www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 8 August, 2013 Page No. 2486-2493

Ipv6 Security: Issue Of Anonymity

Varsha Alangar [1],Anusha Swaminathan[2]

[1]Meenakshi Sundararajan Engineering College (Affiliated to Anna University), Department of Computer Science Engineering, Kodambakkam, Chennai, Tamil Nadu, India
varsha.alangar@gmail.com

[2] Meenakshi Sundararajan Engineering College (Affiliated to Anna University), Department of Computer Science Engineering, Kodambakkam, Chennai, Tamil Nadu, India
g8anush@gmail.com

August 20, 2013

Abstract:

IPv6, the latest revision of the Internet Protocol, is intended to replace IPv4, which still carries the vast majority of Internet traffic as of 2013. The advent of IPv6 changes not only the network components, but also the security field shifts. We see new types of attacks or at least variations of the attacks we know from IPv4. Although IPv6 was designed with the aim of superseding its ancestors; it is defected in its ability to provide security to its users, anonymity being one such issue. Anonymity is preferred by internet users, and in IPv4, this has been achieved to some extent using NAT. However in IPv6, the protocol re-introduces a transparent end-to-end connectivity, thus eliminating masquerading feature that was previously obtained via NAT. The documented methods of mapping MAC and IPv6 addresses also exposes the users to be easily identified. The preference of anonymity would have to trade off with the performance. This brings the issue of challenges in preserving anonymity in IPv6. This article provides an overview of the IPv6 security vulnerabilities that arise with the launch of IPv6 and a possible solution to overcome the problem with anonymity. We propose the use of a "default deny" policy in firewall that forbids any request not explicitly mentioned by the user.

Keywords: IPV6, Security, Attacks, Firewall

1. INTRODUCTION

In order to understand the issue at hand, it is important to have an in-depth knowledge about IPv6, its features and the reason it has started replacing the ever popular IPv4. The IPv6 protocol has solved some, but not all, of the security problems found in IPv4 networks. One example is the mandatory inclusion of IP Security (IPsec) in the IPv6 protocol, which makes it fundamentally more secure than the older IPv4 standard. However, given its flexibility, the IPv6 protocol introduces new problems. A mobile IP protocol is built into the IPv6 protocol, and security solutions for this protocol are still under development. In addition, the dynamic configuration flexibility of IPv6 (such as stateless address auto configuration) could also become a serious security problem, if not implemented correctly. The overall enhancements in IPv6 may provide better security in certain areas, but there are areas that attackers may be able to exploit. This article will focus on the security improvements over IPv4, possible threats, mainly the concerns for anonymity and also a possible solution to curb it.

2. IPV6: AN OVERVIEW

An Internet Protocol or IP address is a number that identifies each sender or receiver of information sent over the internet. The computer industry has been using IPv4 (Internet Protocol version 4) for these addresses since that protocol was developed. That technology is now reaching its technical limits for supporting unique Internet addresses, due in part to a large amount of growth with mobile devices including: mobile phones, notebook computers and wireless handheld devices. With IPv4 addresses running out this year, the entire Internet industry must adopt a new protocol called, IPv6, also called the Next Generation Internet Protocol (IPng). IPv6 is an Internet. Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks, closely adhering to the design principles developed in the previous version of the protocol, Internet Protocol Version 4 (IPv4). IPv6 was first formally described in Internet standard document RFC 2460, published in December 1998. In addition to offering more addresses, IPv6 also implements features not present in IPv4. It simplifies aspects of address assignment (stateless address auto-configuration);network renumbering and router announcements when changing

network connectivity providers. It simplifies processing of packets by routers by placing the need for packet fragmentation into the end points. In other words, with this new protocol, there will be increased address space, which will allow many more devices and users on the Internet. Many companies, including Yahoo!, are coming together to help motivate organizations across the industry- Internet service providers, hardware manufacturers, operating system vendors and other web companies- to prepare their services for their transition. We are committed to helping prepare our users for the day when IPv4 will no longer be supported, by giving them a chance to verify whether their systems are compatible with IPv6.

