International Journal of Advance Research in Science and Engineering
Vol. No.4, Issue 11, November 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

SECURITY VULNERABILITIES FOR THE FUTURE OF THE WEB IPV6 PROTOCOL SUITE

Biny Pal Singh Gill[1], Raman Solanki[2]

[1,2]IT, Guru Gobind Singh Indraprastha University, (India)

ABSTRACT

The concept of 'Web' has been possible because of interconnection of devices and these interconnections have been possible because of a network layer protocol- IPv4.Internet Protocol Version 4(IPv4)has been in existence for about 20 years and was responsible for revolutionizing the Internet. Lately, however the number of devices on the network has increased manifolds. IPv4 has not been able to cope up. It has been running out of addresses. Thus IPv6 has come into picture with an enormous address space, solving the address problem for many years in the future. IPv6 has become the future of the web. In fact with the idea of 'always connected' devices, millions of systems are connected to the web at the same time. Only a protocol like IPv6 can support such a huge number of devices. But IPv6 comes with its own set of security concerns. These are largely unexplored and therefore most of the network administrators are still wary of deploying IPv6 over their networks. This paper covers the vulnerabilities and security threats to IPv6 and their possible solutions.

Keywords: IPv4, IPv6, Vulnerabilities, Web Security.

I. INTRODUCTION

IPv6 was defined in RFC 2460 in mid-1990's. It was designed to be the next generation Internet Protocol address standard which would supplement and then finally replace the IPv4 protocol suite used in the Internet presently [1].

IPv6 gives huge scalability because it uses 128 bits for addressing[2]. This means we have 340 undecillion ($3.4X10^{38}$) addresses i.e. about 52 Trillion addresses per person if the population of the world is 6.5 billion [3] currently.

Not only does IPv6 provide a big range of addresses, it also gives high Quality of Service(QOS), end-to-end networking , high degree of mobile connectivity and many other benefits.

IPv6 Address

IPv6 Address is a 128 bit address consisting of 8 sections , each 2 bytes in length[4]. Example

FDDA: AB94:0064:3610:000F:CCFF:0000:FFFF

Is an IPv6 address. It can be abbreviated by dropping the leading 0's

FDDA: AB94:64:3610:F:CCFF:0:FFFF

Consecutive 0's can be replaced with a double semicolon.

FABC: 0:0:0:0: AABB: 0:FFFF

Can be abbreviated as

FAC::AABB:0:FFFF

Transitioning

IPv6 can work with IPv4 so that transitioning becomes smoother and the already existing IPv4 infrastructure can be used.

Three strategies are used for this transitioning[4]:

1. Dual Stack
2. Tunneling
3. Header Translation

Dual stack-For smooth from IPv4 to IPv6, everysystem supports both IPv4 and IPv6 protocol stacks, and according to the type of communication, uses the appropriate stack.

Tunneling- This is a situation where source anddestination support only IPv6 but the underlying network support IPv4. Then the IPv6 packet is encapsulated inside the IPv4 packet for transmission.

Header Translation- This is a situation where one hostis IPv6 and the other host is IPv4. So the header format of IPv6 has to be completely translated to IPv4 to be understood by the destination.

II. IPV6 ATTACKS

IPv6 was considered to be a very secure protocol because IPsec was mandatory in the original protocol. The Authentication Header provides data integrity and data authentication for the whole packet. The IPv6 Encapsulating Security Payload header provides confidentiality, authentication and data integrity to the encapsulated payload. The security features in IPv6 can be used to prevent various network attack methods including IP spoofing, some Denial of Service attacks (where IP Spoofing has been employed), data modification and sniffing activity. However, issues with the security features still exist, concerning IKE, PKIand the strength of the encryption algorithms used for global interoperability[7].

Today however, IPsec is optional in the current versions of IPv6. This makes IPv6 all the more vulnerable to security threats. There are a number of attacks that will be discussed in the paper[8]:

III. ATTACKS AGAINST IPV6

a. Transitioning Attacks
i. Dual Stack Attacks
ii. Tunneling Attacks
iii. Header Translation Attacks
b. Multicast Attacks
c. Extension Header Attacks

IV. ATTACKS AGAINST ICMPV6

d. Router Advertisement Spoofing
e. Router Advertisement Flooding

f. Neighbor Solicitation/Advertisement Spoofing

g. Duplicate Address Detection

Dual-stack attacks:

