IPv6 Security

Pedro Lorga - lorga@fccn.pt

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*

Contributors

- János Mohácsi, NIIF/HUNGARNET - Hungary
- Octavio Medina, Octavio Medina, Laurent Toutain, ENST
- Bernard Tuy, Jérôme Durand, Emmanuel Goiffon, Renater
- Peter Kirstein, Steve Hailes 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 beginning in IPv6
  - One can rely on certain features existing
- When new services were considered, their security was part of IPv6 thinking
- Some of the areas where the thinking is obvious are:
  - IPsec
  - 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 Mecanisms

Scanning Gateways and Hosts

- Subnet Size is much larger

  (about 500.000 years to scan a /64 subnet@1M addresses/sec)

  – NMAP doesn't even support for IPv6 network scanning

- But…

  - IPv6 Scanning methods are likely to change (DNS, easy to remember numbering)
  - Compromising a router at key transit points

Scanning Multicast Addresses

- 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)
  - Addresses must be filtered at the border in order to make them unreachable from the outside

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 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		

Firewalls

- IPv6 architecture and firewall - requirements
  - 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 IPv4/IPv6 transition and coexistence
  - Not breaking IPv4 security

Firewalls

- 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)

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!

Autoconfiguration/Neighbour Discovery

- Neigbor Discovery ~ security ~ Address Resolution Protocol
  - – No attack tools – arp cache poisoning
  - – No prevention tools – dhcp snooping
- DHCPv6 with authentication is possible
- ND with IPSec also possible

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 implementation follow the RFC 2463 (ICMPv6)
- Implement RFC 2827 (Ingress Filtering)
- Implement ingress filtering of IPv6 packets with IPv6 multicast source address

Other threats

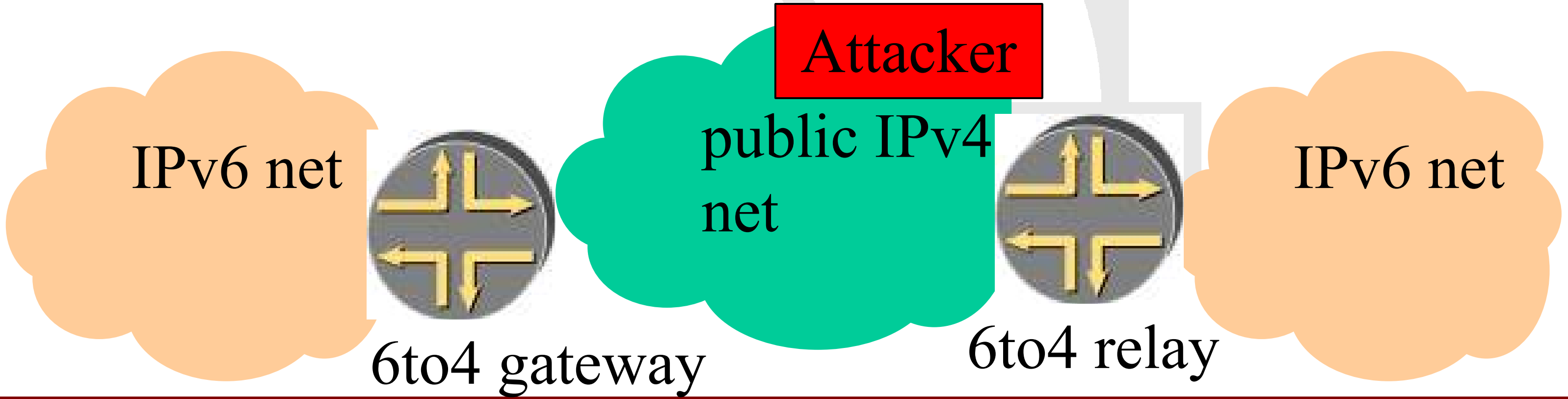
- IPv6 Routing Attack
  - Use traditional authentication mechanisms for BGP and IS-IS.
  - Use IPsec to secure protocols such as OSPFv3 and RIPng
- Viruses and Worms
- Sniffing
  - Without IPsec, IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4
- Application Layer Attacks
  - 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

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

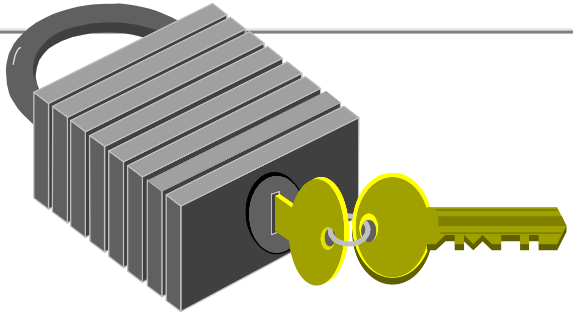
- For example, via 6to4 tunneling spoofed traffic can be injected from IPv4 into IPv6.
  - IPv4 Src: Spoofed IPv4 Address
  - IPv6 Src: 2002:: Spoofed Source



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

IPSec



- General IP Security mechanisms
- provides
  - authentication
  - confidentiality
  - key management
- 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

Security: IPsec

- Work made by the IETF IPsec wg
- Applies to both IPv4 and IPv6 and its implementation is:
  - Mandatory for IPv6
  - Optional for IPv4

- IPsec Architecture: RFC 2401

- IPsec services
  - Authentication
  - Integrity
  - Confidentiality
  - Replay protection

- IPsec protocols: AH (Authentication Header - RFC 2402) & ESP (Encapsulating Security Payload - RFC 2406)

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, PANA, VPNs

But even these are ready for experimental deployment