2.1 Why switch over to IPv6?

IPv6 provides a great solution to the address space crunch that was the underlying reason for the widespread adoption and usage of the Network Address Translation. A lack of address space resulted in a proportionately higher demand for the domain names in comparison to the availability of the same on the supply side. This led to a squeeze in the availability of IP address thereby resulting in a situation where the IP address prices were shooting through the roof. The situation further made sense for the organizations to go for Network Address Translation technique as a cost-cutting tool.

In this way, the address space constraint in the IPv4 fuelled the popularity and widespread usage of the Network Address Translation process to overcome the situation. If an organization couldn't have enough IP addresses, then it could share them or create them over the local network through the use of a Proxy server and then map the internal IP addresses to the real IP addresses over the Internet thereby making the online communication process streamlined.

The Internet Protocol version 6 or IPv6 eliminates the need for Network Address Translation by offering a much larger address space that allows the network resources to have their own unique real IP address. In this way, IPv6 strikes at the very root of the problem for which Network Address Translation (NAT) provided a solution.

IPv6 offers a significantly larger address space that allows greater flexibility in assigning unique addresses over the Internet. IPv4 (the currently used standard protocol over the Internet that carries bulk of the network traffic), provides 32 bits of address space while the IPv6 offers 128 bits of address space that is easily able to support 2128 or 3.4W1038 or about 340 billion unique IP addresses. This allows a provision for permanent unique addresses to all the individuals and hardware connected to the Internet. Moreover, the extended address length eliminates the need to use techniques such as network address translation to avoid running out of the available addresses.An escalating demand for IP addresses acted as the driving force behind the development of IPv6. According to industry estimates, in the wireless domain, more than a billion mobile phones, Personal Digital Assistants (PDA), and other wireless devices will require Internet access, and each will need its own unique IP address.

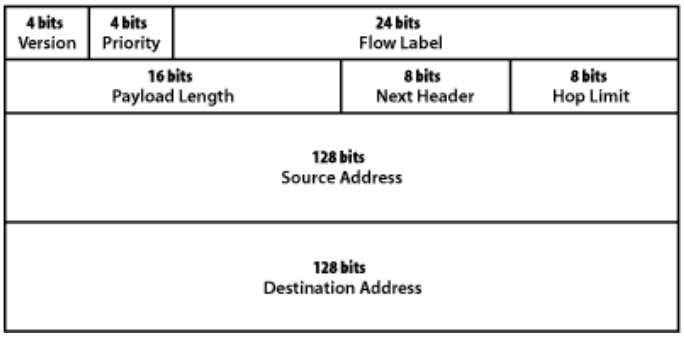
Moreover, billions of new, always-on Internet appliances for the home - ranging from the TV to the refrigerator - will also come online through the different technologies. Each of these devices will also require their own unique IP address. With the exponentially increasing demand for IP addresses, the world is fast outgrowing IPv4 and waiting to embrace IPv6.

In this way, the IPv6 protocol does away with the need to use Network Address Translation technique to make up for the address space crunch by creating local IP addresses over the LAN and mapping them to the real IP addresses used over the network.

IPv6 also offers superior security features thereby allaying the fears of allocating static IP addresses to the various network resources and throwing them open to attacks in the virtual space. The security issue is often used in the defence of the Network Address Translation process. However, the core principle of Internet is to offer an end-to-end connectivity to the different network resources.This principle is violated by the widespread use of network address translation. It is like missing the woods for the trees. In this context, IPv6 provides a long-term solution to meet the address space crunch as well as the security concerns of the Internet users. For all practical purposes, IPv6 offers an almost endless supply of IP addresses that can be allocated to the exponentially increasing network devices that are being added to the Internet with each passing day. This large pool of IP addresses will provide an abundant supply of usable IP addresses and easily match the demand for the same. This equilibrium will bring the Internet address prices back to normal levels.

