CPNI
Centre for the Protection
of National Infrastructure

CPNI VIEWPOINT

SECURITY IMPLICATIONS OF IPv6

MARCH 2011

Abstract: IPv6 is coming to a network near you. CPNI has extracted salient points from recently published documents to highlight some of the major security implications of the transition to IPv6. Further guidance on this topic will be available in April 2011.

Disclaimer:

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Executive summary

What is IPv6?

The Internet Protocol version 4 (IPv4) is the core technology employed in the internet to transfer information from one system to another. For more than 25 years, IPv4 has been the core underlying technology enabling services such as the internet, web-browsing, e-mail and mobile smart-phones. However, as a result of the growth of the internet, IPv4 is unable to provide a unique address to each system willing to interconnect with others.

To overcome the exhaustion of IPv4 addresses, the Internet Protocol version 6 (IPv6) was developed, with addresses to allow the foreseeable future growth of the internet. While a number of myths have been created around the capabilities of the IPv6 protocol, its main driver is the increased address space.

Advantages provided by IPv6

The main advantage of IPv6 is that it provides much more address space. Being a more recent protocol, IPv6 does have a few design improvements over IPv4, particularly in the areas of auto-configuration, mobility and extensibility. However, increased address space is the main benefit of IPv6.

What are the key security concerns?

There are a number of factors which make the IPv6 protocol suite challenging from a security standpoint.

- IPv6 implementations are much less mature than their IPv4 counterparts making it likely that a number of vulnerabilities will be discovered and mitigated before their robustness matches that of the existing IPv4 implementations.

- Security products such as firewalls and Network Intrusion Detection Systems have less support for the IPv6 protocols than for their IPv4 counterparts.

- A number of transition/co-existence technologies have been developed to aid in the deployment of IPv6 and the co-existence of IPv6 with the IPv4 protocol. These technologies will increase complexity which may introduce new attack vectors in existing networks.

- Technical personnel have less confidence with the IPv6 protocols than with their IPv4 counterparts. This creates an increased likelihood that security implications are overlooked when the protocols are deployed.

What should be done?

Complete a risk assessment on how IPv6 and related technologies (such as transition/co-existence technologies) may affect the security of existing IPv4 networks.

Develop a transition plan; IPv6 affects every network and there is no ‘do nothing’ option.

Ensure that relevant staff, e.g. network engineers and security administrators, are confident with IPv6 and related technologies before they are required to deploy and operate IPv6 in production networks.

Work with equipment and application suppliers to improve the robustness of their implementations, such that the robustness of IPv6 implementations roughly matches that of typical IPv4 implementations.

Security implications of IPv6

A brief comparison of IPv4 security and IPv6 security

The security implications of the basic IPv6 protocol are, in general, very similar to those of IPv4. Similar vulnerabilities are present in both protocols, with the only differences lying in the specific attack vectors provided by each of protocol.

However, IPv6 protocol suite comprises a number of supporting protocols that are, in general, more complex than their IPv4 counterparts (or that were not even present in the IPv4 protocol suite). For example, for the purpose of host configuration, IPv6 provides not only DHCPv6 (the equivalent of DHCP for IPv4), but also a mechanism for StateLess Address Auto-Configuration (SLAAC) that introduces a number of attack vectors which were not present in IPv4.

Regardless of the similarities and differences between IPv4 and IPv6, a key aspect in the resulting level of security of IPv6 networks is the level of IPv6 support in security devices. It is generally the case that there are better security features in IPv4 products compared with IPv6 products, either in terms of the variety of products, the variety of features or performance. This will probably make it difficult to enforce exactly the same policies in IPv6 networks as are enforced in IPv4 networks, at least for a period of time. Consequently, this situation could be exploited by attackers who may leverage IPv6 to bypass network security controls.

Transition planning

There are a variety of different network scenarios in which the IPv6 protocols can be deployed, and a variety of transition mechanisms that might be employed in each of those scenarios for the purpose of deploying IPv6.

It is important that the appropriate scenario and mechanisms are identified at the outset before resources are expended or weaknesses exposed.

