The Truth about IPv6 Security

Fernando Gont

UTN/FRH

FutureNet: MPLS, Ethernet and Beyond

Boston, MA, USA, May 10-13, 2010

Agenda

- Brief comparision of IPv4 and IPv6
- A few myths about IPv6 security
- Transition Technologies
- Ongoing work on IPv6 security at UK CPNI
- Key areas where further work is needed
- Conclusions

Brief comparision of IPv4 and IPv6

- IPv4 and IPv6 are very similar in terms of functionality

	IPv4	IPv6
Addressing	32 bits	128 bits
Auto-configuration	DHCP & RS/RA	ICMPv6 RS/RA & DHCPv6 (opt)
Address resolution	ARP	ICMPv6
IPsec support	Optional	Mandatory
Fragmentation	Both in hosts and routers	Only in hosts

Mandatory IPsec support

Myth: "*IPv6 has improved security as a result of its mandatory IPsec support*"

- IPsec already existed for IPv4
- The mandatory-ness of IPsec for IPv6 is just words on paper
- Also, there are problems with its deployment as a general end-to-end security mechanism
- Deployment of IPsec(v6) has similar problems as those of IPsec(4). As a result, IPsec(v6) is not deployed as a general end-to-end security mechanism, either

Larger address space

Myth: "*It is unfeasible to brute-force scan an IPv6 network for alive nodes, as the IPv6 address space is so large. Such a scan would take ages!*"

- [Malone, 2008] (*) measured IPv6 address assignement patterns
- For hosts,
  - 50% autoconf, 20% IPv4-based, 10% Teredo, 8% "low-byte"
- For infrastructure,
  - 70% "low-byte", 5% IPv4-based
- Anyway, most compromised systems are hosts. Once a host is compromised, brute-force scanning becomes trivial

Size matters… only if you use it properly! ;-)

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

Auto-configuration & address-resolution

- Based on Neighbor Discovery messages (ICMPv6) – DHCPv6 is optional
- Stateless autoconfiguration more powerful than the IPv4 counterpart… but also provides more potential vectors for attackers to exploit (e.g., THC's IPv6 attack suite)
- Less support in Layer-2 boxes for mitigation of ND attacks
- Secure Neighbor Discovery (SEND) was specified for mitigating ND security threats, employing:
  - Cryptographically-Generated Addresses (CGAs)
  - RSA signatures (RSA signature option)
  - Certificates
- Not widely supported (e.g., no support in Windows XP/Vista/7 or KAME)
- Even then, SEND does not eliminate (nor should it) Layer-4+ attack vectors (e.g., DNS spoofing)

Transition technologies

- Original IPv6 transition plan was dual-stack (yes, it failed)
- Current strategy is a transition/co-existence plan based on a toolbox:
  - Configured tunnels
  - Automatic tunnels (ISATAP, 6to4, Teredo, etc.)
  - NATs (NAT64, NAT46, ALGs, etc.)
- Automatic-tunneling mechanisms are enabled by default in Windows Vista and Windows 7
- They may be (and have been) leveraged to bypass local network policies
- Some automatic tunnels use anycast IPv4 addresses:
  - Where is your Teredo and 6to4 traffic going through?
  - This might (or might not) be of concern to you

Ongoing work

(or “what we’re doing on v6 security”)

Ongoing work on IPv6 security at CPNI

- The UK CPNI (Centre for the Protection of National Infrastructure) is currently working on a security assessment of the IPv6 protocol suite
- Similar project to the one we carried out years ago on TCP and IPv4:
  - Security assessment of the protocol specifications
  - Security assessment of common implementation strategies
  - Production of assessment/Proof-Of-Concept tools
  - Publication of best practices documents
- Currently cooperating with vendors and other parties

Further work

(or “what’s missing?”)

Key areas in which further work is needed

- IPv6 Resiliency
  - Implementations have not really been the target of attackers, yet
  - Only a handful of publicly available attack tools
  - Lots of vulnerabilities and bugs still to be discovered.
- IPv6 support in security devices
  - IPv6 transport is not broadly supported in security devices (firewalls, IDS/IPS, etc.)
  - This is key to be able enforce security policies comparable with the IPv4 counterparts
- Education/Training
  - Pushing people to "Enable IPv6" *point-and-click style* is simply **insane**.
  - Training is needed for engineers, technicians, security personnel, etc., **before** the IPv6 network is running.

Conclusions

(or “so what?”)

Conclusions

- Most security vulnerabilities have to do with Layer4+
- No layer-3 protocol will help an unsecured DNS, broken browser, or broken database application
- Even when it comes to previously-known Layer3 issues, IPv6 is not that different from IPv4 to make a difference ☺
- After all, IPv6 is…

"96 more bits, no magic"

-- Gaurab Raj Upadhaya

Questions?

Acknowledgements

- UK CPNI, for their continued support
- Future-Net organizers, for the invitation to present in this conference

Fernando Gont

fernando@gont.com.ar

http://www.gont.com.ar