Vulnerabilities in IPv6

INTRODUCTION

Ipv6 (Internet Protocol version 6) is a network layer that is utilized by packet-switched internet worked applications. The protocol is the successor to IPv4 and is used for Internet based general applications. According to many reports, IPv6 has much vulnerability that allows hackers and malware to use of the “holes” and compromise networks and systems.[1] This paper discusses various vulnerabilities of IPv6 and also presents the differences from IPv4.

SUMMARY AND KEY FINDINGS

The following are the summary of key findings.

1. There are some differences in the native security features of IPv4 and IPv6 that has lead to IPv6 being called as a vulnerable protocol. While these differences were designed to make IPv6 more efficient, they have created vulnerabilities. Some of them are Provision of Bigger address space, New Header Format, Stateless auto configuration of address, Downward Compatibility of IPv6 with Pv4 and absence of Checksum error validation. These features have lead to enhanced vulnerabilities in IPvPotential weaknesses and vulnerabilities in IPv6 that hackers could exploit are: Tunneling using IPv6, Inconsistent IPv6 Support, allowing reconnaissance activity and allowing malware that allows IPv6 on Compromised Hosts.[2]

2. Kinds of malware that will be most effective on IPv6 networks include: worms that random IP address space probing, malicious code that uses uniformly

---

[1] “IPv6: The New Internet Age.” *R&D.* Web. 2005. 10-11.

[2] Ibid. 10-11.

distributed random number generator and biasing the search space, Worms that seek network information from information sources such as mirroring the IPv6 address architecture, IPv6, Neighbor Discovery logs, Routing protocols and tables, that peer-to-peer networks, malicious codes and viruses that participate in maintenance topology and listen to requests and responses to gather information about vulnerabilities.[3]

3. Other of malware that can make use of the Ipv6 vulnerability include Reconnaissance, Unauthorized access, Header manipulation and fragmentation, Layer 3 and 4 spoofing, Address Resolution Protocol (and Dynamic Host Configuration Protocol attacks, Broadcast amplification attacks or smurf, Routing attacks, Viruses and worms, Transition, translation, and tunneling mechanisms and many others such as Sniffing, Application Layer Attacks, Rogue Devices, Man-in-the-Middle Attacks, Flooding, etc.[4]

4. More than 100 countries across the world have made it mandatory of systems to be compliant with Ipv6. Many ISPs, governments and research labs have been set up in the US and other countries for IPv6 research and implementation. Japan, China, Korea and Taiwan are at the forefront in the implementation while some countries in Europe still have to take up the implementation.[5]

---

[3] "IPv6 Accessible Sites: List of Countries and Sites that Develop". *IPv6.* 13 June 2008 <http://www.ipv6.org/v6-www.html>.

[4] Ibid.

[5] "EC IST Project. Legal Aspects of the New Internet Protocol". *The IPv6 Portal*. 13 June 2008 <http://www.ipv6tf.org/pdf/ipv6legalaspects.pdf>. 58-68.

ANSWERS TO RESEARCH QUESTIONS

This section provides answers to some key questions on Ipv6 vulnerabilities.

Q1. What Are the Major Differences in "Native" Security Features between IPv4 and IPv6?

Bigger Address Apace. It must be noted that addresses in IPv6 are of 128 bit while in IPv4 it was 32. With a longer address space, the need for NAT address for configuring the MAC addresses are done away with as was the case with IPv4 and in effect the system becomes much simpler since there is no sub netting required. But this larger space address allows malware to hack into the system or point to dangerous URLs that compromise the network 1.[6]

New Header Format. In the IPv6 protocol, the optional and fields that are not required in the header have been placed in the extension header regions that occur after the IPv6 header and this has reduced the load on the header and allows URLs to be accessed faster. This allows about four times more information to be packed into the header and makes searches on Google with keywords much faster and easier. But the problem is that with proper malware coding, expert hackers can write a malware code in the header and allows dangerous scripts to be downloaded when dangerous websites or mails are opened. Following is an example of an alert that is given by an antivirus package when it detected such malware in the header. If user clicks the “click here” link, then the script would be launched and the computer would be compromised 2.[7]

---

[6] “What is IPv6.” *MSTechNet.* 13 June 2006 <http://technet2.microsoft.com/windowsserver/en/library/b2c271bf-abd1-4218-87a9-176dcdd83b1b1033.mspx?mfr=true>.