As a minimum, the transition plan[1] should include:

- A requirements analysis to identify scope;
- A sequencing plan for implementation;
- Development of IPv6 policies and mechanisms;
- Development of training for key team members;
- Development of a test plan for compatibility and inter-operability;
- Maintenance and monitoring programmes;
- An ongoing update plan for critical architecture;
- A plan for the phased withdrawal from service of IPv4 services and equipment.

[1] Transition Plan adapted from NIST SP800-14

Security implications of a dual-stack approach

IPv6 is not backwards compatible with IPv4. This generally means that at least during the transition period IPv6 will need to operate in parallel with IPv4. This has a number of security and operational implications.

Running a dual-stack (IPv4 and IPv6 simultaneously) increases the complexity of the network as a system. Dual-stack nodes need to implement two different sets of protocols, network administrators need to configure two different set of protocols, security administrators need to enforce security policies for two different sets of protocols, and so on. At core routers, support of both IPv4 and IPv6 protocols generally means that two instances of routing protocols and routing tables must be supported, which increases the complexity of the network, may increase the hardware requirements, and increases the available attack surface.

In some cases, legacy devices may not provide the necessary IPv6 functionality to match that currently provided for IPv4, and this may result in asymmetric functionality or enforced policies for IPv4 and IPv6. [CORE, 2007] is an advisory about an IPv6 vulnerability found in a very secure operating system. This is probably a good example that running two protocol stacks comes at a cost.

Transition technologies may also add to this burden, as in general they not only result in increased complexity, but also prevent existing security devices from enforcing the same type of policies they can apply to native IPv4 or native IPv6 traffic.

Security implications of NAT-free network architectures

Network Address Translators (NAT) provide a number of benefits in a network such as reduced host exposure, host privacy/ masquerading and topology hiding. The current internet architecture has incorporated the use of NATs originally as a stop-gap mechanism for the imminent exhaustion of the IPv4 address space.

As IPv6 allows the assignment of at least one ‘public’ address to each device connected to the internet, it is generally claimed or assumed that IPv6 network architectures will not accommodate NAT devices. This would drastically change the architecture of most current networks, in which NATs isolate internal nodes from the public internet unless communication has been initiated from the internal realm of the NAT (i.e. the ‘internal’ network). That is, exposure of nodes to the public internet would tend to increase.

However, it should be noted that the deployment of IPv6 does not necessarily imply a return to end-to-end connectivity, nor does it preclude similar network architecture to that achieved today through the use of NATs. For instance, it is very likely that IPv6 will be deployed in enterprises along with a perimeter firewall that only allows packets to traverse the firewall from the external realm to the internal realm if communication was initiated from the internal realm (i.e. ‘only allow return traffic for communications initiated from the internal network’).

A number of other technologies might be employed to achieve a similar level of host privacy/masquerading and network topology hiding to that currently achieved in IPv4 with NATs and other technologies.

Security implications of IPv6 within IPv4 networks

A number of transition technologies have been developed to aid in the deployment of IPv6 and the co-existence of IPv6 with IPv4 deployments. Some of these technologies aid in the deployment of IPv6 by enabling communication between islands of one network protocol (e.g. IPv6) across networks that employ some other network protocol (e.g. IPv4). This is achieved with the ‘tunnelling’ paradigm, in which one network protocol (e.g. IPv6) is encapsulated within another network protocol (e.g. IPv4).

While these technologies provide a valuable functionality, this comes at the cost of increased complexity, with the consequent security implications. For example, tunnels may introduce Denial-of-Service (DoS) attack vectors, and may prevent network security devices from enforcing the same security controls that they can readily enforce on non-tunnelled traffic.

Furthermore, some transition technologies require little or no management, and are enabled by default in some popular operating systems. This may result in a site or node making unintended use of IPv6 transition/co-existence technologies which could increase the exposure to attack, and/or be leveraged by attackers to bypass network security controls.

As a result, IPv6 transition/co-existence technologies should be a concern not only to network engineers and security administrators operating or managing IPv6 networks, but also to network engineers and security administrators operating or managing IPv4 networks, whose security policies might be by-passed by leveraging these technologies.

IPv6 support in network devices

A concern when planning to deploy IPv6 should be the level of IPv6 support (if any) in each of the different network devices. There is ongoing work at the IETF[2] to specify a number of desired features for different IPv6 network devices.