2.2 Packet format

An IPv6 packet has two parts: a header and payload.



The header consists of a fixed portion with minimal functionality required for all packets and may be followed by optional extensions to implement special features.

The fixed header occupies the first 40 octets (320 bits) of the IPv6 packet. It contains the source and destination addresses, traffic classification options, a hop counter, and the type of the optional extension or payload which follows the header.

This *Next Header* field tells the receiver how to interpret the data which follows the header. If the packet contains options, this field contains the option type of the next option. The "Next Header" field of the last option, points to the upper-layer protocol that is carried in the packet's payload.

Extension headers carry options that are used for special treatment of a packet in the network, e.g., for routing, fragmentation, and for security using the IPsec framework.

Without special options, a payload must be less than 64kB.

With a Jumbo Payload option (in a *Hop-By-Hop Options* extension header), the payload must be less than 4 GB.

2.3 Addressing

Compared to IPv4, the most obvious advantage of IPv6 is its larger address space. IPv4 addresses are 32 bits long and number about 4.3×10^9 (4.3 billion). IPv6 addresses are 128 bits long and number about 3.4×10^{38} (340 undecillion). IPv6's addresses are deemed enough for the foreseeable future.

IPv6 addresses are written in eight groups of four hexadecimal digits separated by colons, such as:

2001:0db8:85a3:0000:0000:8a2e:0370:7334.

IPv6 unicast addresses other than those that start with binary 000 are logically divided into two parts: a 64-bit (sub-) network prefix, and a 64-bit interface identifier.

For stateless address auto configuration (SLAAC) to work, subnets require a /64 address block, as defined in RFC 4291 section 2.5.1. Local Internet registries get assigned at least /32 blocks, which they divide among ISPs. The obsolete RFC 3177 recommended the assignment of a /48 to end-consumer sites. This was replaced by RFC 6177, which "recommends giving home sites significantly more than a single /64, but does not recommend that every home site be given a /48 either". /56s are specifically considered. IPv6 addresses are classified by three types of networking methodologies: unicast addresses identify each network interface, anycast addresses identify a group of interfaces, usually at different locations of which the nearest one is automatically selected, and multicast addresses are used to deliver one packet to many interfaces. The broadcast method is not implemented in IPv6. Each IPv6 address has a scope, which specifies in which part of the network it is valid and unique. Some addresses are unique only on the local (sub-) network. Others are globally unique.

2.4. Features of IPv6:

Easier management of networks
End-to-end connective integrity
Unconstrained address abundance
Platform for innovation and collaboration
Integrated interoperability and mobility
Improved security features

- IPv6 networks provide auto configuration capabilities. They are simpler, flatter and more manageable, especially for large installations.
- Direct addressing is possible due to vast address space - the need for network address translation devices is effectively eliminated.
- 3.4 x 1038 = 340 trillion addresses - about 670 quadrillion addresses per square millimeter of the Earth's surface.
- Given the numbers of addresses, scalability and flexibility of IPv6, its potential for triggering innovation and assisting collaboration is unbounded.
- IPv6 provides interoperability and mobility capabilities which are already widely embedded in network devices.
- IPSEC is built into the IPv6 protocol, usable with a suitable key infrastructure.

