

IPv6 Security: Threats and solutions

János Mohácsi
NIIF/HUNGARNET

Outline of the presentation

- Threats against IPv6– comparing with IPv4
 - Scanning
 - Unauthorised access – IPv6 firewalls review
 - Fragmentation attacks
 - Spoofing
 - Host initialisation attacks
 - Broadcast amplification attacks
 - Other types of attacks
- Specific IPv6 related problems
- IPv6 Security infrastructure

Threats

Scanning and addresses

Scanning in IPv6

- Subnet Size is much larger
 - Default subnets in IPv6 have 2^{64} addresses (approx. 18×10^{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

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 address 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
- Other possible network hiding: DNS splitting

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

- Private addresses as defined RFC 3041
 - prevents device/user tracking from
 - makes accountability harder
- New privacy extended IPv6 addresses generated CGA (cryptographically generated addresses)
 - maintains privacy
 - accountability possible by link administrators
- New feature: Host ID could be a token to access to a network. – additional security possible

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 address 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

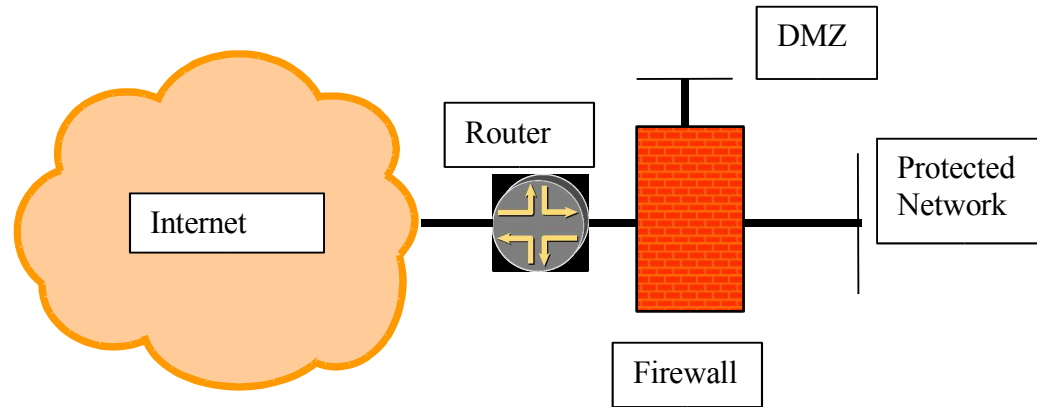
- non-routable + bogon address filtering slightly different
 - in IPv4 easier deny non-routable + bogon
 - in IPv6 easier to permit legitimate (almost)

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		

IPv6 Firewalls

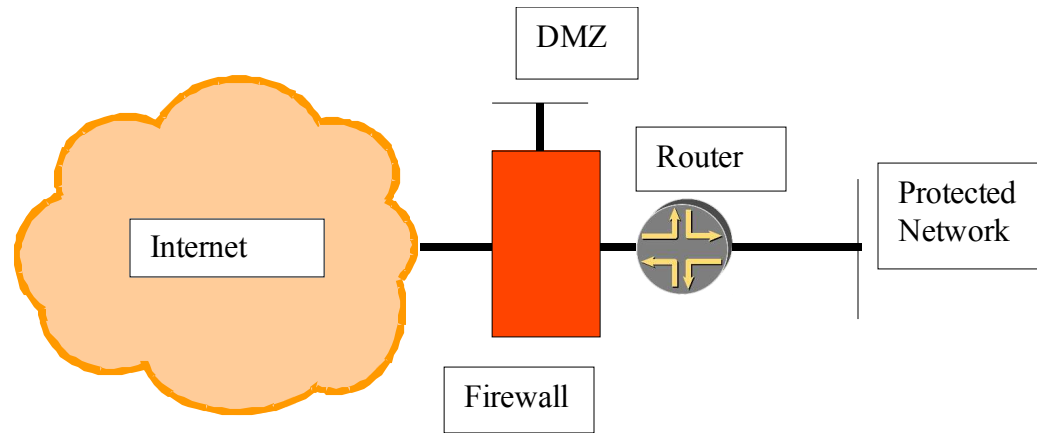
- IPv6 architecture and firewall - requirements
 - No need to NAT – same level of security with IPv6 possible as with IPv4 (security and privacy) – even better: e2e security with IPSec
 - Weaknesses of the packet filtering cannot be made hidden by NAT
 - “IPv6 does not require end-to-end connectivity,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

