



**111 Short Module on Security**

# Copy ...Rights



IPv6 Deployment and Support

- ***This slide set is the ownership of the 6DEPLOY project via its partners***
- ***The Powerpoint version of this material may be reused and modified only with written authorisation***
- ***Using part of this material must mention 6DEPLOY courtesy***
- ***PDF files are available from [www.6deploy](http://www.6deploy)***
- ***Looking for a contact ?***
  - ***Mail to : [martin.potts@martel-consulting.ch](mailto:martin.potts@martel-consulting.ch)***
  - ***Or [bernard.tuy@renater.fr](mailto:bernard.tuy@renater.fr)***

# Acknowledgements



IPv6 Deployment and Support

- **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 (now Arch Rock)**
- **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?



IPv6 Deployment and Support

- **Security was considered from the start in IPv6**
- **Some of the key improvements:**
  - **IPsec useable with the core protocols**
  - **Cryptographically Generated Addresses (CGA)**
  - **SEcure Neighbor discovery (SEND)**
  - **Protocol for Authentication and Network Access**
  - **Making intrusion harder**

# Threats to be Countered 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**
    - **e.g. Rbot.DUD**

# Scanning Gateways and Hosts

IPv6 Deployment and Support

- **Subnet Size is much larger**
  - **About 500,000 years to scan a /64 subnet @ 1M addresses/sec**
- **But...**
  - **NMAP does support IPv6 network scanning**
  - **IPv6 Scanning methods are changing**
    - **DNS based, parallelised scanning, common numbering**
  - **Compromising a router at key transit points**
    - **Can discover addresses in use**

# Scanning Multicast Addresses



IPv6 Deployment and Support

- **New Multicast Addresses - IPv6 supports new multicast addresses enabling attacker to identify key resources on a network and attack them**
  - **E.g. Site-local all DHCP servers (FF05::5), and All Routers (FF05::2)**
  - **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 contain requests**

# Security of IPv6 addresses



IPv6 Deployment and Support

- **Cryptographically Generated Addresses (CGA) IPv6 addresses [RFC3972]**
  - Host-ID part of address is an encoded hash
    - Binds IPv6 address to public key
  - Used for securing Neighbor Discovery [RFC3971]
  - Is being extended for other uses [RFC4581]
- **Private addresses as defined [RFC 4941]**
  - prevents device/user tracking from
  - makes accountability harder
- **Host-ID could be token to access network**



---

# Autoconfiguration/Neighbor Discovery



IPv6 Deployment and Support

- **Neighbor Discovery (cf Address Resolution Protocol)**
  - Can suffer similar problems of ARP cache poisoning
- **Stronger solution with SEcure Neighbor Discovery (SEND) [RFC3971] uses CGA**
  - Available in IOS-12.4(24)T, Linux/BSD (DoCoMo's SEND Project)
- **DHCPv6 with authentication is possible**
- **ND with IPSec also possible**

---

# Unauthorised Access Control



IPv6 Deployment and Support

- **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**

# Unauthorised Access control



IPv6 Deployment and Support

- **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
- Simpler due to IPv6 address hierarchy
- However host part of the address is not protected
  - You need IPv6  $\leftrightarrow$  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



IPv6 Deployment and Support

- **Be sure that your host implementations follow the ICMPv6 spec [RFC 4443]**
- **Implement Ingress Filtering**
  - **Defeats 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

- **Some security issues with transition mechanisms**
  - **Tunnels often interconnect networks over areas supporting the “wrong” version of protocol**
  - **Tunnel traffic often not anticipated by the security policies. It may pass through firewall systems due to their inability to 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 authorised systems should be allowed as tunnel end-points**

