IPV6 and Deep Packet Inspection

Parvathaneni.Tejaswini, K.V.S.Mounika, A.Rama Krishna

Abstract – The current version of the internet, IPV4 was depleted of addresses on february3, 2011. The storage of address has led to the introduction of IPV6 which has 128-bit (16-byte) source and destination IP addresses. Many organisations do not see a reason to convert to IPV6, and believe they are not running IPV6.Whether an organisation knows it or not, any laptop/PC running Vista or Windows 7 is a vulnerability from which attacks can come that will be invisible to IPV4 networks.

Since the Internet today uses IPV4 for 99% of the traffic, it will be slow migrations to IPV6.Three transition strategies are being employed: header translation, dual stack and tunnelling of IPV6 inside IPV4.Tunneling is the most precarious method for today's IPV4 networks. The IPV6 packet is included inside the message field of an IPV4 packet. The content of the IPV6 packet will not be noticed by an IP4 firewall or intrusion detection system. Hidden IPv6 traffic running across an organisation's network can wreak havoc, allow malware to enter the network, and be the basis for a denial of service attack. The only defence against such attacks is deep packet inspection (DPI).

The widespread use of DPI is inevitable. The first serious security breach caused by tunnelled IPV6 inside an IPV4 packet is certain to come in the near future. This event will be a stimulus to organisation to defend against such attacks.

Keywords: Cyber terrorism, Deep packet inspection, IPv4, IPv6, Security.

I. INTRODUCTION

The Impending World Of Ipv6

A. Additional Addresses

The current version of the Internet, IPV4, was depleted of addresses on February 3, 2011.The shortage of addresses has led to the introduction of IPV6 which has 128-bit (16-byte) source and destination IP addresses. This address space is: 2^{128} or about $3.4x10^{38}$ (340 trillion trillion trillion).

IPV6 will create an era of "throw-away" IP addresses. Every light bulb, door lock, package of lunch meat, quart of milk, jar of mustard could be given an IPV6 address and an RFI chip that communicates the status. The lunch meat could indicate it is going stale, the mustard jar could transmit that it is past the recommended use period, the battery in our flashlight could send a "replace me" message to an RFID reader, the light bulb could indicate it is near end of life, the fire detector could transmit "my battery needs to be replace," etc.

With every new technology, there are new security threats and vulnerabilities. Inequality of ipv4 distribution of addresses has caused other countries to embrace IPV6 before the United States. China is the world leader in IPV6 because of the need for more IP addresses, which cannot be supplied by

IPV4, the current version of the Internet. The implications of the USA being behind in this field are ominous for security of organisations.

B. IPV4 & IPV6 will coexist for a Long Time

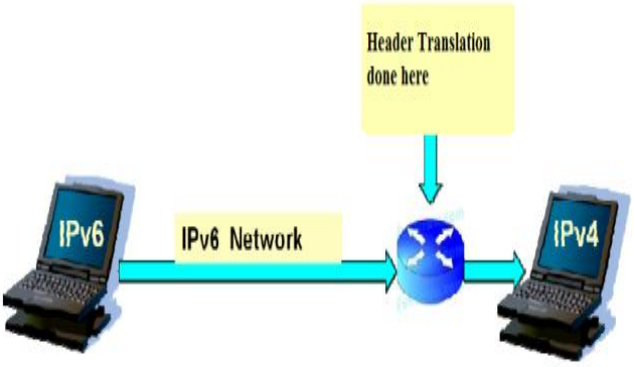
Since the Internet today uses IPv4 for 99% of the traffic, it will be a slow migration to IPV6. Many organisations do not see a reason to convert to IPV6, and believe they are not running IPV6. However, Microsoft Vista and Windows 7 have IPv6 compatibility enabled as the default setting. Whether an organisation knows it or not, any laptop running Vista or Windows 7 is a vulnerability from which attacks can come that will be invisible to IPV4 networks.

II. MIGRATION STRATEGIES FROM IPv4 TO IPv6

There are three techniques being used in the transition period from IPv4 to IPv6. Each of these techniques is shown below

A .Header Translation

Header translation can be used when sending IPv6 traffic to an IPv4 network as the end destination. This transition strategy is not likely to become a preferred transition method, because the advantages of both protocols can be lost.