IPv6 firewall setup - method 1



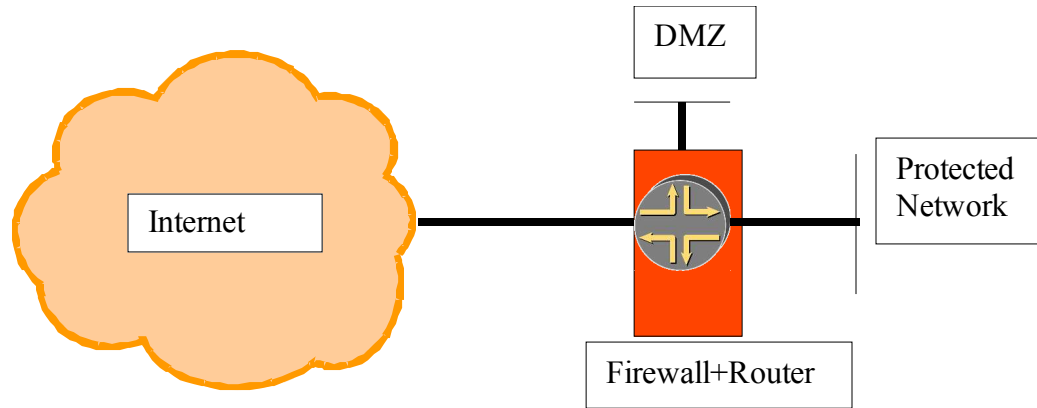
- Internet router firewall net architecture
- Requirements:
 - Firewall must support/recognise ND/NA filtering
 - Firewall must support RS/RA if SLAAC is used
 - Firewall must support MLD messages if multicast is required

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

Firewall setup

- No blind ICMPv6 filtering possible:

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

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 join 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

Interoperability of filtered applications

- FTP:
 - Very complex: PORT, LPRT, EPRT, PSV, EPSV, LPSV (RFC 1639, RFC 2428)
 - virtually no support in IPv6 firewalls
 - HTTP seems to be the next generation file transfer protocol with WEBDAV and DELTA
- Other non trivially proxy-able protocol:
 - no support (e.g.: H.323)

Overview of IPv6 firewalls

	IPFilter 4.1	PF 3.6	IP6fw	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 Discovery	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
Fragmentation support	Weak	Complete block	Weak	Good	Weak	Average	Weak	Average	Weak
Stateful firewall	Yes	Yes	No	Csak USAGI	Reflexive firewall	Yes	ASP necessary	Yes	No
FTP proxy	No	Next version	No	No	since 12.3 (11)T	Yes	No	No	No
Other	QoS support	QoS support, checking packet validity	Predefined rules in *BSD	EUI64 check,	Time based ACL		No TCP flag support today, HW based	IPSec VPN, routing support	Graphical and central configuration

Threats

Fragmentation and header handling

Header Manipulation and Fragmentation Best Practices

- Deny IPv6 fragments destined to an internetworking device - Used as a DOS vector to attack the infrastructure
- Ensure adequate IPv6 fragmentation filtering capabilities. For example, drop all packets with the routing header if you don't have MIPv6
- Potentially drop all fragments with less than 1280 octets (except the last fragment)
- All fragment should be delivered in 60 seconds otherwise drop

Threats

L3-L4 spoofing

L3- L4 Spoofing in IPv6

- While L4 spoofing remains the same, IPv6 address are globally aggregated making spoof mitigation at aggregation points easy to deploy
- Can be done easier since IPv6 address is hierarchical
- However host part of the address is not protected
 - You need IPv6 \leftrightarrow MAC address (user) mapping for accountability!

Threats

IPv4 ARP and DHCP attacks -
Subverting host initialization

Autoconfiguration/Neighbor Discovery

- Neighbor Discovery ~ security ~ Address Resolution Protocol
 - No attack tools – arp cache poisoning
 - No prevention tools – dhcp snooping
- Better solution with SEND
 - based on CGA: $\text{token1} = \text{hash}(\text{modifier}, \text{prefix}, \text{publickey}, \text{collision-count})$
 - RFC3972 available!
- DHCPv6 with authentication is possible
- ND with IPSec also possible