Because of the above benefits, the IPv6 protocol has great potential to not only relieve IPv4 address space shortage, but to build larger, more efficient networks, and support greater international interoperability. It can allow business innovation and opportunity through just-in-time processes, mobility features and location-based services. Below are some less obvious examples of how IPv6 might assist business:

- **IPv6 can lift production efficiency via real-time information:**
  Computers and networks substantially boosted productivity in the mid-1990s partly because business managers could obtain access to sales information in real time. IPv6 can provide even greater inventory control, with real-time information that allows production planning to meet customer demand more accurately, and reduces the need to continue paying for redundant production capacity.
- **IPv6 can shift time-based maintenance regimes to performance:**
  Currently industry uses time-based maintenance regimes, i.e. after a certain period, do a certain type of maintenance. IPv6 can support extensive sensor networks which can provide information on the *actual* usage of an item (or its current performance level) so that maintenance can be scheduled when it is genuinely needed.
- **IPv6 can help us move beyond economies of scale and the tyranny of distance:**
  Linking of market information to production capacity allows production to be more responsive to market needs. In addition, the introduction of digital control technology into production facilities means that shorter runs are possible, without compromising cost savings from economies of scale. Interoperability derived from IPv6 will allow better integration with global markets, which will overcome some of the challenges of our remote location in the world.

3. SECURITY CONSIDERATIONS

3.1. Massive Size of the IP Address Space Makes Port Scanning Harder:

When they start, attackers usually employ port scanning as a reconnaissance technique to gather as much information as possible about a victim's network. It is

estimated that the entire IPv4 based Internet can be scanned in about 10 hours with enough bandwidth, given that IPv4 addresses are only 32 bits wide. IPv6 dramatically increases this limit by expanding the number of bits in address fields to 128 bits. By itself, such a massive address space creates a significant barrier for attackers wanting to conduct comprehensive port scanning. However, it should be noted that the port scanning reconnaissance technique used in IPv6 is basically the same as in IPv4, apart from the larger IP address space. Therefore, current best practices used with IPv4, such as filtering internal-use IPv6 addresses in border routers, and filtering un-used services at the firewall, should be continued in IPv6 networks.

3.2. Cryptographically Generated Address (CGA)

In IPv6, it is possible to bind a public signature key to an IPv6 address. The resulting IPv6 address is called a Cryptographically Generated Address (CGA). This provides additional security protection for the IPv6 neighborhood router discovery mechanism, and allows the user to provide a "proof of ownership" for a particular IPv6 address. This is a key differentiator from IPv4, as it is impossible to retrofit this functionality to IPv4 with the current 32-bit address space constraint. CGA offers three main advantages:

1. It makes spoofing attacks against, and stealing of, IPv6 addresses much harder.
2. It allows for messages signed with the owner's private key.
3. It does not require any upgrade or modification to overall network infrastructure.

3.3. Replacing ARP by Neighbor Discovery (ND) Protocol

In the IPv4 protocol, a layer two (L2) address is not statically bound to a layer three (L3) IP address. Therefore, it can run on top of any L2 media without making significant change to the protocol. Connection between L2 and L3 addresses is established with a protocol named Address Resolution Protocol (ARP), which dynamically establishes mapping between L2 and L3 addresses on the local network segment. ARP has its own security vulnerabilities (such as ARP Spoofing). In the IPv6 protocol, there is no need for ARP because the interface identifier (ID) portion of an L3 IPv6 address is directly derived from a device-specific L2 address (MAC Address). The L3 IPv6 address, together with its locally derived interface ID portion, is then used at the global level across the whole IPv6 network. As a result, the security issues related to ARP no longer apply to IPv6. A new protocol called Neighbor Discovery (ND) Protocol for IPv6 is defined in RFC 486111 as a replacement to ARP.

4. IPV6 SECURITY:

The prevailing Internet Protocol standard is IPv4 (Internet Protocol version 4), which dates back to the 1970s. There are well-known limitations of IPv4, including the limited IP address space and lack of security. IPv4 specifies a 32-bit IP address field, and available address spaces are rapidly running out. The only security feature provided in IPv4 is a security option field that provides a way for hosts to send security and handling restrictions. As a result, the Internet Engineering Task Force (IETF) has been working on the IPv6 (Internet Protocol version 6) specifications in order to address these limitations, along with a number of performance, ease-of-configuration, and network management issues. The core IPv6 specifications have been defined by various Request for Comments (RFCs) such as RFC 24602 (IPv6 Protocol), RFC 48613 (IPv6 Neighbor Discovery), RFC 48624 (IPv6 Stateless Address Auto-Configuration), RFC 44435 (Internet Control Message Protocol for IPv6 (ICMPv6)), RFC 42916 (IPv6 Addressing Architecture), and RFC 43017 (Security Architecture for IP or IPsec).