[7] “EC IST Project. Legal Aspects of the New Internet Protocol”. *The IPv6 Portal*. 13 June 2008 <http://www.ipv6tf.org/pdf/ipv6legalaspects.pdf>. 51-55.

Stateless Auto Configuration of Address. Hosts running IPv6 can be automatically configured into a IPv6 routed network that have the ICMPv6 router. During the initiation of the connection, the host transmits a link-local multicast router connection request. Some networks allow the routers to respond automatically and send a router advertisement packet with parameters for network-layer configuration. This is a good advancement but hackers can ride piggyback on such requests to gain information of the SOCKS layer. Ipv4 on the other hand would require manual configuration and this is not possible anymore in today's Internet. IPv6 is also called as universal plug and play and this feature would allow any genuine request to be given connection. But such gullibility allows hackers to gain entry into networks. Certain types of virus and Trojans are designed specifically for this protocol.[8]

Downward Compatibility. Ipv6 has to be downward compatible to allow legacy applications to be connected. In some cases, users may be asked to download a patch to allow the update to be installed. This is a very critical area and hackers can impersonate genuine security certificates and get unwary users to download auto dialers and Trojans that would run in the background and launch attacks from the host

---

8 "What is IPv6." *MSTechNet.* 13 June 2006 <http://technet2.microsoft.com/windowsserver/en/library/b2c271bf-abd1-4218-87a9-176dcdd83b1b1033.mspx?mfr=true>.

computer, to the network and even the net. This is not the fault of Ipv6 but this fact does play an important role. [9]

Checksum. IPv4 utilizes a checksum field verifies the full packet header. Some fields like the TTL field would essentially change while being forwarding and the router recomputed the checksum and while this process is slower, it is very secure. IPv6 has done away with checking for error at the network layer and uses the transport protocols and the link layer to carryout the error checking. The IPv6 process is much faster but inherently it has done away with an integral and simple part of the security and this feature allows networks to be compromised.[10]

Q2. What Are Some Potential Weaknesses and Vulnerabilities in IPv6 that Hackers Exploit?

IPv6 was created to solve the problems of address space restrictions of IPv4 and also to extend more security and routing capabilities. But IPv6 can be compromised and made to deliver malware by avoiding detection by Intrusion Detection Systems and firewalls that may not have been set up to recognize IPv6 traffic. In some cases, malware is utilized to reconfigure vulnerable hosts to allow IPv6 traffic. Compromise of IPv6 to deliver malware can be done by malicious application of traffic tunneling, incomplete or inconsistent support for IPv6, IPv6 auto-configuration capability, malware designed to enable IPv6 support on susceptible hosts Tunneling and others.[11]

---

[9] Bellovin, Steven M., Cheswick Bill. “Worm Propagation Strategies in an IPv6 Internet. Login Journal.” *New Security Paradigms Workshop*. Vol. 31: (1). New York: ACM, 2006. 70-77.

[10] Ibid. 70-77.

[11] Ibid. 70-77.

Tunneling Using IPv6. Tunneling is used for internet data transmission where the public internet is utilized to relay private network data. This is done by encapsulating the network data of private networks and protocol information within the public network packets. By using this method, information from private network protocol is processed in a normal manner by the public network and the data encapsulation that is used in along with encryption and authentication, gives a genuine advantage to users who want an efficient way to connect private networks. But IPv6 can be misused for encapsulating malware and relay it by taking advantage of auto configuration feature and any pre-existing network conditions. So, in effect, malware gets easy access to the network.[12]

Inconsistent IPv6 Support. When the IPv6 support is incomplete, malware tunneling is promoted by the new protocol. Though many operating systems are now given updates and patches to support IPv6, there are some monitoring and filtering applications that do not support IPv6 across all ports and subnet masks. In some cases, firewall and intrusion detection systems do not recognize potential malware and may allow the dangerous script to enter the network. Some types of small firewalls that are typically installed in homes display a prompt that may ask for permission to allow a certain application to connect. An unwary user may click 'yes, always allow' prompt and this gives the malware freedom to launch any type of attack, send a receive information, launch DoS attacks, send Spam mail using the users mail box and the email addresses and so on.[13]

---

[12] Kamra, Abhinav et al. "*The Effect of DNS Delays on Worm Propagation in an IPv6 Internet*." Vol. 4. New York: Columbia University, 2005. Print. 13-14.

