IPv6 Security

2nd South East Europe 6DISS Workshop
Plovdiv, Bulgaria
27-29 June 2007

Athanassios Liakopoulos
(aliako@grnet.gr)

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*
- *Looking for a contact ?*
  - *Mail to : martin.potts@martel-consulting.ch*
  - *Or bernard.tuy@renater.fr*

Acknowledgements

- János Mohácsi, NIIF/HUNGARNET - Hungary
- Octavio Medina, Octavio Medina, Laurent Toutain, ENST
- Bernard Tuy, Jérôme Durand, Emmanuel Goiffon, Renater
- Peter Kirstein, Steve Hailes, Piers O'Hanlon, UCL
- Wolfgang Fritsche, IABG
- Jim Bound, Hewlett Packard
- Patrick Grostete, Cisco
- Mohsen Souissi, AFNIC
- Alain Durand, Sun Microsystems
- Bill Manning, ISI
- Alain Baudot, France Telecom R&D
- Pedro Lorga, FCCN
- And many others

What is new with IPv6?

- Security was considered from the start in IPv6
  - One can rely on certain features existing
  - When new services were considered, their security was part of IPv6 thinking
- Some of the key improvements:
  - IPsec useable with the core protocols
  - Cryptographically Generated Addresses (CGA)
  - SEcure Neighbor Discovery (SEND)
  - Making intrusion harder

Threats to be encountered in IPv6

- Scanning Gateways and Hosts for weakness
- Scanning for Multicast Addresses
- Unauthorised Access Control
- Firewalls
- Protocol Weaknesses
- Distributed Denial of Service
- Transition Mechanisms
- Worms/Viruses
  - There are already worms that use IPv6 (Rbot.DUD,

Scanning Gateways and Hosts

- 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)
- 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

Scanning Multicast Addresses

- New (IPv6) multicast addresses - IPv6 supports multicast addresses that can enable an attacker to identify key resources on a network and attack them
  - – For example, and all DHCP servers (FF05::5)
    - All-node/all-router multicast addresses are in IPv4 (2240.0.1,2) already
      - – Though these can provide for new DoS opportunities
  - – Addresses must be filtered at the border in order to make them unreachable from the outside
    - IPv6 specs forbids the generation of ICMPv6 packets in response to messages to global multicast addresses that certain requests

Security of IPv6 addresses

- Cryptographically Generated Addresses (CGA) IPv6 addresses [RFC3972]
  - Host-ID part of address is carry hashed information about public key
    - Binds IPv6 address to public key without requiring a key management infrastructure
  - Used for securing Neighbor Discovery [RFC3971]
  - Is being extended for other uses [RFC4581]
- Private addresses as defined [RFC 3041]
  - prevents device/user tracking from
  - makes accountability harder
- Host-ID could be a token to access to a network

Autoconfiguration / Neighbor Discovery

- Neighbor Discovery (cf Address Resolution Protocol)
  - Can suffer similar problems of ARP cache poisoning
- Better solution with SEcure Neighbor Discovery (SEND) [RFC3971]
  - Uses CGA
    - Linux implementation: DoCoMo's Open Source SEND Project
- DHCPv6 with authentication is possible
- ND with IPSec also possible

Unauthorised Access Control

- Policy implementation in IPv6 with Layer 3 and Layer 4 is still done in firewalls
- Some design considerations!
  - Filter site-scoped multicast addresses at site boundaries
  - Filter IPv4 mapped IPv6 addresses on the wire

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

Unauthorised Access control

- Non-routable + bogon (unallocated) address filtering slightly different
  - in IPv4 easier deny non-routable + bogons
  - in IPv6 simpler 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
Deny	3ffe::/16	host/net	any	service
deny	any	any		

L3- L4 Spoofing

- 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 <– >MAC address (user) mapping for accountability!

Amplification (DDoS) Attacks

- There are no broadcast addresses in IPv6
  - This would stop any type of amplification attacks that send ICMP packets to the broadcast address
  - Global multicast addresses for special groups of devices, e.g. link-local addresses, etc.
- IPv6 specifications forbid the generation of ICMPv6 packets in response to messages to global multicast addresses
  - 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 implementations follow the ICMPv6 specification [RFC 4443]
- Implement Ingress Filtering
  - Defeating Denial of Service Attacks which employ IP Source Address Spoofing [RFC 2827]
- Implement ingress filtering of IPv6 packets with IPv6 multicast source address