B. Dual stack implementation

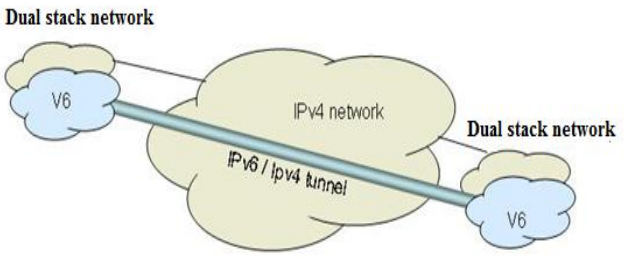
Dual stack can be used when a network handles both kinds of traffic. Although dual stack is the transition method most likely to be widely deployed, it essentially doubles the network security problem. Dual stack is expected to be the preferred method of transitioning to IPv6.

Manuscript Received on November, 2012

Parvathaneni.Tejaswini, Electronics and Computer Engineering, KL University, Guntur, Krishna District, Andhra Pradesh, India.

K.V.S.Mounika, Electronics and Computer Engineering, KL University, Guntur, Krishna District, Andhra Pradesh, India.

A. Rama Krishna, , Electronics and Computer Engineering, KL University, Guntur, Krishna District, Andhra Pradesh, India.



A dual-stack network is as secure as its weakest protocol family. This is called fate-sharing; for example, if the IPv6 access is not protected while the IPv4 is controlled, then malicious user will use IPv6 for the attacks. It is really important to have congruent security policies for IPv4 and IPv6. Dual-stack (or "native dual-stack") refers to side –by-side implementation of IPv4 and IPv6. That is, both protocols run on the same network infrastructure, and there's no need to encapsulate IPv6 inside Ipv4 (using tunnelling) or vice-versa.

Dual stack is defined in RFC 4213. Although this is the most desired IPv6 implementation, as it avoids the complexities and pit falls of tunnelling, it is not always possible, since outdates network equipment may not support Ipv6.A good example is cable TV based internet access. In modern cable TV networks, the core of the HFC network is likely to support IPv6. However, other network equipment or customer equipment may require software updates or hardware upgrades to support IPv6.

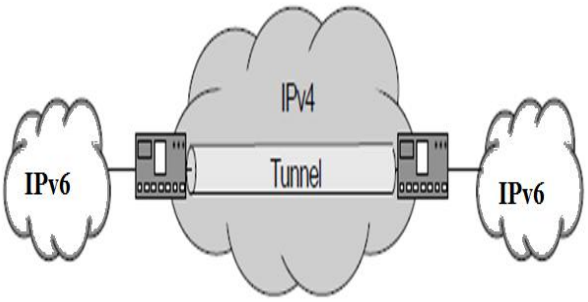
C. Tunnelling

Tunnelling is the most precarious method for today's IPv4 networks. The IPv6 packet is inside the message field of an IPv4 packet. The contents of the IPv6 packet will not be noticed by an IPv4 firewall or intrusion detection system. Cyber terrorists can use this vulnerability to deliver malware, penetrate database, plant bots, etc.

The tunnels are used like a mechanism to transport IPv6 packets through IPv4 networks. The way to this is an encapsulating the IPv6 diagram in a IPv4 packet, so that the final packet can be handled by the routers of the IPv4 network without problems. Because not all networks support dual-stack, tunnelling is used for Pv4 networks to talk IPv6 networks (and vice-versa). Many current internet users do not have IPv6 dual-stack support, and thus cannot reach IPv6 sites directly. Instead they must use IPv4 infrastructure to carry IPv6 packets. This is done using a technique known as tunnelling, which encapsulates IPv6 packets within IPv4, in effect using IPv4 as a link layer for IPv6.

