IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. III (Jan – Feb. 2015), PP 13-18
www.iosrjournals.org

Security Issues in Next Generation IP and Migration Networks

Junaid Latief Shah[1], Javed Parvez[2]
[1] *Department of Computer Science, University of Kashmir, Srinagar, India*
[2]*Department of Computer Science, University of Kashmir, Srinagar, India*

Abstract: *As networks are mushrooming, the growth and development of IPv6 is gaining more importance. The wide scale deployment of this protocol into operational networks raises certain issues with security being one of the most compelling ones. The next generation internet protocol (IPng) introduces vulnerabilities in addition to those inherent in IPv4. While the existing security infrastructure like IPSec, SSL, PKI, and DNSSec might be sufficient for IPv4, the protocol security associated with IPv6 and migration networks needs to be assessed and analyzed. Until the time complete migration to IPv6 takes place, the internet migration techniques need to be secured. If left unprotected, these techniques pose a serious threat to networks. This paper presents an analysis of network attacks that are common in IPv4 and makes a comparative analysis of how these attacks may impact the IPv6 network. The paper also establishes guidelines and principles for mitigating these attacks. Additionally, the paper addresses the security issues that arise while migrating to IPv6 and outlines the secure mitigation techniques.*

Keywords: *IPv4, IPv6, IPSec, SSL, PKI, DNSSec*

I. Introduction

Initially during the design phase of end-to-end model, internet was seen as knowledge sharing “friendly” environment with no inherent security architecture. But the present day internet has become a hostile environment with network vulnerabilities. The introduction of IPv6 into current operational networks is seen as one of the biggest security challenges. With IPv4, the internet’s end to end model [1] has worked well for the past three decades, but due to address space depletion, complex set of configurations and limited security for exponential growth of internet, the migration to next generation of internet protocol i.e. IPv6 seems inevitable. As a result of large scale deployment of IPv6, security [2] has become an intrinsic issue in modern day internet-based computing. Although introduction of IPv6 will give birth to new protocol attacks, the existing and known IPv4 threats will certainly prevail in a polymorphic manner in IPv6 [4].Security framework in IPv6 is similar to one in IPv4 [3] with IPSec being mandatory, which was earlier considered optional in the legacy protocol. IPv6 might be inherently more secure than IPv4 in an ideal and well-coded application environment, but in reality the IPSec deployment with IPv6 will face same challenges and issues as prevalent in IPv4-IPSec deployment. Since most of the security breaches occur at the application level, the successful deployment of IPSec does not guarantee any network security. IPv6 is therefore usually deployed without any cryptographic protection making it vulnerable to network attacks. The migration from IPv4 to IPv6 has its own security implications which can influence the confidence of stakeholders who are ready for transition. During migration phase legacy IPv4 protocol has to coexist with IPv6 for substantial amount of time leaving room for older network vulnerabilities.

II. Security Loopholes in IPv4/IPv6

Depletion of address space and security vulnerabilities was the main motivation behind the deployment of IPv6. Several unanticipated vulnerabilities are likely to further emerge with large scale deployment of the new internet protocol. The following section throws light on some of the possible vulnerabilities and attacks, and additionally provides relevant security guidelines.

A. Reconnaissance Attacks

In this type of attack, the intruder gains as much information about the target network by network scanning as he does through passive data mining techniques. The network scanning provides intruder specific information regarding hosts and internetworking devices and their interconnections and also some loopholes which can be exploited. In IPv4, methods like ping sweeps, port and application scans are mostly used for collecting this information. Ping sweeps (which help in determining IP addresses that are being used in the organization) flood a network with ICMP or layer 4 ping messages that solicit a reply. Based on the data obtained, an intruder formulates hypothesis regarding layout of the target network. After learning about the network and its reachable systems, Port scans help hackers to listen to specific services [5] on ports that could be potentially vulnerable.

In IPv4, port scanning is a simple task as most of the IPv4 segments are class C addresses with 8 bits allocated for host. Scanning an IPv4 subnet at the rate of one host per second amounts to

2^8 hosts × (1 sec/1 host) × (1 min/60 sec) = 4.267 minutes.