Mixed IPv4/IPv6 environments

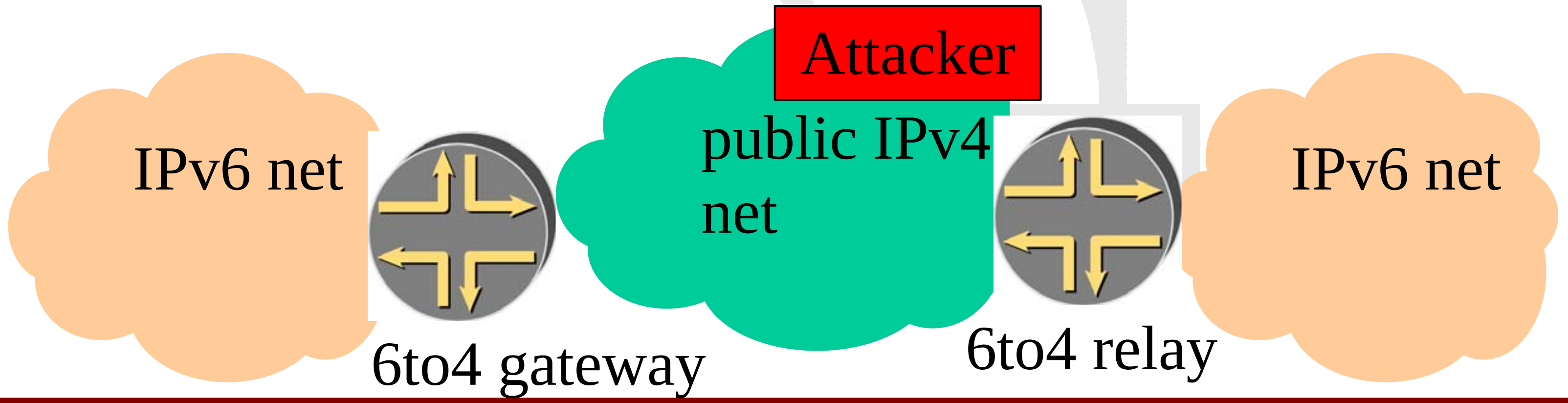
- There are security issues with the transition mechanisms
  - Tunnels are extensively used to interconnect networks over areas supporting the “wrong” version of protocol
  - Tunnel traffic many times has not been anticipated by the security policies. It may pass through firewall systems due to their 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

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 tunnelling spoofed traffic can be injected from IPv4 into IPv6.
  - IPv4 Src: Spoofed IPv4 Address
  - IPv6 Src: 2002:: Spoofed Source



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
- TCP ICMP attacks – slight differences with ICMPv6
  - http://tools.ietf.org/html/draft-gont-tcpm-icmp-attacks-05
- 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

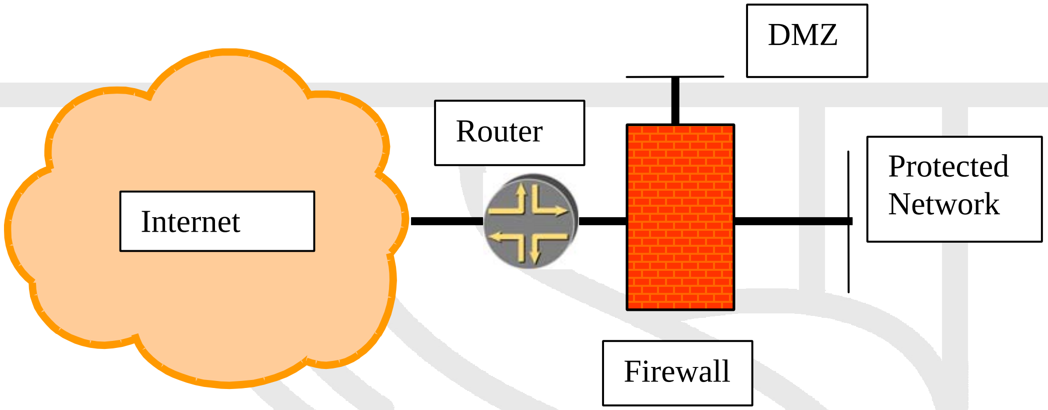
Vulnerability testing/assessment

- Testing tools
  - – Ettercap, nmap, LSOF, Snoop, DIG, Etherape, Wireshark, Fping, Ntop, SendIP, TCPDump, WinDump, IP6Sic, NetCat6, Ngrep, THC Amap
- Assessment tools
  - – SAINT, nessus, ndpmon,