With the advantage of a smooth 4to6 transition throughDual Stack mechanism, it has its own security pitfalls also. For example, if there is a worm that has infected a host in a network, it will work by searching other hosts in the same subnet. Then it will spread by infecting those vulnerable hosts also. If the network is only IPv4, searching is done using 'Brute Force Scan'. This may take time in a large subnet. One may feel that IPv6 subnets which are hugemay be safe from this attack. However that's not the case. A worm in IPv6 uses ICMPv6 multicast ping. This is an echo request to multicast address, e.g. FF02::1 to discover on-link nodes. Well known multicast addresses like these make it easier to find key systems within a network e.g.FF05::2 is a site-local all routers address. Hence spreading of a worm would be faster in a dual stack network than in native IPv4 network. [5]

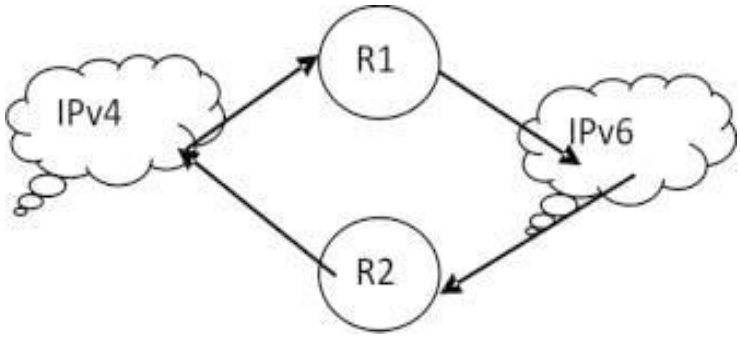

Figure 1 Tunneling Attack

V. TUNNELING ATTACKS

For tunneling, each end point of the tunnel must know its peer IP address before sending a packet to it. If the end points are pre-configured with IPv4 addresses then, considering huge sizes of IPv6 networks, it will become extremely difficult for the network administrator to manually configure these addresses.[6]

Thus Automatic Tunnels are introduced. Here, an end point's IPv4 address is computationally derived from the destination's IPv6 address. All the end points assume that once a packet arrives at the tunnel, its destination is also part of the tunnel. For example if we consider ISATAP (Inter-Site automatic Tunnel Addressing Protocol) tunnels, every end point has an IPv6 address of the following format:

<tunnel prefix><constantstring><IPv4 address>

Common to all end points. | 32 bit | End point

Routing Loop Attack can be introduced in these tunnels. Refer to Figure 1, the attacker exploits the fact that R2 does not know that R1 does not configure addresses from Prf2(tunnel prefix of R2) and that R1 does not know

that R2 does not configure addresses from Prf1(tunnel prefix of R1). The IPv4 network acts as a shared link layer for the two tunnels. Hence, the packet is repeatedly forwarded by both routers [9].

Header Translation Attack

Header translation is performed by a router which does a 6to4 or 4to6 translation of the headers. 'End to End Authentication' and 'Encrypted Security Payload' option of IPv6 are not present in IPv4. 'AH' shows integrity and 'ESP' shows integrity and confidentiality of the packet. Once these IPSec options are removed, the packet becomes very insecure and prone to attacks.

Multicast attacks

IPv6 protocol does not support broadcast communication but it does support multicast communication. However there are some special addresses which can be very dangerous. An 'All Nodes 'address is FF02::1, 'All Router' address is FF05::2 and 'All DHCP Server' address is FF05::5. These addresses enable an attacker to identify important resources on a network and attack them.

VI. EXTENSION HEADER ATTACKS

An IPv6 packet has a simpler header so that routing can be performed efficiently. The size of the header is fixed (40 bytes) and the options come as extension headers after the main header. Thus the router does not have to check all the extension headers. Although they need to check the Hop-by-Hop option.[10]Firewalls that should enforce their security policy must recognize and parse through all existing extension headers since the upper-layer protocol information reside in the last header. An attacker is able to chain lots of extension headers in order to pass through firewalls. He can also cause a denial of service attack, if an intermediary device or a host is not capable of processing lots of chained extension headers and might fail.

In addition to the above attacks, the Padn option in the Hop-by-Hop Extension header can be converted into a covert channel. Padn option is normally used for alignment purposes and has a string of 0's. An attacker can put malicious data in this option.

