 firewall setup - method1



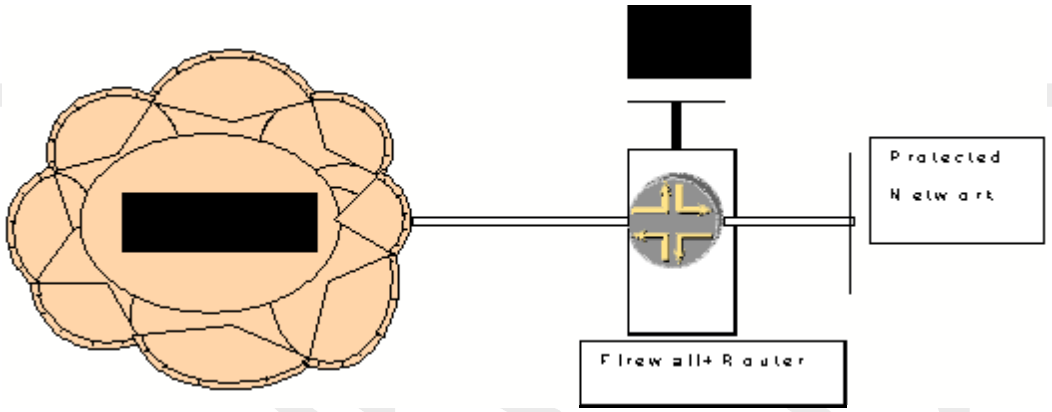
- Internet ↔router↔firewall↔net architecture
- Requirements:
  - Firewall must support/recognise ND/NA filtering
  - Firewall must support RS/RA if SLAAC is used
  - Firewall must support MLD messages if multicast is required

IPv6 firewall setup - method2



- Internet ↔ firewall ↔ router ↔ net architecture
- Requirements:
  - Firewall must support ND/NA
  - Firewall should support filtering dynamic routing protocol
  - Firewall should have large variety of interface types

IPv6 firewall setup - method3



- Internet ↔ firewall/router(edge device) ↔ net architecture
- Requirements
  - Can be powerful - one point for routing and security policy
    - very common in SOHO (DSL/cable) routers
  - Must support what usually router AND firewall do

Problems with ICMPv6

- **draft-ietf-v6ops-icmpv6-filtering-bcp-xx**
- ICMPv6 is a fundamental component of IPv6 networks
  - Some parts of ICMPv6 have an essential role in establishing communications
  - Less of an 'auxiliary' than ICMP in IPv4
- Some ICMPv6 messages can be a threat to open networks
- Firewall filtering important for maintaining security
- Need to balance effective IPv6 communications against security needs

Major ICMPv6 Functions

- Error messages (4 types)
- Echo Request and Response
- Neighbor finding (NS, NA, RS, RA)
  - Duplicate Address Detection
  - IP and Link Layer Address exchange
  - Router Identification
  - Stateless Address Auto-configuration
- Network renumbering (NS, NA + renumber)
- Path MTU determination (Packet Too Big)
- Multicast Listener Discovery (4 messages)
- Mobile IPv6 support (4 messages)
- Node information lookup (2 messages)

Possible Firewall setup

- No blind ICMPv6 filtering possible:

[IPv6 specific]	Echo request/reply	Debug
	No route to destination	Debug – better error indication
	TTL exceeded	Error report
	Parameter problem	Error report
	NS/NA	Required for normal operation – except static ND entry
	RS/RA	For Stateless Address Autoconfigration
	Packet too big	Path MTU discovery
	MLD	Requirements in for multicast in architecture 1

[required]

Firewall setup 2

- No blind IP options (→ extension Header) filtering possible:

Hop-by-hop header	What to do with jumbograms or router alert option? – probably log and discard – what about multicast report messages?
Routing header	Source routing – in IPv4 it is considered harmful, but required for IPv6 mobility – log and discard if you don't support MIPv6, otherwise enable only Type 2 routing header for Home Agent of MIPv6
ESP header	Process according to the security policy
AH header	Process according to the security policy
Fragment header	All but last fragments should be bigger than 1280 octets