[13] Ibid. 13-14.

Reconnaissance Activity. provides with increased security. So along with malware tunneling where the malware actually enters a network, reconnaissance activity that includes port scanning and sniffing, botnet activity for outbound communication traffic and other such problems can occur. Users who suspect that their system is infected may have to format their hard disks as anti virus applications may not be able to remove the malware. In extreme cases, the malware can even format the hard disk and at the least, it can send credit card information to a remote hacker.[14]

Malware that Allows IPv6 on Compromised Hosts. In some cases, malicious code allows IPv6 on a compromised host. This situation creates an unobserved channel that a hacker can use to launch attacks. There are many tools that can be used to launch IPv6 on a compromised host and some of them are 6tunnel, nt6tun and others. These tools are actually legitimate applications that were designed to allow easier communication by allowing IPv6 to downward integrate with IPv4, but these tools are misused to launch malicious attacks. It was feared that Ipv4 would soon run out of capacity to accommodate additional addresses, much like the Y2K problem since it had only a 32 bit encryption. By allowing downward compatibility, it was felt that the best use can be made of existing Ipv4 addresses, but unfortunately hackers have made use of this feature for malicious purpose.[15]

---

[14] Ibid. 13-14.

[15] Bellovin, Steven M., Cheswick Bill. “Worm Propagation Strategies in an IPv6 Internet. Login Journal.” *New Security Pardigms Workshop*. Vol. 31: (1). New York: ACM, 2006. 70-77.

Q3. What Kinds of Malware Do Security Experts Expect Will Be Most Effective on IPv6 Networks?

According to Zou,[16] there have been thousands of worms, Trojans and viruses that launch attack on networks and computers and the authors' point that with IPv6, there would be more exploits from hackers. One method that worms employee to find suitable vulnerable targets is by using random IP address space probing. IPv4 with smaller 32 bit address space allowed this easily since bots would run scans on such addresses. But with the 128 but address of IPv6, this problem should have become more difficult, time consuming and expensive since the address is about four times longer. But address space scanners such as CodeRed and Slammer use advanced heuristics scan to reduce the search space and also take up multi level searching and this has removed the advantage that IPv6 gave.

The authors predict that there would be two types of address space scans - uniformly distributed random number generator and biasing the search space. Worms also take advantage of local knowledge and patterns in address space assignment. The malware can reduce the search space by a large percentage. Other strategies used include wide area and local area search and this would be mirroring the IPv6 address architecture. Worms would access different types of information sources to find existing networks and embed themselves and then spread locally inside a network. Some sources of information that worms can use include IPv6, Neighbor Discovery that is utilized to map IP addresses to local network addresses such as Ethernet addresses

[16] Zou, Cliff C., Towsley Don. "Routing Worm: A Fast Selective Attack Worm Based on IP Address." *In Proceedings of the Workshop on Principles of Advanced and Distributed Simulation (PADS).* Amherst: University Massachusetts. June 2005. 1-16.

and a worm that has infected even one node in a LAN can find the addresses of other nodes in the LAN. Routing protocols and tables are other sources of information for malware. Some networks use internal routing protocols like RIP and OSPF. In such cases, worm can directly consult the host routing tables by using the UNIX netstat command or act as a passive listener in a routing protocol and find other subnets in the network and launch attacks.

Martin[17] has pointed that peer-to-peer networks such as Kaaza, BitTorrent, Morpheus, Gnutella and other play host to a number of malware and worms. Malicious codes and viruses tend to participating in maintenance topology and listen to requests and responses to gather information about vulnerabilities. They also send queries and gather addresses from different hosts. In many cases, they are hidden in the header files of content such as songs and movies that are exchanged. Some worms also travel through protocols such as Jabber and IRC. The author points out that such types of malware would have a high rate of download.

Convery[18] has pointed out different types of malware that can make use of the Ipv6 vulnerability. Some of them include Reconnaissance, Unauthorized access, Header manipulation and fragmentation, Layer 3 and 4 spoofing, Address Resolution Protocol (and Dynamic Host Configuration Protocol attacks, Broadcast amplification attacks or smurf, Routing attacks, Viruses and worms, Transition, translation, and tunneling mechanisms and many others such as Sniffing, Application Layer Attacks,

---

17 Martin, David M, Rajagopalan Sivaramakrishnan. “Blocking Java Applets at the Firewall.” *In Proceedings of the Symposium on Network and Distributed System Security.* Web. Feb. 2006. 1-10.