Threats

Broadcast amplification

Amplification (DDoS) Attacks

- There are no broadcast addresses in IPv6
 - This would stop any type of amplification/"Smurf" attacks that send ICMP packets to the broadcast address
 - Global multicast addresses for special groups of devices, e.g. link-local addresses, site-local addresses, all site-local routers, etc.
- IPv6 specifications forbid the generation of ICMPv6 packets in response to messages to global multicast addresses (exception Packet too big message – it is questionable practice).
 - Many popular operating systems follow the specification
 - Still uncertain on the danger of ICMP packets with global multicast source addresses

Mitigation of IPv6 amplification

- Be sure that your host implementation follow the RFC 2463
- Implement RFC 2827 ingress filtering
- Implement ingress filtering of IPv6 packets with IPv6 multicast source address

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

Specific IPv6 related problems

Specific IPv6 related threats

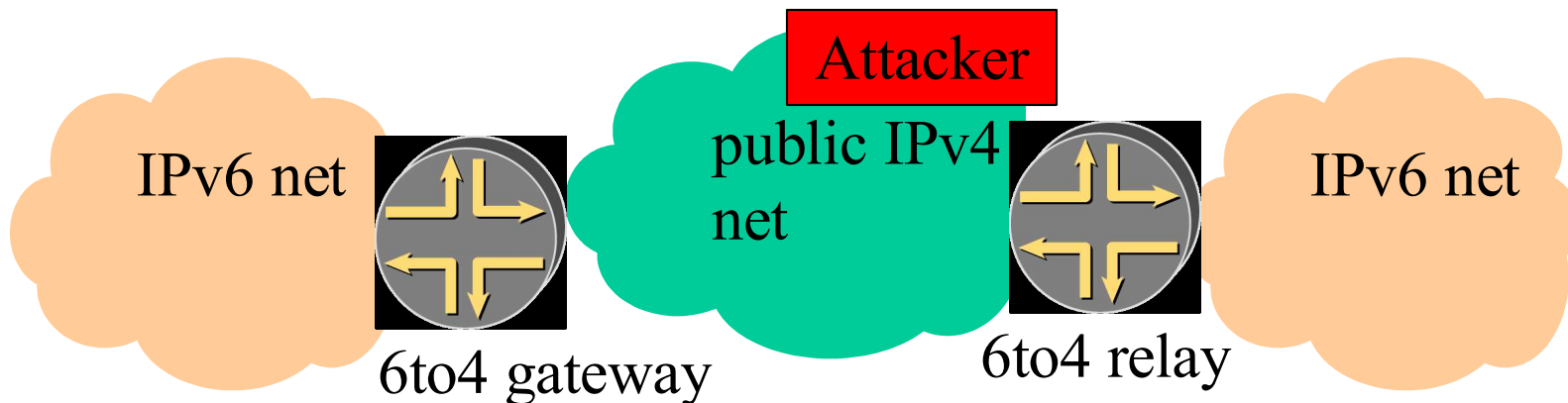
Transition Mechanisms

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

L3 – L4 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 endpoints
 - Automatic tunnels can be secured by IPsec

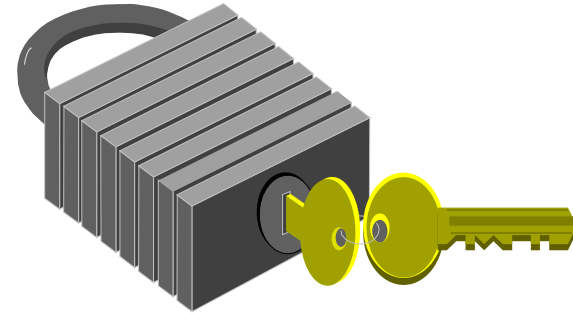
IPv6 security infrastructure

- IPsec
- Firewalls
- AAA
 - Radius only -> Diameter?
 - TACACS+ - no plan

IPv6 Security infrastructure

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
- IPSec is not a single protocol. Instead, IPSec provides a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms provide security appropriate for the communication.
- IPSec is mandated in IPv6 – you can rely on for e2e security



IPv6 Security infrastructure

Firewalls

See earlier and the references

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

Thank you!

- Acknowledgement to Patrick Grossetete, Stig Veenas, Ladislav Lhotka, Jerome Durand, Tim Chown, Gunter van de Velde and Eric Marin for their comments.
- Further informations:
 - <http://www.6net.org> And <http://6net.niif.hu>
- Questions: mohacsi@niif.hu