IPv6 Security

111 Short Module on Security

Copy …Rights

- *Looking for a contact ?*
  - *Mail to : martin.potts@martel-consulting.ch*
  - *Or jordi.palet@consulintel.es*

Acknowledgements

- Carlos Martinez, Arturo Servin – LACNIC
- Jordi Palet - Consulintel
- 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

Agenda

- Comparison of IPv4 and IPv6
- Vulnerabilities in IPv6
- Recommendations

IPv4 / IPv6 Comparison

Comparing IPv4 / IPv6 in One Slide

- IPv4 and IPv6 have very similar features. However the way these features is implemented is different.

	IPv4	IPv6
Addressing	32 bits	128 bits
HW address resolution	ARP	ICMPv6 ND/NA
Host auto-configuration	DHCP & ICMP RS/RA	ICMPv6 RS/RA & DHCPv6 (optional)
IPsec	Optional	Recommended (not mandatory)
Fragmentation	Both hosts and routers can fragment	Only hosts fragment packets

Addressing

- IPv6 uses 128 bit addresses
- In a similar way to IPv4
  - Addresses can be aggregated in prefix in order to simply routing
  - Different «types» of addresses are defined
    - unicast, anycast, multicast
  - Addresses can have different "scopes"
    - link-local, global
- A network host can use different addresses of different types and scopes at each given time
  - This is less common in IPv4, but it can also happen

HW Address Resolution

- Hardware address resolution is needed when transmitting IP (v4/v6) datagrams over an Ethernet / 802.11 or similar layer 2 segment
- IPv4
  - ARP: address resolution protocol
    - A separate entity from the rest of the stack
- IPv6
  - ARP features are folded into ICMPv6's ND (neighbor discovery) sub-protocol

Host Auto-Configuration

- Host-autoconfiguration allows “plug-and-play” network access
- IPv4
  - DHCP + some ICMP messages
- IPv6
  - Two ways: stateless and stateful
  - SLAAC: Stateless Auto Configuration (ICMPv6)
  - DHCPv6: similar to v4 DHCP, stateful

Fragmentation

- Packet fragmentation occurs when a packet being forwarded is too big for the outgoing link MTU
- IPv4
  - Any intermediate router can fragment and reassemble
- IPv6
  - Only hosts can fragment and reassemble
  - Path MTU discovery (ICMPv6)

IPSec

- IPSec allows encryption of IP packet flows
- IPv4
  - IPSec was an afterthought and was implemented years after IPv4 was widely deployed
  - Thus IPSec support was never included in host requirements
- IPv6
  - IPv6 was born with IPSec support already considered
  - IPSec support is however a recommendation but it's not a mandatory requirement

Vulnerabilities and Attacks

Inherent vulnerabilities

- Less experience working with IPv6
- New protocol stack implementations
- Security devices such as Firewalls and IDSs have less support for IPv6 than IPv4
- More complex networks
  - Overlaid with tunnels
  - Dual stack (two protocols on the same wire)

Neighbor Discovering Protocol

- Instead of ARP (IPv4), IPv6 uses Neighbor Discovering Protocol (NDS)
- NDP is based on ICMPv6
- Instead of a broadcast (ARP), NDP uses Neighbor Solicitation y Neighbor Advertisement messages

NDP associated vulnerabilities

- DoS attacks to routers by filling Neighbor Cache with many entries
- Some mittigations are:
  - Rate-limit processing the Neighbor Solicitation (NS)
  - Monitoring NDP traffic (i.e. NDPMon)
  - Deploy SEND (SEcure Neighbor Discovery) RFC3791
  - Static entries
  - draft-gashinsky-v6nd-enhance-00

Autoconfiguration

- Two flavors:
  - Stateless: SLAAC (Stateless Address Auto-Configuration), based in ICMPv6 (Router Solicitation and Router Advertisement)
  - Stateful: DHCPv6
  - SLAAC is mandatory and DHCPv6 is optional
- Routers send Router Advertisement (RA) messages to communicate configuration parameters:
  - Prefixes
  - Routes
  - MTU, hop-limit
  - Timers

Vulnerabilities associated with autoconfiguration

- Rogue RAs and Rogue DHCPv6 servers
  - Intentionally
    - Man in the middle attacks
  - Accidentally
    - Windows sharing!!!
- DoS attacks
- Some considerations documented in RFC6104 and draft-gont-v6ops-ra-guard-evasion

Mitigation of Rogue RAs

- RA-guard for switches (RFC6105) and RA-monitor
  - But only for accidental RAs
  - Cannot detect complex attacks (next hop, fragmentation)
  - Router Advert MONitoring Daemon (RAMOND)
- SEND
- Static configuration

Attack on Address Resolution

- **Attacker can claim victim's IP address**

Attack on DAD

- Attacker hacks any victim's DAD attempts
- IP address can't be configured

SEND ?

- SEND offers efficient mitigation to many issues, but not all, and is not easy to deploy
- Proxying link-operation at first-hop could provide almost the same and a simpler deployment model
  - Requires deployment of smart switches

Transition Mechanisms

- Protocol 41 and other tunnels
  - Unauthorized traffic leaving your network as tunnels (6to4, Teredo, tunnels)
- Automatic tunnels
  - Where is your traffic going?
- Relays to IPv6
  - Who is using your relays?