18 Convery, Sean, Miller Darrin. *IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation*. Cisco Publications, 2003. Print. 4-22.

Rogue Devices, Man-in-the-Middle Attacks, Flooding, etc. In reconnaissance, malware attempts to get information about the target network by using scanning and data mining through search engines or public documents.

In Unauthorized access the worm attempts to exploit the open transport policy in the protocol. Nothing in the IP protocol stack limits the set of hosts that can establish connectivity to another host on an IP network. Malware uses this feature to connect to upper-layer protocols and applications on internetworking devices and end hosts. In fragmentation and other header manipulation attacks the malware uses fragmentation to avoid network security devices, such as NIDS or stateful firewalls and also to attack the networking infrastructure directly.

ARP and DHCP attacks subvert the host initialization process or a device that a host accesses for transit and subversion of host bootstrap conversations happens through either rogue or compromised devices or spoofed communications. The worms tries to get end hosts to communicate with an unauthorized or compromised device or to be configured with incorrect network information such as default gateway, DNS server IP addresses. Broadcast amplification attacks or “smurf” attacks, are a DoS attack tool that takes advantage of the ability to send an echo-request message with a destination address of a subnet broadcast and a spoofed source address, using the victim’s IP. All end hosts on the subnet respond to the spoofed source address and flood the victim with echo-reply messages.

Q4. *Which Countries Have the Biggest IPv6 Pure Networks?*

As per the report released on the IPv6 Forum,[19] Japan Japan has taken up IPv6 implementation in a big way and the Japanese government has pushed forward various

[19] “IPv6: The New Internet Age.” *R&D.* Web. 2005. 10-11.

programs to push IPv6 implementation such as tax incentives for designing IPv6 applications. South Korea has also taken up the implementation and the ministry of communication has devised a new platform called IT839, selecting eight applications, three infrastructure and nine services. Because of the government support and early adoption by communication carriers, domestic equipment makers, large and small research organizations are increasing the development of equipment needed for deployment of the next generation Internet address systems.

China has instituted a full IPv6 adoption policy by creating the China Next Generation and budgeting more than 170 million USD for completion by 2006. A group called 6TNET has been formed along with Japan and Chinese leaders and they have launched the CNGI that will the largest commercial backbone built from scratch for a single technology and this would become the base for all services in China for fixed, mobile, GRID and research. Even Taiwan which serves as the hub of low cost networking devices has created a consortium of 10 vendors leading to the creation of the IPv6 steering committee to set up the IPv6 forum Taiwan.

The US department of Defense has announced that all equipment purchased after June 2003 should be IPv6 compatible and has published a roadmap to migrate their networks to IPv6. This move also encouraged the German and French ministries of Defense to take up the implementation. The European commission has funded a number of projects for IPv6 implementation. The French government set up the French IPv6 Task Force by using voluntary work and set up the IPv6 competency center in Brittany and a regional IPv6 Task Force.

The author says that the rest of Europe is lagging in the implementation since the industry is not participating in a big way and only 4 of 120 products are IPv6 compliant.

Only a few European ISP providers have realized the geopolitical impact and France Telecom is the only large European ISP that has won large projects for IPv6. Japan has 17 large ISP while Korea has 4 big and 70 small and medium ISP and these have implemented IPv6.

According to the IPv6 website, more than a 100 countries across the world have made it mandatory of systems to be compliant with Ipv6. Since Ipv4 has not been phased out in some areas, Ipv6 has been allowed the downward compatibility feature. Some of the countries including United States, UK, and some countries in Europe, African countries such as Nigeria, Australia, India and many others. The report says, “The European Commission has set a target of getting at least a quarter of EU industry, public authorities and households to switch to IPv6 internet addressing by 2010. A recent report from the OECD had warned that the shortage of older IPv4 internet addressing threatened the rise of mobile internet services. In the short term, businesses and public authorities might be tempted to try to squeeze their needs into the strait jacket of the old system, but this would mean Europe is badly placed to take advantage of the latest internet technology, and could face a crisis when the old system runs out of addresses. Twenty-five per cent of all European users should have the opportunity to use IPv6 by the end of 2010, and should be able to access most of their normal services and content with it. The EU Commission will set this goal in a statement, to be published at the end of May, on the new internet protocol and progress in the net. Detlef Eckert of the General Directorate for Information Society and Media presented the key points of the statement and a related action plan at the RIPE meeting in Berlin. The Commission is joining organizations like the Réseaux IP Européens Network Coordination Centre (RIPE) in calling for rapid action in the face of dwindling reserves of