Overview of IPv6 firewalls

	IP Filter 4.1	PF 3.6	IP6 fw	Iptables	Cisco ACL	Cisco PIX 7.0	Juniper firewall	Juniper NetScreen	Windows XP SP2
Portability	Excellent	Good	Average	Weak	Weak	Weak	Weak	Weak	Weak
ICMPv6 support	Good	Good	Good	Good	Good	Good	Good	Good	Good
Neighbor Dissovery	Excellent	Excellent	Good	Excellent	Excellent	Excellent	Good	Excellent	Weak
RS/RA support	Excellent	Excellent	Good	Excellent	Excellent	Excellent	Excellent	Excellent	Good
Extension header support	Good	Good	Good	Excellent	Good	Good	Good	Good	Weak
Fragmantation support	Weak	Complete block	Weak	Good	Weak	Average	Weak	Average	Weak
Stateful firewall	Yes	Yes	No	Csak USAGI	Reflexive firewall since 12.3 (11)T	Yes	ASP necessary	Yes	No
FTP proxy	No	Next version	No	No	No	Yes	No	No	No
Other	QOS support	QoS support, checking packet vailidity	Predefined rules in *BSD	EUI64 check,	Time based ACL	Time based ACL	TCP flag support only in upcoming 7.2, HW based	IPSec VPN, routing support	Graphical and central configuration

Threats

Spoofing

Spoofing in IPv6

- IPv6 address are globally aggregated making spoof mitigation at aggregation points easy to deploy
  - uRPF for IPv6 between ISP's and customers
  - Not always implemented

- However host part of the address is not protected
  - You need IPv6 <– >MAC address (user) mapping for accountability

Threats

Autoconfiguration problems

Autoconfiguration/Neighbor Discovery

- SLAAC
  - Neigbor Discovery ~ security
    - Some L2 switches now can make sure ND/NA/RA/RS come from the correct interface
  - SEND for the future
    - RFC3972 available! not really there...
- DHCPv6 with authentication is possible

Threats

Broadcast amplification

Amplification (DDoS) Attacks

- There are no broadcast addresses in IPv6
  - Good thing!
  - But multicast addresses everywhere !
    - e.g. link-local addresses, site-local addresses, all site-local routers, etc.
- Make sure you control what comes into these groups!
  - Would you like someone to be able to send packets at all DHCPv6 servers at a one time and potentially attack them all together?
  - Make sure source addresses are unicast addresses ☺

Other threats...

Just to keep in mind...

Other threats

- IPv6 Routing Attack
  - Use traditional authentication mechanisms for BGP and IS-IS.
  - Use IPsec to secure protocols such as OSPFv3 and RIPng
- Viruses and Worms
- Sniffing
  - Without IPsec, IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4
- Application Layer Attacks
  - Even with IPsec, the majority of vulnerabilities on the Internet today are at the application layer, something that IPsec will do nothing to prevent
- Man-in-the-Middle Attacks (MITM)
  - Without IPsec, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4
- Flooding
  - Flooding attacks are identical between IPv4 and IPv6