In IPv6, this scenario is totally different as it uses 64 bits for subnet addressing and 64 bits for host addressing. Therefore an IPv6 subnet requires

2^{64} hosts $^{\times}$ (1 sec/1 host) × (1 year/ 31,536,000 sec) = 584,942,417,355 years

Scanning such a large address space is almost impossible [3], [6] making Reconnaissance attack very difficult in IPv6. However there are other ways around. The multicast address structure in IPv6 allow an intruder to find major key systems like routers, servers etc allowing it to scan vulnerabilities in these systems. Software tools like NMAP (Network Mapper) and Alive6 program (shipped with THC-IPv6 attacking toolkit) also help in launching Reconnaissance attacks in IPv6.

Security Guidelines

The large address space in IPv6 makes Reconnaissance attacks difficult, but not impossible. There are several recommendations to help thwart such attacks. The major network identifier devices should not be sequential and should not start at the lower end of the IPv6 subnet. From a security point of view, it is not a good idea to list the router as the first host on the network.

The usage of Random node ID's is recommended making scanning of the subnet more difficult. Any random mechanism of assigning the host address is good as long as there is a balance between security and maintainability. Many newer operating systems support the use of private addressing for end hosts. The use of private addressing with random node ID's can help keep the hosts randomly allocated and evenly distributed across the subnet.

B. Host Initialization Attacks

The host initialization process in IPv4 is carried out with protocols like ARP and DHCP. These protocols are vulnerable to spoofed communications by making end hosts to communicate with rogue or compromised devices or getting these devices configured with manipulated network information like DNS server address, default gateway address or address mask etc. In IPv4, a DHCP client usually boots up by broadcasting a message. Before the valid DHCP server responds to the client, a rogue DHCP server responds. In this way, a rogue server is able to set initial critical settings including the default gateway DNS server thereby enabling Man-in-the-Middle attacks. Thus DHCP messages can be spoofed allowing an attacker to utilize all the valid messages on the server.

The host initialization attacks do not change much when ported to IPv6. IPv6 provides provision for Stateful and stateless auto configuration of IP addresses thereby relieving the network administrator from the cumbersome task of manually assigning IP addresses and maintenance of DHCP servers in large enterprises. Stateless auto configuration works by combining two pieces of information: the network prefix, which can be obtained from the routers located in the network segment to which the host is attached and the hardware address, which can be obtained from the host's NIC card. Stateful auto-configuration uses the services of DHCPv6 server for generating the required address. The IPv6 neighbor discovery protocol is the key player in stateless auto configuration. After address generation, a node uses the services of NDP to discover other nodes using the same link. The protocol also lets the node discover routers and gateway devices to maintain reachability information on the detected active neighbors. NDP messages form part of ICMPv6 which is used for error reporting and diagnostic purposes. To configure an interface network address, a node first sends a router solicitation message (RS) to all routers multicast address to find the router and obtain network prefix value. Once the address has been configured, a node can use duplicate address detection (DAD) to check if that address is unique. In DAD procedure, a node sends a neighbor solicitation (NS) packet encapsulated with its tentative IP address with the purpose of obtaining a response packet from any node that might already be using the newly generated address. If the reply to the NS message is negative, the node that generated the address assumes it to be unique and uses it.ICMPv6 messages open the door for many attacks like Denial-of-Service (DOS) and Man-in-the-Middle (MITM) attacks when they are not secured through IPSec. The DAD procedure can be used as a platform to launch DOS attack. For executing this, an attacker usually sniffs the local link for a NS packet. The attacker falsely responds with neighbor advertisement packet informing the new node that it is already using that address. Upon reception of NA, the new node again generates another address and repeats the DAD procedure, the attacker again falsely responds with NA packet. Eventually the new node gives up without initializing its interfaces. An MITM attack gets executed when a malicious node impersonates a network segment's default gateway. The malicious node takes advantage of the fact that receiving node does not validate router advertisements (RA).Thus any node that receives a false RA updates its communication channel parameters blindly based on RA. A malicious node can propagate bogus address prefix information to re-route legitimate traffic to prevent the victim from accessing the network.