IP addresses. Businesses alone are not doing enough to avert an impending shortage of Internet Protocol addresses, and governments must work with them to secure the future of the Internet economy, according to a report published Thursday by the Organization for Economic Cooperation and Development. The number of IP addresses, needed for Web sites, servers and PCs to communicate with one another over the Internet, is limited, and almost 85 percent of addresses are now in use. At the current rate of growth, the pool of available addresses will be exhausted by 2011."[20]

Q5. What Are the Major Centers for IPv6 Research and Development Outside the U.S.?

Transition to IPv6 has become imperative for many countries, as the fear of running out of addresses is very real. Many countries have given a deadline for compliance to the new protocol. Other than US, there are development centers in Microsoft development centers in India, UK, Japan and other countries. In countries such as India, labs have been in colleges such as BITS Pilani, IITs and other famous colleges. Governments of many countries have set up task forces for development and implementation of IPv6 protocols. It must be noted that in many countries, ISP providers have their own centers for the implementation and development of IPv6. Large organizations and software developers need to make their applications compatible before the software can be sold and this is one area that sees great activity as new threats and vulnerabilities are discovered.[21]

---

[20] "EC IST Project. Legal Aspects of the New Internet Protocol". *The IPv6 Portal.* 13 June 2008 <http://www.ipv6tf.org/pdf/ipv6legalaspects.pdf>.

[21] Ibid.

Gaps and Suggestions for Further Research

The paper has examined a number of issues related to vulnerabilities of IPv6, types of malwares that can attack and the method in which the malicious code launches an attack. There is some gap in the paper as types of vulnerabilities and types of attacks have been discussed, what remains is plugging the vulnerability and identifying ways in which networks can be made to resist attack. This is an important aspect that has to be researched further as it will help administrators to fight malware attacks, protect assets and ensure that their systems are not compromised. A further addition to future research will be to examine the IPv6 protocol in detail and along with a listing of different attacks, methods, procedures and applications to stop attacks from being launched should be examined. There are also a number of tools, updates and patches that can be downloaded free to plug the vulnerability. Efforts should be made to document such wares and procedures to install them should be provided.

Works Cited

Bellovin, Steven M., and Bill Cheswick. “Worm Propagation Strategies in an IPv6 Internet. Login Journal.” *New Security Pardigms Workshop* 31.1 (2006): 70-77.

Convery, Sean, and Darrin Miller. *IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation.* Cisco Publications, 2003. Print.

“EC IST Project. Legal Aspects of the New Internet Protocol”. *The IPv6 Portal*. 13 June 2008 <http://www.ipv6tf.org/pdf/ipv6legalaspects.pdf>.

“IPv6 Accessible Sites: List of Countries and Sites that Develop”. *IPv6*. 13 June 2008 <http://www.ipv6.org/v6-www.html>.

“IPv6: The New Internet Age.” *R&D.* Web. 2005. 10-11.

Kamra, Abhinav et al. “The Effect of DNS Delays on Worm Propagation in an IPv6 Internet.” *INFOCOM.* Vol. 4. New York: Columbia University, 2005. Print.

Martin, David M, and Rajagopalan Sivaramakrishnan. “Blocking Java Applets at the Firewall.” *In Proceedings of the Symposium on Network and Distributed System Security.* Web. Feb. 2006.

“What is IPv6.” *MSTechNet.* 13 June 2006 <http://technet2.microsoft.com/windowsserver/en/library/b2c271bf-abd1-4218-87a9-176dcdd83b1b1033.mspx?mfr=true>.

Zou, Cliff C., and Don Towsley. “Routing Worm: A Fast Selective Attack Worm Based on IP Address.” *In Proceedings of the Workshop on Principles of Advanced and Distributed Simulation (PADS)*. Amherst: University Massachusetts. June 2005.