End-to-End Model

- End-to-End connectivity without NAT
- NAT and NAT-PT (Protocol Translation) for IPv4 used as security strategy (should it be?)
- RFC5902 “Thoughts on IPv6 NAT”
- IPv6-to-IPv6 address mapping (stateless NAT66 as discussed by IETF). Maps a private IPv6 address range (ULA)

In IPv4 Networks

- I do not have IPv6 in my network and I won’t support it. I do not care then
- Well, you should
- Even though you do not run IPv6 in your network, you may be vulnerable:
  - Rogue RA (Windows Network Sharing)
  - 6to4, Teredo and other tunnel technologies
- All these may open holes in your network security

Recommendations

Countering Threats in IPv6

- Scanning Gateways and Hosts for weakness
- Scanning for Multicast Addresses
- Unauthorised Access Control
- Firewalls
- Protocol Weaknesses
- Distributed Denial of Service
- Transition Mechanisms

Scanning Gateways and Hosts

- Subnet Size is much larger
  - About 500,000 years to scan a /64 subnet@1M addresses/sec
- But…
  - IPv6 Scanning methods are changing
    - DNS based, parallelised scanning, common numbering
  - Compromising a router at key transit points
    - Can discover addresses in use
- Avoid:
  - Using easy to guess addresses

Scanning Multicast Addresses

- **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**
    - **To prevent smurf type of attacks: IPv6 specs forbid the generation of ICMPv6 packets in response to messages to global multicast addresses that contain requests**

Security of IPv6 addresses

- 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 Neighbour Discovery [RFC3971]
  - Is being extended for other uses [RFC4581]
- Privacy addresses as defined [RFC 4941]
  - prevents device/user tracking from
  - makes accountability harder

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**

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			Doc prefix - NO
permit	2001::/16	host/net	any	service	
permit	2002::/16	host/net	any	service	6to4 - YES
permit	2003::/16	host/net	any	service	
Deny	3ffe::/16	host/net	any	service	6bone - NO
deny	any	any			

Consult for non exisiting addresses at:
http://www.space.net/~gert/RIPE/ipv6-filters.html

Spoofing

- IPv6 address are globally aggregated making spoof mitigation at aggregation points easy to deploy
- Simpler to protect due to IPv6 address hierarchy
- 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 stops 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
  - No packets with multicast sources should be allowed

Mitigation of IPv6 amplification

- 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

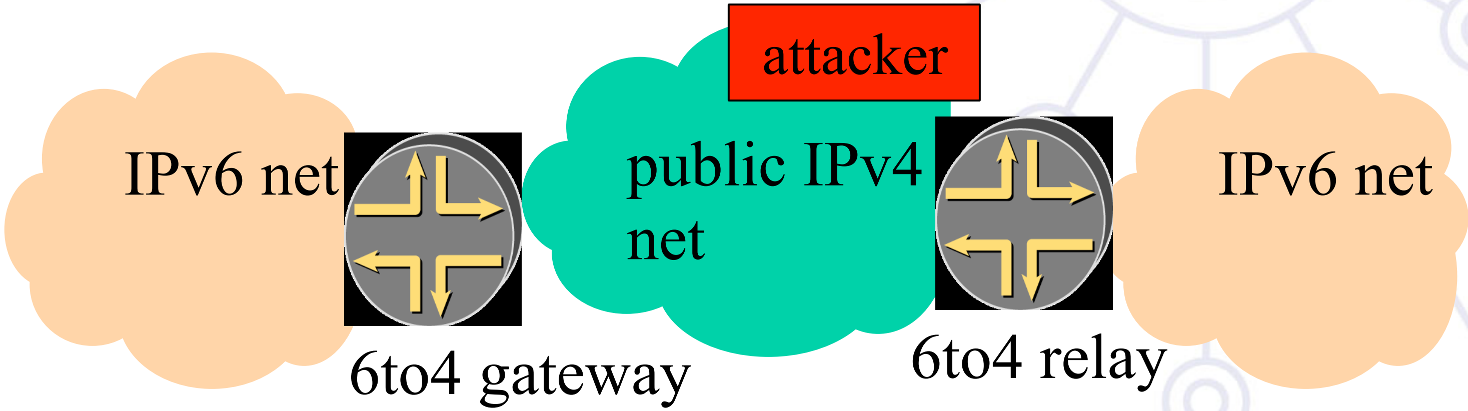
- Some security issues with transition mechanisms
  - Tunnels often interconnect networks over areas supporting the “wrong” version of protocol
  - Tunnel traffic often not anticipated by the security policies. It may pass through firewall systems due to their inability to check two protocols in the 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

- ~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
  - l2tp tunnel – udp therefore better handled by NATs

L3 – L4 Spoofing in IPv4 with 6to4

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



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
  - 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

- **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	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

IPv6 specific (Parameter problem, NS/NA, RS/RA, Packet too big, MLD)

required (NS/NA, RS/RA, Packet too big)

Firewalls L4 issues

- Problematic protocols for stateful filtering
  - FTP
    - Complex: PORT, LPRT, EPRT, PSV, EPSV, LPSV (RFC 1639, RFC 2428)
  - Other non trivially proxy-able protocol:
    - No support (e.g.: H.323)
    - Skype
- Check with your firewall manufacturer for protocol support

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