Because not all network support dual stack, tunnelling is used for IPv4 networks to talk to IPv6 networks. Many current internet users do not have IPv6 dual-stack support, and thus cannot reach IPv6 sites directly. Instead, they must use Ipv4 infrastructure to carry IPv6 packets. This is done using a technique known as tunnelling, which encapsulates IPv6 packets within Ipv4 packets which encapsulate Ipv6 datagram. Some routers or network address translation devices may block protocol 41. To pass through these devices, you might use UDP packets to encapsulate IPv6 datagram's. Other encapsulation schemes, such as AYIYA or Generic Routing Encapsulation, are also popular.

Conversely, on IPv6-Only internet links, when access to IPv4 network facilities is needed, tunnelling of IPv4 over IPv6 protocol occurs, using the IPv6 as a Link layer for IPv4.



D. Automatic Tunnelling

Automatic tunnelling refers to a technique where the routing infrastructure automatically determines the tunnel endpoints. 6 to 4 is recommended by RFC 3056. It uses protocol 41 encapsulation. Tunnel endpoints are determined by using a well-known IPv4 any-cast address on the remote side and embedding IPv4 address information within IPv6 addresses on the local side. 6to4 is the most common tunnel protocol currently deployed.

Teredo is an automatic tunnelling technique that uses UDP encapsulation and can allegedly cross multiple NAT boxes. IPv6, including 6to4 and Teredo tunnelling, are enabled by default in Windows Vista and Windows 7. Most UNIX systems implement only 6to4, but Teredo can be provided by third-party software such as Miredo. ISATAP treats the IPv4 network as a virtual Ipv6 local link, with mappings from each Ipv4 address to a link-local IPv6 address. Unlike 6to4 and Teredo, which are inter-site tunnelling mechanisms, ISATAP is an intra-site mechanism, meaning that it is designed to provide IPv6 connectivity between nodes within a single organisation.

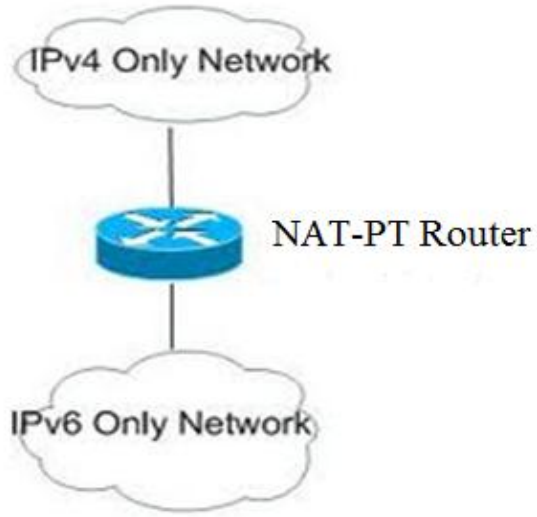
E. Configured and Automated tunnelling (6in4)

In configured tunnelling, the tunnel end points are explicitly configured, either by an administrator manually or the operating system's configuration mechanisms or by an automatic service known as a tunnel brokers this is also referred to as automated tunnelling. Configured tunnelling is usually more deterministic and easier to debug than automatic tunnelling, and is therefore recommended for large, well-administered networks. Automated tunnelling provides a compromise between the ease of use of automatic tunnelling and the deterministic behaviour of configured tunnelling.

Raw encapsulation of IPv6 packets using IPv4 protocol number 41 is recommended for configured tunnelling: this is sometimes known as 6 in 4 tunnelling. As with automatic tunnelling, encapsulation with in UDP may be used in order to cross NAT boxes and firewalls.

F. Translation NAT/PT

This technique allows the communication between only-IPv6 and only-IPv4 systems, and it consists in translating the headers of the packets (only the common fields) of IPv6 and Ipv4.



This translation of addresses made by NAT/PT has the same problem of the "regular" NAT, as the process in the same:

- Bottle neck, unique failure point.
- Viability and scalability.
- Limitation of the usable applications, as the E2E communication is not possible when using NAT.

Because of all this problems, NAT/PT is not so popular within the internet.

III. THREAT OF IPV6

Tunnelling of IPv6 inside an IPv4 packet will be invisible to an organisation using only IPv4. Hidden Ipv6 traffic running across an organisation's network can wreak havoc, allow malware to enter the network, and be the basis for a denial of service attack.