# IPv6 transition mechanisms



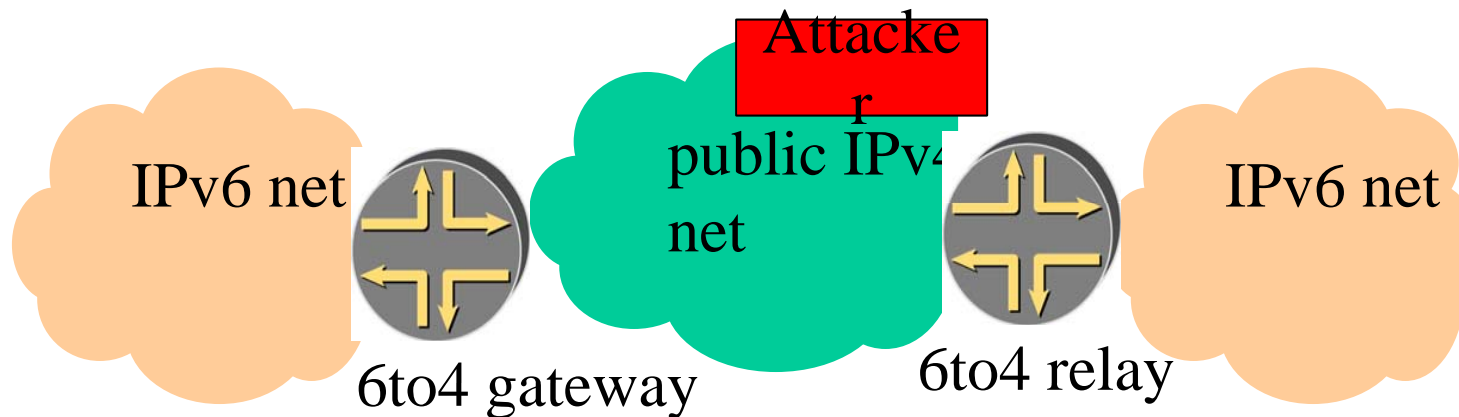
IPv6 Deployment and Support

- **~15 methods possible in combination**
- **Dual stack:**
  - enable the same security for both protocol
- **Tunnels:**
  - ip tunnel – punching the firewall (protocol 41)
  - gre tunnel – probably 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
- **ICMP attacks – slight differences with ICMPv4**
  - Recommendations for Filtering ICMPv6 Messages in Firewalls (RFC4890)
  - TCP ICMP attacks – slight differences with ICMPv6
    - <http://tools.ietf.org/html/draft-ietf-tcpm-icmp-attacks-06>
- **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



IPv6 Deployment and Support

- **Testing tools**

- **Nmap, Ettercap, Lsof, Snoop, DIG, Etherape, Wireshark, Fping, Ntop, SendIP, TCPDump, WinDump, IP6Sic, NetCat6, Ngrep, THC Amap**

- **Assessment tools**

- **SAINT, nessus, ndpmon,**

# Firewalls



IPv6 Deployment and Support

- **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**
  - **Not breaking IPv4 security**
- **Most firewalls are now IPv6-capable**
  - **Cisco ACL/PIX, Juniper NetScreen, CheckPoint**
  - **Modern OSes now provide IPv6 capable firewalls**

# Firewall setup



IPv6 Deployment and Support

## ■ 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 (e.g. Extension header errors)
NS/NA	<b>Required for normal operation – except static ND entry</b>
RS/RA	<b>For Stateless Address Autoconfiguration</b>
Packet too big	<b>Path MTU discovery</b>
MLD	Requirements in for multicast

IPv6 specific

# Firewalls L4 issues



IPv6 Deployment and Support

- **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)**

# Security: VPNs



IPv6 Deployment and Support

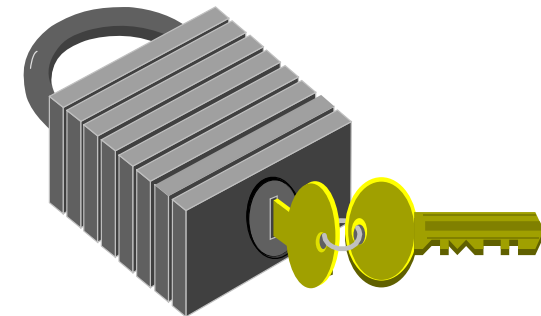
- **Layer 2 solutions**
  - **MPLS**
- **IPSecurity**
  - **IPSec - Suite of protocols**
- **Other solutions**
  - **E.g. OpenVPN, Tinc, yavipin**

# Security: IPSec



Support

- **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



IPv6 Deployment and Support

- **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)**
  - **IPsec modes: Transport Mode & Tunnel Mode**
- **Implementations**
  - **Linux-kernel (USAGI), Cisco IOS-12.4(4)T, BSD&OSX(Kame)**

# Summary



IPv6 Deployment and Support

- **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**