Security Guidelines

To detect DHCPv6 auto configuration or neighbor discovery abuses in IPv6, no security tools are available till date. These messages are normally filtered out at a router or a firewall like ICMP message. Since most of these attacks have limited domain, they therefore have a minimal impact on the network. The Secure Neighbor Discovery Protocol (SEND) is used as an alternative to IPSec for securing the Neighbor Discovery Protocol. SEND uses cryptographically generated addresses (CGA's) to verify the sender's ownership of claimed address. CGA's are IPv6 addresses in which part of the address is generated by applying a cryptographic one way hash function based on a node's public key and auxiliary parameters. The hash value can then be used to verify the binding between public key and node's address. In some environments, network administrators use a static entry for default route of a system which can be a cumbersome process.

C. Broadcast Amplification Attack (Smurf Attack)

The Broadcast Amplification Attack gets executed when an attacker spoofs the source address of victim and sends an echo request message to the subnet broadcast destination address. All the end hosts respond back to the spoofed source address and thus flood the victim with echo reply messages. The spoofed messages can be used to attack a single host at once or at least to use all hosts on a network to attack a single host. The first one can be used to run DOS attack against the whole network while the latter one is a kind of Distributed DOS in which many hosts try to interrupt a single host. These types of attacks are called amplification attacks because they multiply the quantity of packets i.e. payload on the network. If an attacker sends packets with a spoofed source address to a multicast group and all nodes in that group respond to that message, the spoofed source address, i.e. the address of the victim will be overwhelmed with traffic. A simple tool such as Smurf6 from the THC-IPv6 attacking toolkit [7] can send echo requests to the "all nodes" multicast address ff02::1. Sometimes, the victim may reside on a remote subnet. In that case all local nodes will be sending echo replies via their default router to the remote host i.e. the attack would not only affect the remote victim but also the local network.

Security Guidelines

A number of popular operating systems don't respond to echo request from a spoofed source address directed at the link local multicast address. Some uncertainty still exists in the protocol about whether end nodes should respond to ICMP messages with global multicast address as the source address. The ingress filtering of packets with IPv6 multicast source address is recommended and those packets with a multicast source address at the border of the network should be dropped.

D. Header Manipulation And Extension Headers

The transport layer information of the packet (TCP or UDP) is indicated by extension headers in IPv6 (RFC 2460).Within the IPv6 header, extension headers are indicated by the next header field and are used to extend the functionality of the protocol. If abused maliciously, extension headers pose a serious threat to a network. A packet can be crafted with unlimited number of extension headers linked together in a big list leading to DOS of intermediary systems along the transmission path or destination systems. Chain-linked list of extension headers is also a way of evading firewalls and network intrusion detection systems. These list-based extension headers could break the payload into a second fragmented packet that cannot be checked by the firewall that is only looking for the initial fragment. Extension headers can be manipulated in this way, thus denying services to the destination host or crashing the hosts stack.

Security Guidelines

These attacks are normally evaded by simple filtering on extension headers or having firewalls that have highly sensitive rules for header scanning. The extension headers that require special handling and attention include Destination options, Mobility and Routing headers. To control different extension headers, a number of different options are available in the Internet Operating Systems (IOS) IPv6 Access Control List (ACL). It is recommended to carry out parsing of complete extension header chain in all routers or middle boxes that receive a packet with extension header which is simpler than adding another level of security. Parsing the entire extension header chain quickly requires hardware optimization which may be difficult (or nearly impossible) because total header structure is non-deterministic.

E. Routing Attacks

These attacks focus on re-routing and redirecting traffic flow, causing disruption in a network. The major approaches usually include flooding of packets, quick announcement and removal of routes and bogus router implantations. Routing attacks can be used to redirect traffic through intermediate hosts before it reaches the actual destination. This could make the destination host believe that traffic was sourced from intermediate node and it could be used to evade firewalls that don't check for the presence of routing extension headers. Routing

Headers provide a base for launching MITM attacks or to rebound/relay packets from a potential victim. Currently there are two types of routing headers; RH0 and RH1. Due to replacement of destination address at every layer-3 hop that processes the routing header, RH0 is always vulnerable. This behavior makes it difficult for firewalls to determine the actual destination of the packet and compare it with firewall policy.