New threats

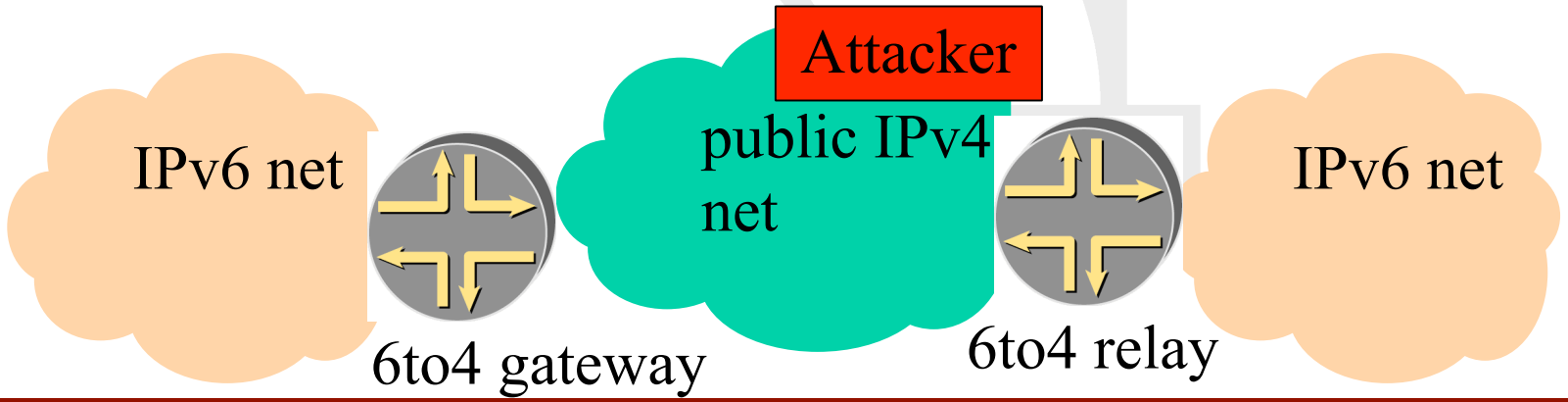
Transition Mechanisms

IPv6 transition mechanisms

- ~15 methods possible in combination
- Dual stack:
  - enable the same security for both protocol
- Tunnels:
  - ip tunnel – punching the firewall (protocol 41)
  - gre tunnel – probable more acceptable since used several times before IPv6
- Remember that your tunnel interface is a new potential hole in your security infrastructure

Spoofing in IPv4 with 6to4

- For example, via 6to4 tunneling spoofed traffic can be injected from IPv4 into IPv6.
  - IPv4 Src: Spoofed IPv4 Address
  - IPv4 Dst: 6to4 Relay Anycast (192.88.99.1)
  - IPv6 Src: 2002:: Spoofed Source
  - IPv6 Dst: Valid Destination



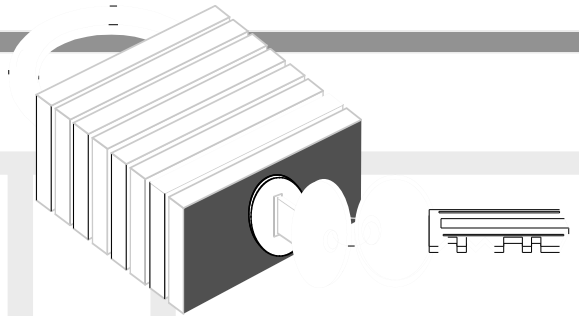
Mixed IPv4/IPv6 environments

- There are security issues with the transition mechanisms
  - Tunnels are extensively used to interconnect networks over areas supporting the “wrong” version of protocol
  - Tunnel traffic many times has not been anticipated by the security policies. It may pass through firewall systems due to their inability check two protocols in the same time
- Do not operate completely automated tunnels
  - Avoid “translation” mechanisms between IPv4 and IPv6, use dual stack instead
  - Only authorized systems should be allowed as tunnel end-points
  - Automatic tunnels can be secured by IPSec

IPv6 Security infrastructure

IPSec

IPSec



- general IP Security mechanisms
- provides
  - authentication
  - confidentiality
  - key management - requires a PKI infrastructure (IKE)
    - new simplified and unified IKEv2 will be available soon.
- applicable to use over LANs, across public & private WANs, & for the Internet
- Easier to deploy with IPv6 as no NAT in the middle!
- IPSec is mandated in IPv6 – you can rely on for e2e security

Summary

- IPv6 has potential to be a foundation of a more secure Internet
- Elements of the IPv6 security infrastructure (Firewalls, IPSec, AAA etc.) are mature enough to be deployed in production environment.

References

- 6NET D3.5.1: Secure IPv6 Operation: Lessons learned from 6NET
- J. Mohacsi, “IPv6 firewalls”, presentation on the 5th TF-NGN meeting, October 2001 available at http:///skye.ki.iif.hu/~mohacsi/athens_tf_ngn_ipv6_firewalls.pdf
- J.Mohacsi, “Security of IPv6 from firewalls point of view”, presentation on TNC2004 conference, June 2004, available at http://www.terena.nl/conferences/tnc2004/programme/presentations/show.php?pres_id=115
- 6NET D6.2.2: Operational procedures for secured management with transition mechanisms
- S. Convery, D Miller, IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0)", presentation at the 17th NANOG, May 24, 2004
- J. Mohácsi, E. Davis: draft-v6ops-ietf-icmpv6-filtering-bcp-00.txt

Thank you!

- Acknowledgement from Patrick Grossetete, Stig Veenas, Ladislav Lhotka, Jerome Durand, Tim Chown, Gunter van de Velde and Eric Marin.
- Questions: mohacsi@niif.hu