IV. ACTIONS TO REDUCE THE THREAT OF INVISIBLE IPV6 TRAFFIC

A. Upgrade today to Ipv6

This is costly, but effective solution, but the best of the choices. Very few organisations, however, have chosen this path because of the financial implications of upgrading their entire network in a short period o time.

B. Block all IPv6 Traffic

This solution is only temporary and difficult to administer. Furthermore, it is ineffective against tunnelled IPv6 traffic, unless a technique known as Deep Packet Inspection (DPI) is employed.

V. DEEP PACKET INSPECTION

Internet communications employ packets with headers containing routing information, including source and destination addresses. Historically, only the leader was examined by network routers. This is inadequate for the detection of tunnelled IPv6 inside an IPv4 packet. Since we are in a world dominated by IPv4, the only way to detect tunnelled IPv6 is to use Deep Packet Inspection.

Deep packet inspection (DPI) also called complete packet inspection and information extraction, is a form of computer network packet filtering that examines the data part of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, instructions, or defined criteria to decide whether the packet may pass or if it needs to be routed to different destination, or, for the purpose of collecting statistical information. There are multiple headers for IP packets; network equipment only needs to use the first of these (the IP header) for normal operation, but use of the second header (TCP,UDP etc.) is normally considered to be shallow packet inspection(usually called Stateful Packet Inspection).

Deep Packet Inspection enables advanced network management, user service, and security functions as well as internet data mining and internet censorship. Although DPI technology has been used for Internet management for many years, some advocates of net neutrality fear that the echnology may be used anti competitively or to reduce the openness of the Internet.

Deep Packet Inspection operates at all layers of a network above the physical layer. Each packet is examined for the information in the entire packet, not just the headers. DPI places a processing burden on the device performing this task, and can be a source of latency in a network. In a ideal world, processing speed requirements of DPI would be met by increases in device technology in accordance with Moore's Law. The current situation is that delays in networks are mostly caused by processing delays.

VI. LEGAL, SOCIAL AND SECURITY IMPLICATIONS

It is inevitable that DPI will be widely employed out of necessity since organisations cannot switch overnight to IPv6. Another aspect is that DPI is a rich source of information for intelligence agencies and government surveillance. DPI is opposed by advocates of network neutrality and the ACLU.

In addition to using DPI to secure their internal networks, Internet service providers also apply this technology on the public networks provided to customers. Common uses of DPI by ISP's are lawful intercept, policy definition and enforcement, targeted advertising, quality of service, offering tiered services.

Service providers are required by almost all government worldwide to enable lawful intercept capabilities. Decades ago in a legacy telephone environment, this was met by creating a traffic access point (TAP) using an intercepting proxy server that connects to the government's surveillance equipment. This is not possible in contemporary digital networks. The acquisition component of this functionality may be provided in many ways, including DPI, DPI-enabled products that can be used-when directed by a court order- to access a user's data stream.

An issue that must be resolved by a security policy for an organisation is encryption. Headers are never encrypted since they need to be read for routing purposes. Messages, however, can be encrypted. Government surveillance is not possible with encrypted traffic. RIM capitulated under pressure

by the Saudis and agrees to place a server in Saudi Arabia, thereby providing the means for government surveillance of Blackberry traffic. Skype also uses encryption; do not look for widespread acceptance of Skype in countries using total surveillance of citizens' electronic communications.

The access control policies for an organisation should be determined by the message content that is found by DPL. Presumably, unencrypted messages of tunnelled IPv6 inside an IPv4 would be easy to decide whether to forward to the addressee. If the message is encrypted, a policy must be established. The simplest solution is to block all tunnelled traffic that has the message encrypted. This policy may have secondary negative effects on an organisation's ability to communicate. To enter the enterprise, a greater risk in taken, since inside the organisation is an individual who may be trying to avoid the internal security policies.