Firewalls

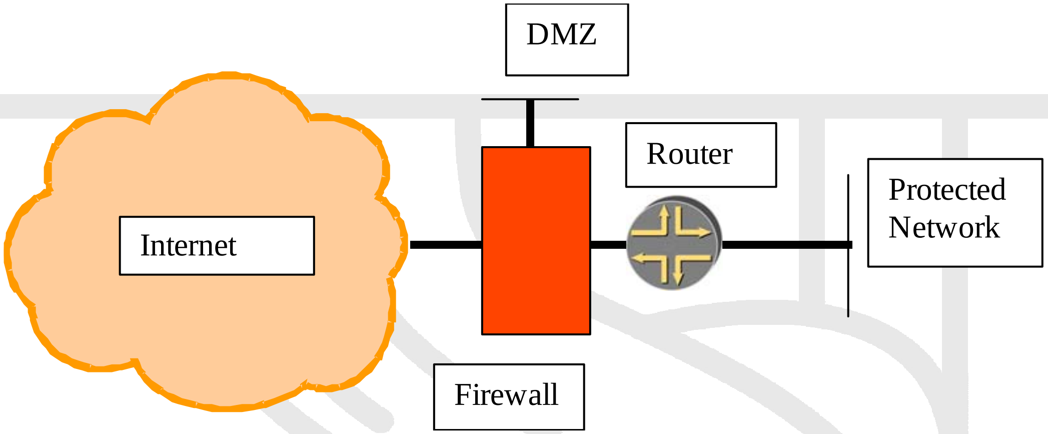
- IPv6 architecture and firewall - requirements
  - No need to NAT – same level of security with IPv6 possible as with IPv4 (security and privacy)
    - Even better: e2e security with IPSec
  - Weaknesses of the packet filtering cannot be hidden by NAT
  - IPv6 does not require end-to-end connectivity, but provides end-to-end addressability
  - Support for IPv4/IPv6 transition and coexistence
  - Support for IPv6 header chaining
  - Not breaking IPv4 security
- There are some IPv6-capable firewalls now
  - Cisco ACL/PIX, iptables, ipfw, Juniper NetScreen

IPv6 firewall setup - method1



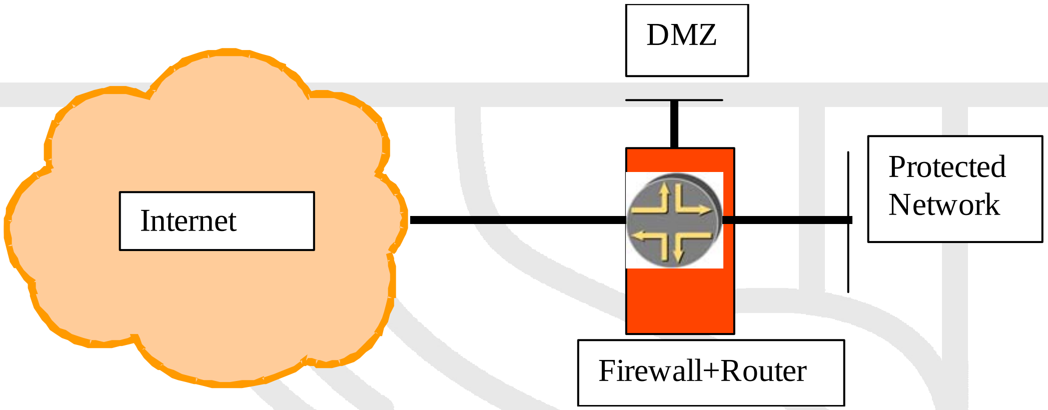
- Internet ↔router↔firewall↔net architecture
- Requirements:
  - Firewall must support/recognise ND/NA filtering
  - Firewall must support RS/RA if Stateless Address Auto-Configuration (SLAAC) is used
  - Firewall must support MLD messages if multicast is required

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

Firewalls L4 issues

- FTP
  - 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)

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
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

IPv6 specific

required

Firewall setup 2

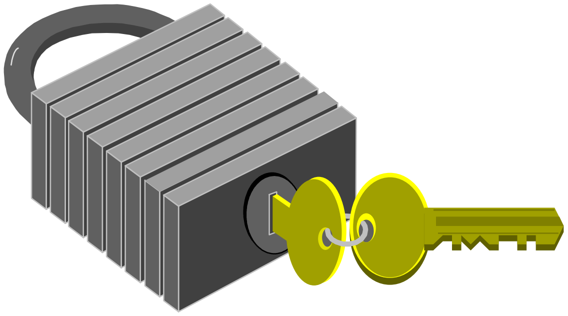
- No blind IP options (→ extension Header) filtering possible:

Hop-by-hop header	What to do with jumbograms or router alert option? – probably log and discard – what about multicast 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

Security: VPNs

- Layer 2 solutions
  - MPLS
- **IPSe**curity
  - IPSec - Suite of protocols
- Other solutions
  - E.g. OpenVPN, Tinc, yavipin

Security: IPSec



- General IP Security mechanisms
  - From the IETF IPsec Working Group
    - http://tools.ietf.org/wg/ipsec/
    - IP Security Architecture: RFC 4301
- Applies to both IPv4 and IPv6:
  - **Mandatory for IPv6**
  - Optional for IPv4
- Applicable to use over LANs, across public & private WANs, & for the Internet
- IPSec is a security framework
  - Provides suit of security protocols
  - Secures a pair of communicating entities

IPsec protocol overview

- IPsec services
  - Authentication
    - AH (Authentication Header - RFC 4302)
  - Confidentiality
    - ESP (Encapsulating Security Payload - RFC 4303)
  - Replay protection, Integrity
  - Key management
    - IKEv2 (Internet Key Exchange - RFC4306)
- Implementations
  - Linux-kernel (USAGI), Cisco IOS-12.4(4)T, BSD&OSX(Kame)

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.
- Other elements are in prototype state
  - CGA, SEND, PANA, VPNs

But even these are ready for experimental deployment