[Singh, H., Beebee, V., Donley, C., Stark, B., Troan, O. 2010] specifies a set of features for an IPv6 Customer Edge (CE) router used in homes or small offices.

[Woodyatt, 2010] recommends a number of features in Customer Premises Equipment (CPE) with the goal of providing ‘simple security’ capabilities at the perimeter of local-area IPv6 networks in homes or small offices.

[Vyncke and Townsley, 2010] specifies desired features for advanced security in IPv6 Customer Premises Equipment (CPE).

[2] IETF: Internet Engineering Task Force

A number of surveys are available that indicate the IPv6 support in different network devices:

- [IPV6READY, 2010] identifies the level of IPv6 support in different network devices.
- [ARIN, 2010] contains a survey of IPv6 support in Broadband CPE.
- [RIPE, 2010a] contains the results of an IPv6 CPE survey carried out by RIPE Labs.
- [ICANN, 2007] contains the results of a survey of IPv6 support in commercial firewalls (dated 2007).

It is generally the case that there is more support for security features in IPv4 products than in IPv6 products, either in terms of variety of products, variety of features, or performance. This will probably make it difficult to enforce exactly the same policies with IPv6 as are enforced with IPv4, at least for a period of time. Consequently, this situation could be exploited by attackers who would probably leverage IPv6 to bypass network security controls, etc..

With both protocols, specific security issues are more likely to be found at the practical level than in the specifications. The practical issues include, for instance, bugs or available security mechanisms on a given product. When deploying IPv6, it is important to ensure that the necessary security capabilities exist on the network components specifically when dealing with IPv6 traffic. For instance, firewall capabilities have often been a challenge in IPv6 deployments.

IPv6 support in applications

Many applications currently do not support IPv6, or have only recently been updated to incorporate support for IPv6. This means that their maturity is less than their IPv4-only counterparts, and it is very likely that a number of vulnerabilities will be discovered in them before their maturity matches that of IPv4 applications.

[Strongburg, 2010] explains how IPv6 access could be leveraged in a popular webmail application for the purpose of anonymity. Similar issues could probably exist in other applications.

It should be noted that application security is not likely to be affected by IPv6 itself, but as a result of a lack of secure software development practices (as it is still the case in IPv4).

[Shin, M-K., Hong, Y-G., Hagino, J., Savola, P., Castro, E. 2005] analyses different scenarios and aspects of application transition such as how to enable IPv6 support in applications.

[Arkko, 2010] discusses IPv6 support in some popular applications.

IPv6 training

In addition to any potential shortcomings of the IPv6 protocols, it is very likely that the ‘human factor’ will play a key role when it comes to the resulting network security.

While IPv6 provides a similar functionality to that provided by IPv4, there are substantial differences in how such functionality is achieved. As a simple example, compare how address resolution is performed in IPv6 vs. IPv4 (i.e., Neighbour Discovery vs. Address Resolution Protocol).

Many organisations are likely to end up deploying the IPv6 protocols without proper training, laboratory experimentation, etc., resulting in the deployment of IPv6 in production networks without the same level of confidence with which the IPv4 protocols have been deployed and are currently operated.

Even if an organisation has no concrete plans to deploy IPv6 in the near term, it is highly likely that the network will be affected by IPv6 issues beyond its immediate control, so it is recommended that network and security staff be trained on the IPv6 protocol suite. It would also be sensible to conduct experimentation in network laboratories, so that expertise is gained before network and security teams are urged to deploy the IPv6 protocols in production networks.

References

Arkko, J. 2010. *Experiences from an IPv6-Only World at Ericsson*. Google IPv6 Implementer's Conference 2010. Slides available at: sites.google.com/site/ipv6implementors/2010/agenda/11_Arkko_goog_nat64exp.pdf

ARIN. 2010. Broadband CPE. ARIN IPv6 Wiki.
Available at: www.getipv6.info/index.php/Broadband_CPE

CORE. 2007. *OpenBSD's IPv6 mbufs remote kernel buffer overflow*
Available at: www.coresecurity.com/content/open-bsd-advisorie

ICANN. 2007. *SAC 021: Survey of IPv6 Support in Commercial Firewalls*. ICANN Security and Stability Advisory Committee.
Available at: www.icann.org/en/committees/security/sac021.pdf

IPV6READY. 2010. *IPv6 Ready Logo Program Approved List*
Available at: ipv6ready.org/db/index.php/public/ .