VII. DPI POLICY DEFINITION AND ENFORCEMENT

Service providers obligated by the service-level agreement with their customers to provide a certain level of service and at the same time, enforce an acceptable use policy, may make use of DPI to implement certain policies that cover copyright infringements, illegal materials, and unfair use of bandwidth. In some countries the ISPs are required to perform filtering, depending on the country's laws. DPI allows service providers to "readily known the packets of information you are receiving online-from e-mail, to websites, to sharing of music, video and software downloads". Policies can be defined that allow or disallow connection to or from an IP address, certain protocols, or even heuristics that identify a certain application or behaviour.

A. Quality of Service

Applications such as peer to peer (P2P) traffic present increasing problems for broadband service providers. Typically, P2P traffic is used by applications that do file sharing. These may be any kind of files. Due to the frequently large size of media files being allowed.

P2P drives increasing traffic loads, requiring additional network capacity. Service providers say a minority of users generate large quantities of P2P traffic and degrade performance for the majority of broadband subscribers using applications such as e-mail or Web browsing which use less bandwidth. Poor network performance increases customer dissatisfaction to a decline in service revenues.

DPI allows the operators to oversell their available bandwidth while ensuring equitable bandwidth distribution to all users by preventing network congestion. Additionally, a higher priority can be allocated to a VoIP or video conferencing call which requires low latency versus web browsing which does not. This is the approach that service providers use to dynamically allocate bandwidth according to traffic that is passing through their networks

Mobile and broadband service providers use DPI as a means to implement tiered service plans, to differentiate walled garden services from value added, all-you-can-eat and one-size-fits-all data services. By being able to charge for a walled garden, per application, per application, per service, or all-you-can-eat rather than a one-size-fits-all package, the operator can tailor his offering to the individual subscriber and increases their Average Revenue per User (ARPU). A policy is created per user or user group, and the DPI system in turn enforces that policy, allowing the user access to different services and applications.

B. Targeted Advertising

Because ISPs route the traffic of all of their customers, they are able to monitor web-browsing habits in a very detailed way allowing them to gain information about their customers' interests, which can be used by companies specializing in targets advertising. At least 100,000 United States customers are tracked in this way, and as many of 10% of U.S. customers have been tracked in this way.

VIII. CONCLUSION

The transmission period between IPv4 and IPv6 is full of future unknowns. Unanticipated security vulnerabilities ate certain. Legal issues on the rights to privacy, surveillance, and Internet neutrality will all come into play. It will be an interesting next stage in the growth of the Internet. The threats caused by the advent of IPv6 must not be ignored by an organization. It is imperative to begin guarding against a major catastrophe caused by in attenuation to be forthcoming world of IPv6.

IPv6 is mostly IPv4 with larger addresses and there is no significant difference between IPv4 and IPv6 with respect to security. In some cases (link-local addresses) IPv6 is slightly more secure, and in other cases difficulties to phrase the extension headers. IPv6 is slightly less secure. Some IPv6 security myths simply do not stand. Security techniques and devices do exist to enforce a security policy for the IPv6 traffic and should be used.

REFERENCES

1. http://isoc.org/wp/worldipv6day
2. http://www.aclu.org/net-neitrality
3. S. Bradner and A. Mankin, "The Recommendations for the Next Generation IP Protocol", RFC 1752, Jan.1995.
4. C.Caicedo, J.Joshi, and S.Tuladhar, "IPv6 Security Challenges", Computer, IEEE Computer Society, February 2009
5. BihrouzanA. Forouzan,"TCP/I P protocol suite", 4th Edition, McGraw Hill.

AUTHOR PROFILE

Parvathaneni.Tejaswini was born in 1992 at Krishna District, Andhra Pradesh. She is pursuing her B.Tech in Koneru Lakshmaiah University. Her interested areas are Networking, Data Communications and Wireless Communications.

K.V.S.Mounika was born in 1992 at Kadapah District, Andhra Pradesh. She is pursuing her B.Tech in Koneru Lakshmaih University. Her interested areas are Networking and Data Communications.

A. Rama Krishna was born in 1987 at West Godavari District, Andhra Pradesh. He is working as a Assistant Professor, Dept.of ECM, K.L.University, Vaddeswaram, A.P, India.