Results of a Security Assesment of the Internet Protocol version 6 (IPv6)

Fernando Gont

SI6 NETWORKS

Hack In Paris 2012
Paris, France. June 18-22, 2012

About...

- Security Researcher at SI6 Networks (www.si6networks.com)
- Have worked on a number of projects for:
  - UK NISCC (National Infrastructure Security Co-ordination Centre)
  - UK CPNI (Centre for the Protection of National Infrastructure)
- Member at CEDI (I+D), UTN/FRH, Argentina
- Active participant at the Internet Engineering Task Force (IETF)
- More information at: http://www.gont.com.ar

Agenda

- Motivation for this presentation
- Brief comparison between IPv6/IPv4
- Security Implications of IPv6
- Security implications of transition/co-existence mechanisms
- Security implications of IPv6 on IPv4 networks
- Key areas in which further work is needed
- Conclusions
- Questions and answers

Motivation for this presentation

So... what is this IPv6 thing about?

- Designed to address the problem of IPv4 address exhaustion
- Has not yet been widely/globally deployed (<1% global traffic)
- Supported by most general-purpose OSes
- ISPs and other organizations have started to take it more seriously:
  - Exhaustion of the free addresses pool at IANA
  - Awareness activities (World IPv6 Day, World IPv6 Launch Day)
  - Imminent exhaustion of free addresses pool at different RIRs
- Looks like IPv6 is finally taking off...

Motivation for this presentation

- Lots of myths about IPv6 security:
  - Security considered during IPv6 design/standardization
  - Security paradigm will change from network-centric to host-centric
  - Increased use of IPsec
  - etc.
- These myths have had a negative impact on IPv6 deployments
- This presentation will try to:
  - Separate fud from fact
  - Influence how you think about “IPv6 security”

General considerations about IPv6 security

Some interesting aspects...

- Less experience with IPv6 than with IPv4
- IPv6 implementations less mature than their IPv4 counterparts
- Less support in security devices for IPv6 than for IPv4
- The complexity of the resulting Internet will increase:
  - Two Internet protocols
  - Increased used of NATs
  - Increased use of tunnels
  - Use of other transition/co-existence technologies
- Fewer well-trained human resources

... even then IPv6 will be the only option to remain in this business

Brief comparison between IPv6/IPv4

Brief comparison between IPv6/IPv4

- Similar in terms of *functionality*, but not in terms of *mechanisms*

	IPv4	IPv6
Addressing	**32 bits**	**128 bits**
Address Resolution	**ARP**	**ICMPv6 NS/NA (+ MLD)**
Auto-configuration	**DHCP & ICMP RS/RA**	**ICMPv6 RS/RA & DHCPv6 (optional) (+ MLD)**
Fault Isolation	**ICMPv4**	**ICMPv6**
IPsec Support	**Optional**	**Optional**
Fragmentation	**Both in hosts and routers**	**Only in hosts**

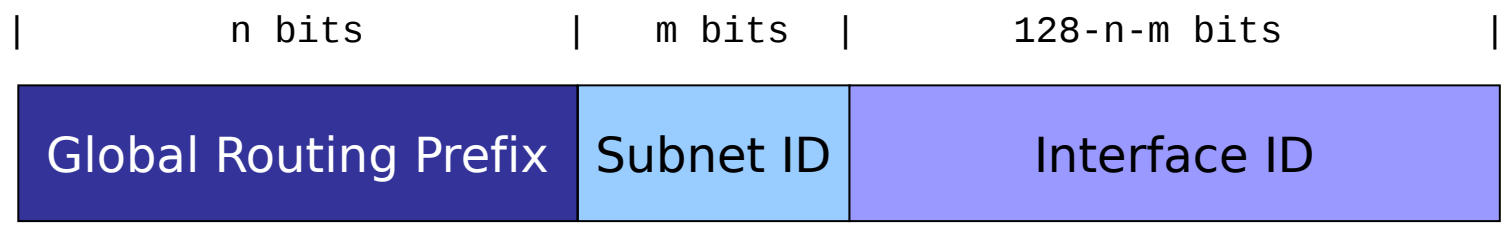
Security Implications of IPv6

IPv6 Addressing
Implications on host scanning

Brief overview of IPv6 addressing

- Main driver for IPv6 deployment
- Employs 128-bit addresses
- Address semantics similar to those of IPv4:
  - Addresses are aggregated intro “prefixes”
  - Several address types
  - Several address scopes
- Each interface typically employs more than one address, of different type/scope:
  - One link-local unicast address
  - One or more global unicast addresses
  - etc.

