Asian Journal of Information Technology 4 (9): 885-887, 2005

The Security Considerations During the Transition from IPv 4 to IPv 6

Syed Muhammad Faheem and M. Nawaz Brohi
Department of Information Technology, Preston University, Ajman Campus, UAE

Abstract: IPv 4 is playing its role with dominancy around the globe connecting hundreds of thousands nodes together. The depletion of address ranges as per the requirement growth led the development of newer version of IP by the Internet Engineering Task Force (IETF). Following several proposals a new version of IP was materialized and officially declared as IPv 6. This protocol uses 128-bit address instead of its predecessor's 32-bit scheme. It has various new features and strong security options. This study discusses the main features and security risks involved during the transition period from IPv 4 to IPv 6, which would be the dominant protocol of the future web.

Key words: 6To4DDos, IPSec, IPv6, MIPv6, security risks, transition

INTRODUCTION

Networks are ubiquitous, via satellite and undersea optical fiber cables, covering almost the whole world. Similarly the necessity to communicate has reached up to a level where even a PDA is required to connect to some network for instant access to the information. Internet Homes[Cisco-iHOME] is another example to exhibit the modern use of networking and bringing its benefits to the ordinary home users. Since its birth Internet Protocol has seen many phases, starting from DARPA's initial deployment to connect its sites, to today's converged networks, which could take voice, video and data altogether.

Internet engineering task force has been working on the development of IPv 6[1,2] to replace the current IPv 4[3] protocol. IPv 6 is the next generation Internet Protocol and it is the latest rendition of IP. IPv 4 has beaconed its exhaustion quite earlier than expected and consequently forced the designers to design another protocol, which finally took the name: IPv 6. IPv 6 has three added advantages over its predecessor, which are Larger Address Space, Inherent Security and Mobility, which help networks to converge very well. Currently in transitional state, IPv 6 is expected to take over IPv 4 Internet in very near future, although there is no fixed schedule for this takeover. Test beds, Pilot projects and new hardware support for this protocol by leading ISPs and companies are already in progress and results have shown significant benefits. Many of them are offering test connections either through configured tunnels or 6 to 4 relay mechanism under 6 Bone network 6 Bone.net[1]. Next generation networks, which inherently include voice video and data support altogether will finally find IPv 6 as its binding glue.

FEATURES OF IPV 6

The exhaustion of IPv 4 Addressing scheme became the primary reason and led the development of IPv 6, which quadrupled its addressing architecture from 32-bits to 128-bits. The basic architecture offers three main types namely Unicast, Anycast and Multicast[4].

IPv 6 is a modified version of IPv 4 in which the changes are made to Layer 3 (the network layer). Other layers are slightly modified. By using a big addressable space IPv 6 enables the use of a global and reachable system. Almost every kind of device will have its unique address. Many of the mobile phone companies are manufacturing IPv 6 enabled sets, which could allow users to connect to Internet from their phone sets[5].

A larger IPv 6 address space allows ISP and Organizations to be represented by one Prefix only. Moreover ISPs can summarize and advertise only one prefix for their entire range of customers. This idea was one of the most desirable tasks when IPv 6 was being created. Autoconfiguration is a new feature offered by IPv 6[6]. It allows end nodes on the local link to configure themselves to their address and default gateway. The re-numbering process will not prevent the loss of UDP / TCP session and is only possible in MobileIP.

Unlike in IPv 4 and ARP is not used in IPv 6. Multicast is the feature which replaced the ARP functionality and is used to address group of similar nodes to carry out the different functions.

Header fields are modified in IPv 6. Though the IPv 6 header is larger than IPv 4 but it is very simple and contains fewer fields. The fixed length of IPv 6 header means it's less costly to CPU to forward IP packets. All fields are adjusted to 64-bit, which means access to memory will be efficient for 64-bit access and storage.

Corresponding Author: Syed Muhammad Faheem, Department of Information Technology, Preston University, Ajman Campus, UAE

Flow label is a new field added to IPv 6 header[7]. This is meant for End-stations not the routers. It enables the special handling of packet for specific purpose. It offers more granular control over packet handling for QoS.

Mobile IPv 6 (MIPv 6)[8] specifies routing support to permit an IPv 6 host to continue using its permanent home address as it moves around the Internet. Mobile IPv 6 supports transparency above the IP layer, including maintenance of active TCP connections and UDP port bindings. Mobility is becoming inevitable for those who want to connect to the NET, most of the time. Services include are corporate networks, e-mails, e-banking, e-payments and very near to come the Internet enabled homes. Mobile phone companies have already begun to implement IP backbone in their core networks.

Security is one the essential features which is mandatory in IPv 6[9]. IPSec protocol implements security via creating tunnels over IP networks or simply by encrypting data. Two protocols work behind IPSec which are AH (Authentication Header No. 51) and ESP (Encapsulating Security Payload No. 50). The Authentication Header is used to provide connectionless integrity and data origin authentication for IP datagrams and to provide protection against replays. The IP Encapsulating Security Payload (ESP) seeks to provide confidentiality and integrity by encrypting data to be protected and placing the encrypted data in the data portion of the IP Encapsulating Security Payload. Depending on the user's security requirements, this mechanism may be used to encrypt either a transport-layer segment (e.g. TCP, UDP, ICMP and IGMP) or an entire IP datagram. Encapsulating the protected data is necessary to provide confidentiality for the entire original datagram.