ISOC, 2011, *Internet Issues – Ipv6*
Available at: www.isoc.org/internet/issues/ipv6_faq.shtml#q9

RIPE. 2010a. *IPv6 CPE Survey*. RIPE Labs
Available at: labs.ripe.net/Members/marco/content-ipv6-cpe-survey

Shin, M-K., Hong, Y-G., Hagino, J., Savola, P., Castro, E. 2005. *Application Aspects of IPv6 Transition*. RFC 4038.

Singh, H., Beebee, V., Donley, C., Stark, B., Troan, O. 2010. *Basic Requirements for IPv6 Customer Edge Routers*. IETF Internet-Draft
(draft-ietf-v6ops-ipv6-cpe-router-07.txt), work in progress.

Strongburg, H. 2010. *GMail complete anonymity possible via IPv6*.
Post to the Full-disclosure mailing-list.
Available at: lists.grok.org.uk/pipermail/full-disclosure/2010-August/075876.html

Vyncke, E., Townsley, M. 2010. *Advanced Security for IPv6 CPE*. IETF Internet-Draft
(draft-vyncke-advanced-ipv6-security-01.txt), work in progress.

Woodyatt, J. 2010. *Recommended Simple Security Capabilities in Customer Premises Equipment for Providing Residential IPv6 Internet Service*. IETF Internet-Draft
(draft-ietf-v6ops-cpe-simple-security-12.txt), work in progress.

Further IPv6 reading

The following documentation provides specific information on deployment issues:

CPNI Guidance: ‘Security Considerations for IPv6 Deployment’ due in March 2011

NIST Special Publication SP800-14 ‘Guidelines for secure deployment of IPv6’ December 2010

6UK.org.uk ‘IPv6 Project Planning Guide’ April 2010

Internet draft ‘Transition Guidelines’ [Arkko and Baker, December 2010] provides an overview of IPv6 deployment models and migration tools.

RFC 3750 [Huitema et al, 2004a] defines a number of scenarios with transition mechanisms in unmanaged networks (typically home networks or small office networks).

RFC 3904 [Huitema et al, 2004b] analyses transition strategies for these scenarios, and also provides a general discussion of transition mechanisms (e.g., the properties of automatic vs. configured tunnels).

RFC 3574 [Soininen, 2003] provides some discussion of transition scenarios for 3GPP networks.

RFC 4029 [Lind et al, 2005] analyses different scenarios for the introduction of IPv6 into an ISP’s existing IPv4 network without disrupting the IPv4 service.

RFC 4057 [Bound} ‘IPv6 Enterprise Network Scenarios’ defines a small set of basic enterprise scenarios and includes pertinent questions to allow enterprise administrators to further refine their deployment scenarios in terms of co-existence with IPv4 nodes, networks and applications, and in terms of basic network infrastructure requirements for IPv6 deployment.

RFC 4852 [Bound, Pouffary, Klynsma, Chown, Green. April 2007] ‘IPv6 Enterprise Network Analysis - IP Layer 3 Focus’ analyses the transition to IPv6 in enterprise networks characterised as having multiple internal links and one or more router connections to one or more Providers, and managed by a network operations entity.

[Carpenter and Jiang, 2010] analyses emerging Service Provider (SP) scenarios for IPv6 deployment, which allow for interworking between IPv6-only and legacy IPv4-only hosts.

RFC 4779 [Asadullah et al, 2007] analyses IPv6 deployment strategies in Service Provider Broadband networks in co-existence with deployed IPv4 services.

RFC 5963 [Gagliano, 2010] provides guidance on the deployment of IPv6 in Internet Exchange Points (IXPs).

RFC 5181 [Shin et al, 2008] analyses IPv6 deployment and integration methods and scenarios in IEEE 802.16 [IEEE, 2004] wireless broadband access networks.