Global Unicast Addresses



- The “Interface ID” is typically 64-bit long
- Can be selected with different criteria:
  - Modified EUI-64 Identifiers
  - Privacy addresses
  - Manually configured
  - As specified by transition/co-existence technologies

Implications on host scanning

Myth: "*IPv6 host scanning attacks are infeasible... they would take ages!*"

- This claim assumes that addresses are "randomized"
- Malone (*) measured IPv6 addresses in the wild, and categorized them into:
  - SLAAC (MAC address embedded in the Interface ID)
  - IPv4-based (2001:db8::192.168.10.1, etc.)
  - "Low byte" (2001:db8::1, 2001:db8::2, etc.)
  - Privacy addresses (randomized Interface ID)
  - "Wordy" (2001:db8::dead:beef, etc.)
  - Resulting from transition technologies (Teredo, etc.)

(*) Malone, D. 2008. *Observations of IPv6 Addresses*. Passive and Active Measurement Conference (PAM 2008, LNCS 4979), 29–30 April 2008.

IPv6 addresses in the real world

- Results obtained by [Malone, 2008] (*):

Hosts

Address Type	Percentage
SLAAC	50%
IPv4-based	20%
Teredo	10%
Low-byte	8%
Privacy	6%
Wordy	<1%
Other	<1%

Routers

Address Type	Percentage
Low-byte	70%
IPv4-based	5%
SLAAC	1%
Wordy	<1%
Privacy	<1%
Teredo	<1%
Other	<1%

(*) Malone, D. 2008. *Observations of IPv6 Addresses*. Passive and Active Measurement Conference (PAM 2008, LNCS 4979), 29–30 April 2008.

Some conclusions

- IPv6 host scanning attacks are feasible
- They have already been seen in the wild
- They will leverage:
  - Patterns in IPv6 addresses
  - “Leaks” at the application layer
  - Multicast addresses, Neighbor discovery, etc. (for local scans)
- Recommendations:
  - Avoid any patterns in IPv6 addresses
  - We should update some standards (see draft-ietf-6man-stable-privacy-addresses)
  - Always consider the use of firewalls and NIDS

IPv6 addressing
Implications on end to end connectivity

Brief overview

- The IPv4 Internet originally followed the “End to End Principle”
  - Dumb network, smart hosts
  - Communication is allowed between any two nodes
  - The network does not inspect the payload of packets
- It is usually argued that this principle fosters innovation
- NATs (and firewalls) have removed this principle from the Internet
- Since IPv6 does not need IPv6, it is expected that IPv6 deployment will return the End to End Principle

IPv6 and the “End to End Principle”

Myth: “*IPv6 will return the 'End to End Principle' to the Internet*”

- It is assumed that the increased address space will return this principle
- However,
  - Global addressing != end to end connectivity
  - Most networks don't care about innovation
  - Users expect in IPv6 the same services they know from the IPv4 world
  - End to end connectivity would increase host exposure
- That is,
  - End to end connectivity is not necessarily desirable
  - Typical IPv6 subnets will only allow outgoing/returning traffic (by means of firewalls)

Address Resolution

Brief overview

- Address resolution: IPv6 → link-layer
- Employs “Neighbor Discovery”:
  - Based on ICMPv6 messages (Neighbor Solicitation y Neighbor Advertisement)
  - Analogous to ARP Request and ARP Reply
  - Implemented on top of IPv6, rather than on top of the link-layer

Vulnerabilities and countermeasures

- IPv4 ARP-based attacks can be ported to the IPv6 world:
  - Man in The Middle
  - Denial of Service
- Possible counter-measures:
  - Deploy SEND
  - Monitor Neighbor Discovery traffic
  - Employ static entries in the Neighbor Cache
  - Restrict access to the local network

Vulnerabilities and countermeasures (II)

- Unfortunately:
  - SEND is hard to deploy
  - Monitoring are (currently) easy to circumvent
  - Use of static entries in the Neighbor Cache does not scale
  - It is usually hard/undesirable to restrict access to the local network
- In summary,
  - The IPv6 situation is similar to that of the IPv4 world
  - Maybe a bit more complicated
    - See draft-gont-6man-nd-extension-headers

Auto-configuration

Brief overview

- Two autoconfiguration mechanisms for IPv6:
  - Stateless Address Auto-Configuration (SLAAC)
    - Based on ICMPv6
  - DHCPv6
    - Based on UDP
- SLAAC is mandatory, while DHCPv6 is optional
- Basic operation of SLAAC:
  - Host request configuration information with ICMPv6 Router Solicitations
  - Routers respond with Router Advertisements:
    - Auto-configuration prefixes
    - Routes
    - Network parameters
    - etc.