There are many transition strategies available to offer integration and coexistence mechanisms from IPv 4 to IPv 6[10]. There is no deadline, as of Y 2K, for IPv 6 transition. The transition is designed in a way that not all IPv 4 nodes are required to be upgraded at the same time. The mechanism allows institutions to offer IPv 6 services over IPv 4 infrastructures. The following are the transition methods that can be applied as per the requirements[11].

- Dual IP layer: Provides complete support for both IPv 4 and IPv 6 in hosts and routers.
- IPv 6 over IPv 4 tunneling: Encapsulating IPv 6 packets within IPv 4 headers to carry them over IPv 4 routing infrastructures. Two types of tunneling are employed: Configured and Automatic.

SECURITY ISSUES

IPv 6 is not a foolproof system, which cannot be hacked. IPv 6 transitional mechanism may allow intruders to gain access to the system and which is not detected by the administrators until they fully switch to IPv 6 and know how to protect an IPv 6 network. Poorly protected sites are the first target to be hacked by IPv 6 enabled hacking tools, which are already in place. Internet hacking gentry maintains IPv 6 Sites indicating that they have gained access to IPv 6. They now offer tools and techniques to communicate to IPv 4 sites and redirecting these to IPv 6.[6To4DDos] is specifically designed to attack an IPv 6 sites and to attack IPv 4 sites by using 6to4 tunneling[12]. An IPv 6 based backdoor simply configures 6to4 on the compromised system and picks and SLA (Site Local Aggregation–the 16 bit IPv 6 subnet number) and a EUI (End User Identifier–the lower 64 bits of the IPv 6 6to4 address) and then listens on that specific backdoor address and port. This port does not show in IPv 4 security scanner.

The Inherent difficulties in scanning larger address space at the Site Level make the detection of stealth backdoors via scanning from external network almost impossible. A fusion of IPv 6 aware network scanning and IPv 6 aware IDs can alleviate this problem.

The same holds true for backdoor or Trojans that connect outwards from a compromised hosts. These attack tools do not hid server ports behind 6 to 4 stealth interfaces but instead hide traffic in SIT tunnels or in UDP-based IPv 6 tunnels. Compromised hosts may advertise IPv 6 routes and forward IPv 6 traffic back and forth thru themselves for an entire network behind firewalls and NAT devices.

Evidences are available for expected attacks done to or by IPv 6 system[13]. The Risks introduced primarily by IPv 6 transition mechanisms can be mitigated and controlled using exiting applications and techniques. Any network should provide controlled routing incase if both IPv 6 and IPv 4 are used, else incase of IPv 4 only network, restriction should be practiced by closing all unwanted ports and SIT/IPv6 tunnels. Administrators need to test and verify these settings often and on.

CONCLUSIONS

The Security risks are inherent and need lots of preparation for selecting the type of transition mechanism with the ISP support. Furthermore in an IPv 4 network the detection of native IPv 6 traffic is a clear indication of

malicious activity being taken place, Similarly if IPv 6 is not supported in a network, presence of SIT traffic would be unusual and should be blocked.

IPv 6 offers many advantages to those who knows and can best utilize them. Many network administrators are unaware of the fact that their network's perimeter security can't detect the malicious activity being injected by IPv 6 hacking community and is being passed through without their awareness. The time is now and we should gear up to develop firm understanding and its deployment with minimum of the security issues.

REFERENCES

1. http://www.6bone.net/ngtrans
2. Raicu, I., 2002. An empirical analysis of internet protocol version 6 (IPv 6) M.Sc. Thesis, Wayne State University.
3. Information Sciences Institute, 1981. University of Southern California, Internet Protocol, Request for comments 791, Internet Engineering Task Force.
4. RFC 3513: Internet Protocol Version 6 (IPv 6).
5. http://pcword.about.com/news/Nov162004id.
6. RFC 2462: IPv 6 Stateless Address Autoconfiguration.
7. RFC 3697: IPv 6 Flow Label Specification.
8. Zeadally, S. and N. Deepak Mavatoor, 2003. Mobile IPv 6 support for highly mobile hosts: Proceedings of IA STED International Conference on Communications Systems and Networks (CSN'03), Benalmadena, Spain.
9. Atkinson, R., 0000. Security Architecture for the Internet Protocol: RFC2401.
10. RFC 2893: Transition Mechanisms for IPv 6 Hosts and Routers.
11. Raicu, I. and S. Zeadally, 2003. Evaluating IPv 4 to IPv 6 transition mechanisms: Proceedings of 10th IEE/IEEE International Conference on Telecommunications (ICT-2003), Tahiti, Papeete, French Polynesia.
12. Warfiled and H. Michae, 0000. Security implications of IPv 6: Internet Security Systems. http://documents.iss.net/whitepapers/Ipv6.pdf
13. http://www.pkcrew.org/index.php.