Security Guidelines

Several protocols don't change their security mechanism while transitioning from IPv4 to IPv6.The Multiprotocol-BGP was extended to carry IPv6 inter domain routing information. Therefore BGP continues to rely on TCP MD5 for authentication. The Intermediate System-to-Intermediate System (IS-IS) protocol [11] was extended in a draft specification [12] to support IPv6.The Open Shortest Path First Version 3 (OSPFv3) [13] and Routing Information Protocol Next Generation (RIPng) [14] have also undergone major change by removing the authentication fields from protocol specification. The Security Mechanisms to secure protocols that have changed with IPv6, OSPFv3, and RIPng are implemented inconsistently across internetworking devices. The usage of IPSec and IPv6 hop limits is recommended to secure the routing protocols and network devices.

F. Firewall Evasion By Fragmentation

Fragmentation attacks aim at evading network firewall and intrusion detection systems. The IPv4 protocol firewalls and IDS provide for deep packet inspection to reassemble packets and compare them to access control rules or attack signatures. Large amount of fragmented traffic has always been an early indicator of intrusion attempt because most baselines of internet traffic indicate that %age of fragmented traffic is low [8].Both the fragments from either IPv4 or IPv6 can be used by hackers to hide or launch attacks on a node. By dividing the packet into small fragments, the attacker can make fragments look legitimate and can try to bypass filtering or detection. To determine the true motive of a hacker would require reassembling all packets. An Attacker can exploit end hosts weaknesses in the method of reassembling the fragmented packets. A common example of this would be overlapping fragments having an overlap in the offset and out of order fragments. In this case, the fragment id's do not match correctly with the data. Fragmentation attacks also involve an attacker sending an incomplete set of fragments making the receiving host wait for the last fragment in the set. Although the default fragments time out is 60 seconds which can consume resources on intermediate systems. Sometimes the attacker uses nested fragments i.e. fragments within fragments to launch attacks where IPv6 protocol has multiple fragmentation headers. Commonly used software to manipulate fragmentation headers includes tools such as Whisker, Fragrouter, Teardrop and Bonk.

Security Guidelines

Similar to IPv4, current IPv6 firewalls and IDS's implement fragment reassembly and other fragmentation checks to mitigate fragmentation attacks. The fragmentation checking process includes inspecting out of cycle fragments and switching these packets into sequence as well as inspecting the number of fragments from a single IP given a unique identifier to determine Denial of Service (DoS) attacks. Till date, IPv6 has no known fragmentation attack tool, but that does not eliminate the threat that such tools exist or can be easily created. Some security guidelines include:

a) When possible, deny IPv6 fragments that are destined to an internetworking device.
b) Ensure adequate IPv6 fragmentation filtering capabilities.
c) Drop all fragments except the last one having size less than 1280 octets.

III. Security Issues In Migration Networks

Migration to IPv6 cannot be achieved overnight. Both the protocols need to coexist for a substantial period of time before IPv4 is phased out. The IETF has come up with several transition mechanisms like dual stacks, tunnels and protocol translation to aid the transition to IPv6.To evaluate the security implications of IPv4 to IPv6 transition and to select the appropriate transition mechanism for the network, the work has already started in 1990 and is still in the evaluation process due to the large infrastructural base of IPv4.This section lists the common vulnerabilities in the IPv4 to IPv6 migration networks and possible mitigation solutions.

