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

Fernando Gont

project carried out on behalf of the UK CPNI

LACNOG 2010

Sao Paulo, Brazil, October 19-22, 2010

Agenda

- Overview of the IPv6 security project at UK CPNI
- Brief comparision of IPv4 and IPv6
- A few myths about IPv6 security
- Key areas where further work is needed
- Conclusions

IPv6 Security at UK CPNI

(overview of the project)

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

IPv6/IPv4 Comparision

(what changes, and what doesn’t)

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 & ICMP RS/RA	ICMPv6 RS/RA & DHCPv6 (opt) (+ MLDv2)
Address resolution	ARP	ICMPv6 ND/NA (+ MLDv2)
IPsec support	Optional	Mandatory (Recommended?)
Fragmentation	Both in hosts and routers	Only in hosts

Security Implications of IPv6

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

The larger IPv6 address space does not necessarily translate into improved resistance to network reconnaissance

(*) 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

Auto-configuration & address-resolution (II)

- Secure Neighbor Discovery (SEND) was specified for mitigating ND security threats, employing:
  - Cryptographically-Generated Addresses (CGAs)
  - RSA signatures (RSA signature option)
  - Certificates
- Not widely deployed, partially as a result of:
  - Not widely supported (e.g., no support in Windows XP/Vista/7)
  - Incompatible with the SLAAC privacy extensions (enabled by default in Windows Vista/7)
  - Incompatible with IPv6 SLAAC (with MAC-derived EUI-64 identifiers), which is required in some network deployments
  - Currently incompatible with DHCPv6, which is required in a number of deployments (there's ongoing work at the IETF, though)
  - The requirement of a Public-Key Infrastructure (PKI) -- a key obstacle to SEND deployment
  - Intellectual Property Rights (IPR) statements on related technologies (e.g., CGAs)
- Even then, SEND does not eliminate (nor should it) Layer-4+ attack vectors (e.g., DNS spoofing) -- i.e., "there are bigger problems to solve"

Transition/co-existence technologies

- Original IPv6 transition plan was dual-stack (*yes, it didn't work out*)
- Current strategy is a transition/co-existence plan based on a toolbox:
  - Configured tunnels
  - Automatic tunnels (ISATAP, 6to4, Teredo, etc.)
  - Translation (e.g., NATs)
- Automatic-tunneling mechanisms are enabled by default in Windows Vista and Windows 7
- They increase the complexity of the network, and thus the potential of vulnerabilities (e.g., see the Nakibly et al routing-loop attacks)
- They may be (and have been) leveraged to bypass local network policies
- Some automatic tunnels use anycast IPv4 addresses or imply the use of relays:
  - Where is your Teredo and 6to4 traffic going through?
  - This might (or might not) be of concern to you

NAT-free network architectures (?)

Myth: *"IPv6 will return end-to-end connectivity in the Internet"*

- Ironically, NAT66 is one of the most frequently-asked IPv6 features
  - NATs are perceived as providing very useful features for renumbering, topology hiding, hostprivacy/masquerading, etc.
- Some transition/co-existence strategies involve NATs (i.e., some NATs will be introduced during the process of deploying IPv6)
- Even without NATs, end-to-end connectivity is not necessarily a desired feature for all systems – actually, some refer to this as an undesired effect

Reality: The typical IPv6 subnet will be protected by a stateful IPv6 firewall ("only allow return traffic"), and the Internet will have a variety of NATs for quite some time

IPv6 Security Implications on IPv4 networks

- Many systems ship with IPv6 “on by default”, which could be leveraged to exploit vulnerabilities or bypass filtering policies (e.g., vi means of link-local addresses)
- A number of systems ship with some IPv6 transition/co-existence technologies enabled by default (e.g. ISATAP or Teredo) – these have been exploited in the past to bypass network policies
- If you don’t want your **edge** network to have IPv6 connectivity, make sure you enforce such policy – i.e., beware of what is going on in your network

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.

> **20 million engineers need IPv6 training, says IPv6 Forum**
> The IPv6 Forum - a global consortium of vendors, ISPs and national research & Education networks - has launched an IPv6 education certification programme in a bid to address what it says is an IPv6 training infrastructure that is "way too embryonic to have any critical impact.“ (**http://www.itwire.com**)

Conclusions

(or “so what?”)

Conclusions

- The security implications of IPv6 should be carefully considered before deploying it
- This is not an argument against IPv6 deployment: it's about being savvy about what you deploy in your network
- In the long term (once IPv6 products match the features and maturity of their IPv4 counterparts, etc.) network security will not be much different from the current state of affairs
- Most vulnerabilities are found in the upper layers
- 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...

Questions?

Acknowledgements

- UK CPNI, for their continued support
- Christian O'Flaherty, Ruth Puente, Florencia Bianchi, and the LACNOG 2010 organizers in general

Fernando Gont

fernando@gont.com.ar

http://www.gont.com.ar