Vulnerabilities and counter-measures

- Spoofed Router Advertisements can be leveraged to perform:
  - Man In the Middle attacks
  - Denial of Service attacks
- Possible counter-measures:
  - Deploy SEND (in your dreams)
  - Monitor RS/RA messages (if you can)
  - Deploy RA-Guard (if Cisco fixes it)
  - Restrict access to the local network (if you can)

Vulnerabilities and counter-measures (II)

- Unfortunately,
  - SEND is hard to deploy
  - Monitoring tools are (currently) easy to circumvent
  - RA-Guard is (currently) easy to circumvent
  - It is usually hard/undesirable to restrict access to the local network
- In summary,
  - The IPv6 situation is a little bit more complicated than that of IPv4

IPsec Support

Brief overview and considerations

Myth: "*IPv6 is more secure than IPv4 because security was considered during the design of the protocol*"

- This claim is usually based on the initial mandatory-ness of IPsec for IPv6
- In practice, such mandatory-ness has always been irrelevant:
  - IPsec **support** was mandatory (not its use!)
  - Implementations essentially ignored this requirement
  - The same IPsec deployment obstacles are present in IPv6
- Even the IETF acknowledged this fact
- Conclusion:
  - There is no reason to expect and increased use of IPsec with IPv6

Security Implications of Transition Technologies

Brief overview

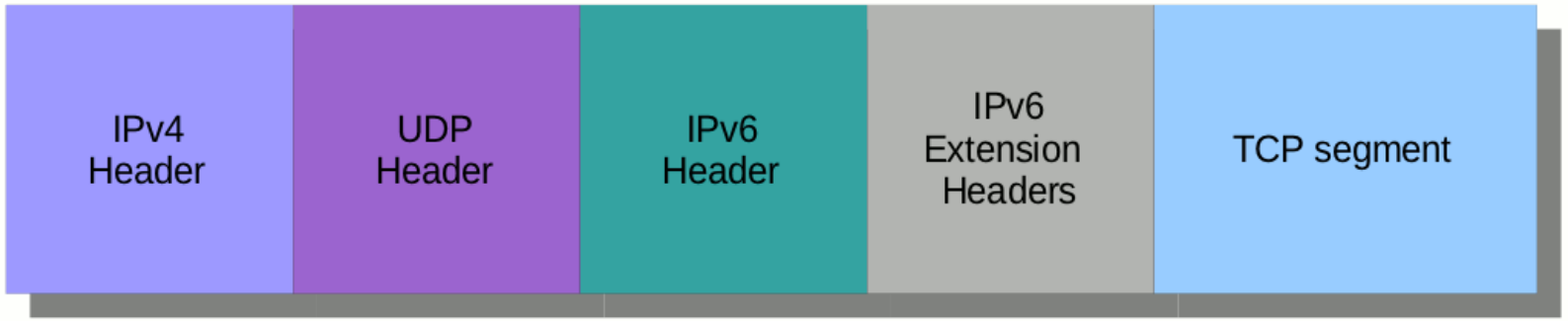
- Original transition plan: dual stack
  - Deploy IPv6 along IPv4, before actually needed it
  - This plan **failed**
- Current strategy is based on a toolbox:
  - Dual stack
  - Tunnels
    - Automatic
    - Configured
  - Translation
    - CGN
    - NAT64
- Most operating systems support a subset of these technologies

Security considerations

- Complexity of the resulting network is increased
- Single Points of Failure (SPoF) are introduced
- Some technologies raise privacy concerns:
  - Which networks does your tunneled traffic traverse?
  - This may (or may not) be a concern to your organization

Security considerations (II)

- Complexity of the resulting traffic is greatly increased
- Deep Packet Inspection is much harder to perform (if at all possible)
- Example: Structure of a Teredo packet:



- “Exercise”: construct a libpcap filter to capture packets destined to host 2001:db8::1, TCP port 25

Security Implications of IPv6 on IPv4 Networks

Brief overview

- Most systems have some some IPv6 support enabled by default
  - Dual stack
  - Teredo
  - ISATAP
  - etc.
- As a result,
  - **Most “IPv4 networks” have already partially deployed IPv6**

Security considerations

- Dormant IPv6 support can be enabled
  - Sending Router Advertisements
  - Enabling transition/co-existence technologies
- Transition technologies may increase host exposure
  - Teredo enables **NAT traversal**
- As a result,
  - There are no “IPv4-only” networks
  - IPv6 security implications should also be considered for IPv4 networks
  - If you don't mean to employ IPv6, make sure that that is the case

Key areas in which further work is needed

Areas in which further work is needed

- IPv6 implementations
  - They have not yet been thoroughly assessed
  - Few assessment tools (THC's and CPNI's)
  - Many bugs and vulnerabilities to be discovered
- IPv6 support in security devices
  - We need feature parity with IPv4
  - Otherwise, we cannot enforce the same security policies
- Education/Training
  - Deploying IPv6 without proper education/training is simply insane
  - Training is needed as different levels of each organization

Some conclusions

Some conclusions

- Beware of IPv6 marketing and mythology
  - They result in negative security implications
- IPv6 prividesa similar service to that of IPv4
  - The actual *mechanisms* are different
  - Devil is in the detail
- Most systems include IPv6 support enabled by default
  - There are no “IPv4-only” networks
  - Every network should consider the IPv6 security implications
- Sooner or later you'll deploy IPv6
  - It is time to learn and experiment with IPv6 (you should have, already!)
  - Only then you should deploy it in production networks

Questions?

Merci!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com