A. Exploiting the Dual Stack

The main flaw with dual stack hosts is that IPv6 stack is enabled by default on several modern operating systems and IPv6 security policy is not enforced accordingly because naive or unaware users neglect the IPv6 migration. This might turn out to be quite dangerous because even if a network does not run IPv6, dual stack hosts are open to local IPv6 attacks. Consider a typical scenario in which an attacker knows that there are some operating systems having IPv6 enabled by default on that LAN. The attacker also learns that all the operating systems are protected against IPv4 attacks but not against IPv6 attacks. The attacker simply waits until a target operating system transmits its periodic router solicitation frame and the attacker might reply to it with router advertisement frame. This causes the node to complete its IPv6 initialization with stateless auto configuration (SLAAC).The next step for the victim machine is to run a DAD procedure. The attacker now has enough information about the target network and might launch IPv6 attack against the target operating system. The attack has a limited scope because the attacker is layer-2 adjacent to the potential victim. The attack success rate also depends on the victim not being protected against the IPv6 threats. Moreover if the network intrusion detection system (NIDS) is not IPv6 aware, the NIDS will not detect those attacks. These threats are also referred to as IPv6 latent threats i.e. existing threats just waiting to be activated.

Protecting the Dual Stack

Fortunately there are multiple ways to protect a dual stack host against the dual stack vulnerabilities.

a) Personal IPv6 Firewalls

Many of the existing network infrastructure components support IPv6 protocol. The need of the hour is to configure them correctly. Cisco Security Agent (CSA 6.0) is an example of a personal firewall and is IPv6 aware. The disabling of IPv6 stack or blocking all IPv6 traffic is a way of mitigating IPv6 latent threats.CSA 6.0 can block all traffic to and from a machine.

b) Microsoft's Group Policy Objects

Microsoft's GPO can be used inside an active directory domain to disable the IPv6 protocol on all interfaces.

c) Blocking Native IPv6 Traffic

The IPv6 Ethernet frames on a LAN with ether type 0x86dd can be blocked using a layer-2 switch. However, having a Virtual LAN Access Control List (VLAN ACL) or Port ACL is a more effective option

B. Exploiting Tunnels

Tunneling is used as a delivery mechanism of IPv6 traffic using existing IPv4 infrastructure. Before discussing about tunnel security, the network administrator should be able to make a clear distinction between the tunnel that is used within the network (i.e. connects two internal IPv6 networks over an IPv4 network) and a tunnel that is used to gain an IPv6 uplink to the internet for an inside network (i.e. a transition method if the ISP does not offer native IPv6). Since most IPv6 security methods lack authentication, integrity and confidentiality mechanisms, consequently, all tunneling mechanisms are susceptible to following attacks [9]:

a) Tunnel Sniffing

If an attacker is able to sniff the IPv4 routing path, he can control the IPv6 tunnel and can execute MITM attacks. The data can be redirected without the knowledge of legitimate user.

b) Tunnel Injection

The attacker can spoof the source IPv4 address of one tunnel end point and inject packets into the IPv6 network of the other tunnel endpoint. If the tunnel end point accepts packets which match the IPv4 address of the other tunnel end point without investigating the inner IPv6 addresses (ACL's etc), the attacker can send any IPv6 traffic into the network. An IPv4-only attacker can send these spoofed packets to the tunnel endpoint; however an attacker is only able to send spoofed IPv6 packets but has no possibility of receiving them from the victim network. Thus, an attacker can only execute DOS attacks. To create forged 6in4 packets, the packet manipulation program Scapy is often being used [10].

Countermeasures for Tunnels

In general, when using tunnels to transfer IPv6 packets into a private network, the firewall should screen the incoming tunnel traffic just the way regular incoming traffic is analyzed. Packets that enter the network through a tunnel should not be able to circumvent any packet filters. The policy applied for incoming IPv4 traffic should also be applied to a tunnel interface for IPv6 traffic i.e. ingress filtering. Unicast Reverse Path Forwarding (uRPF) should be enabled in order to block injected traffic from spoofed source IPv6 addresses that reside on the inside network. ACL's or tunnel inspection mechanisms would prevent the encapsulation of the spoofed 6in4 packets. Using IPSec between two endpoints adds authentication, confidentiality and integrity to all connections between two networks.