VII. ROUTER ADVERTISEMENT SPOOFING

If a rogue router starts sending spoofed router advertisement messages, all the nodes will update their routing tables with the new information which they have no way of verifying. Thus the rogue router now becomes one of their default routers, if the nodes communicate to the internet, the rogue router acts as a 'Man In the Middle' and can intercept all traffic.

VIII. OUTER ADVERTISEMENT FLOODING

During stateless auto configuration of addresses, new machines create unique addresses using network prefix provided by a router. This is done using Router Solicitation and Router Advertisement messages. However, an IPv6 device can be part of multiple networks(no upper limit). Therefore a RA Flooding attack can be launched by a rogue server which floods the network by RA Advertisement messages. Normally a node on the network has no way of authenticating a server. This causes the CPU to generate countless IPv6 addresses. This can cause

a system to hang and in fact this attack can bring down a network within seconds.

IX. NEIGHBOR SOLICITATION/ ADVERTISEMENT SPOOFING

IPv6 uses ICMP messages for discovery of neighboring devices on a network. These are multicast 'Neighbor Solicitation' and 'Neighbor Discovery' messages. An attacker can spoof these messages. He can send a fake binding of IP+MAC address. The IP address is that of a valid node but MAC address is that of the attacker. The victim node will update their Neighbor Cache which binds MAC addresses to IP addresses when they receive spoofed IP packets, which they cannot verify.[11] Thus the attacker can intercept all messages between the nodes by this method. Also a Denial of Service (DoS) attack can be administered by providing an invalid link layer address.

X. DUPLICATE ADDRESS DETECTION ATTACK

Duplicate Address Detection (DAD) is a technique during address auto configuration phase in which during the process of SLAAC, a node creates a unique IPv6 address on its own . It creates a local address using its MAC address and the link local address. It then multicasts this message, called a DAD message, to the entire network to check for duplicity. If the address is unique the router responds back with the network prefix. This prefix along with the MAC address becomes a unique IPv6 address for a device. An attacker can launch a Denial of Service attack if he answers to all DAD messages from a new node which is in the process of getting an IPv6 address assigned. The node thinks that this address is a duplicate one as is used by some other node. Thus it can never get an IP address and thus cannot become part of the network until the attacker stops the attack.

XI. CONCLUSIONS

IPv6 is no doubt the next generation in networking and no quick fix in IPv4 can slow down the evolution of IPv6. With its revolutionizing features and a never ending address space, IPv6 is welcoming the future with open arms. However the implementation is riddled with a number of security challenges which, if ignored can lead to disastrous consequences. Thus following the paradigm of 'Better safe than sorry', network administrators must take all the vulnerabilities in consideration and take adequate steps to safeguard themselves. A number of white collared hackers along with many other people from the industry are exposing new vulnerabilities of IPv6 everyday and are also giving solutions for protection. We must be fully prepared to embrace IPv6 but with complete security in place.

REFERENCES

Books:

[1] Foruzan, A. Behrouz,TCP/IP Protocol Suite, Third Edition, TataMcGraw-Hill Company,2012.

[2] Raghavan Arun, Secure Neighbour Discovery, ReportCS625: Advanced Computer Networks

Journal Papers:

[1] Minoli, D. Kouns, J., Security in an IPv6 Environment,CRCPress,USA,2009.

[2] Davies, J.,Understanding IPv6,2nd edition, Microsoft Press, USA, 2011.

[3] Hogg, S.,Vyncke, E.,IPv6 Security, Cisco Press, USA, 2009.

[4] Mayer Karl, Fritsche Wolfgang, Security models and dual-stack (IPv6/IPv4) implications**,** IABG,2010.

[5] Gabi Nakibly, Security Vulnerabilities of IPv6 Tunnels, Info Sec Institute, 2014.

[6] Penny HermannSeton, Security Features in IPv6, SANS Institute InfoSec Reading Room,2002.

[7] Weber Johannes,IPv6 Security-An Overview, Ripe Network Coordination Center, 2013.

[8] G.Nakibly, F.Templin,, Routing Loop Attack Using IPv6 Automatic Tunnels: Problem Statement and Proposed Mitigations, Internet Engineering Task Force (IETF):RFC 6324,August 2011.

[9] Naidu .P Santosh, PatchaAmulya,IPv6: Threats Posed By Multicast Packets, Extension Headers and Their CounterMeasures, IOSR Journal of Computer Engineering (IOSR-JCE),Volume 15, Issue 2 (Nov. - Dec. 2013), PP66-75,www.iosrjournals.org

.