C. Protocol Translation (NAT 64)

The basic security drawback with NAT64 is that it breaks the end-to-end communication model and is thus incompatible with IPSec. Therefore IPSec use is not recommended. The protocol translation attracts DoS attacks in which an IPv6 attacker generates many outbound requests to deplete the IPv4 addresses and port pools of NAT64 device (Pool Depletion Attack). This type of attack is also possible in the IPv4-only NAT devices [9]. Although the Application Level Gateways (ALG) must inspect all packets which consume resources like CPU

Time and Memory Load, the NAT64 ALG as well as IPv4-only ALG does not add any security component. They just perform the basic job of connecting two different internet protocols.

IV. Conclusion

As summarized in this paper, IPv6 has both advantages as well as drawbacks from the security point of view. The paper carried out an extensive survey over the vulnerabilities and security weaknesses of IPv6. To ensure suitable and timely deployment of IPv6, the security aspects should be thoroughly considered. IPv6 provides number of security features over IPv4, such as mandatory usage of IPSec, but these features come with overheads and performance issues. This demands optimization in hardware and software like enhancing router filtering capabilities or implementing strong firewall rules. The similarities in two protocols help in implementing strong security policies to secure IPv6 networks. However new and additional characteristics in IPv6 demand new solutions to protect the next generation of integrated computer networks.

References

[1]. Bradner, S. "The End-to-End Security." IEEE Security & Privacy, vol., no. pp(2006): 76-79.

[2]. Treese, Win. "The state of security on the internet." NetWorker 8.3 (2004): 13-15.

[3]. Convery, Sean, and Darrin Miller. "Ipv6 and ipv4 threat comparison and best-practice evaluation (v1. 0)." Cisco systems (2004).

[4]. Caicedo, Carlos E., James BD Joshi, and Summit R. Tuladhar. "IPv6 Security Challenges." IEEE Computer 42.2 (2009): 36-42.

[5]. Ford, Matthew D. "New Internet Security and Privacy Models Enabled by IPv6." SAINT Workshops. 2005.

[6]. Popoviciu, Ciprian. Deploying ipv6 networks. Pearson Education India, 2006.

[7]. Marc "van Hauser" Heuse. THC IPv6 Attack Toolkit. http://www.thc.org/thc-ipv6/,2012.

[8]. Shannon, Colleen, and David Moore. "Characteristics of fragmented IP traffic on Internet links." Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement. ACM, 2001.

[9]. Hogg, Scott, and Eric Vyncke. IPv6 security. Pearson Education, 2008.

[10]. Biondi, Philippe. "Scapy." see http://www. secdev. org/projects/scapy (2011).

[11]. Callon, Ross W. "Use of OSI IS-IS for routing in TCP/IP and dual environments." (1990).

[12]. Hopps, Christian. "Routing IPv6 with IS-IS." (2008).

[13]. Coltun, Rob, et al. OSPF for IPv6. RFC 2740, December, 1999.

[14]. Malkin, Gary Scott. "RIPng protocol applicability statement." (1997).

[15]. Wadhwa, Mohit, and Manju Khari. "Security Holes in Contrast to the New Features Emerging in the Next Generation Protocol." International Journal of Computer Applications 20.3 (2011): 35-39.

[16]. Weber, Johannes, Christoph Wegener, and Jörg Schwenk. "Master Thesis IPv6 Security Test Laboratory." (2013).

[17]. Barker, Keith. "The security implications of IPv6." Network Security 2013.6 (2013): 5-9.

[18]. Shah, J. L., & Parvez, J. (2014, September). Evaluation of queuing algorithms on QoS sensitive applications in IPv6 network. In Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on(pp. 106-111). IEEE.

[19]. Shah, J. L., & Parvez, J. (2014, July). An examination of next generation IP migration techniques: Constraints and evaluation. In Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on (pp. 776-781). IEEE.

[20]. Shah, J. L., & Parvez, J. (2014, July). Performance evaluation of applications in manual 6in4 tunneling and native IPv6/IPv4 environments. In Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on (pp. 782-786). IEEE.

[21]. Shah, Junaid Latief and Javed Parvez. "Migration from IPv4 to IPv6: Security Issues and Deployment Challenges." *International Journal of Advanced Research in Computer Science and Software Engineering* 4.1 (2014):373-76.