IP Security, or IPsec for short, provides interoperable, high quality and cryptographically based security services for traffic at the IP layer. It is optional in IPv4 but has been made mandatory in the IPv6 protocol. IPsec enhances the original IP protocol by providing authenticity, integrity, confidentiality and access control to each IP packet through the use of two protocols: AH (authentication header) and ESP (Encapsulating Security Payload).

4.1 Issues in security

Although IPv6 is a security-enabled protocol, migration from IPv4 can create new risks and weaken an organization's security strategy.Though, the security provided by IPv6 is a great improvement over IPv4, it has its shortcomings. Among these are the following:

- Due to export laws, the strength of the encryption algorithms to be used to ensure global interoperability is limited.
- IPsec relies on a public-key infrastructure (PKI) that has not yet been fully standardized.
- There is some additional work needed in the IKE area and in improving protection against Denial of Service/Flooding attacks.

Security practitioners need education/training on IPv6. IPv6 will come to the networks under your control – it's only a matter of time. As with any new networking technology, it's essential that you learn the basics of IPv6, especially the addressing scheme and protocols, in order to facilitate incident handling and related activities.Security tools need to be upgraded.

IPv6 is not backwards compatible. The hardware and software used to route traffic across networks and perform security analyses won't work with IPv6 traffic unless they are upgraded to versions that support the protocol. This is especially important to remember when it comes to perimeter-protection devices. Routers, firewalls and intrusion-detection systems may require software and/or hardware upgrades in order to "speak" IPv6. Many manufacturers already have these upgrades available. For example, Cisco networking devices support IPv6 as of IOS release 12.0S.

Existing equipment may require additional configuration. The devices that do support IPv6 typically treat it as an entirely separate protocol (as they should). Therefore, the access control lists, rule bases and other configuration parameters may need to be reevaluated and translated to support an IPv6 environment.

Tunneling protocols create new risks. The networking and security communities have invested time and energy in ensuring that IPv6 is a security-enabled protocol. However, one of the greatest risks inherent in the migration is the use of tunneling protocols to support the transition to IPv6. These

protocols allow the encapsulation of IPv6 traffic in an IPv4 data stream for routing through non-compliant devices.

Therefore, it's possible that users on your network can begin running IPv6 using these tunneling protocols before you're ready to officially support it in production. If this is a concern, block IPv6 tunneling protocols (including SIT, ISATAP, 6to4 and others) at your perimeter.IPv6 auto configuration creates addressing complexity.

Auto configuration, another interesting IPv6 feature, allows systems to automatically gain a network address without administrator intervention. IPv6 supports two different auto configuration techniques.

Stateful auto configuration uses DHCPv6, a simple upgrade to the currentDHCP protocol, and doesn't reflect much of a difference from a security perspective.

On the other hand, stateless auto configuration must be looked out for. This technique allows systems to generate their own IP addresses and checks for address duplication. This decentralized approach may be easier from a system administration perspective, but it raises challenges for those of us charged with tracking the use (and abuse!) of network resources.

4.2. Neighbor discovery and Stateless Address Auto-configuration

Neighbor discovery (ND) is a replacement for ARP, and stateless address auto configuration—which allows an IPv6 host to be configured automatically when connected to an IPv6 network—is a lightweight DHCP-like function provided in ICMPv6. They are both powerful and flexible options in the IPv6 protocol. However, ND may be still subject to attacks that could cause IP packets to flow to unexpected places.

Denial of service may be one of the results. Also, such attacks could be used to allow nodes to intercept and optionally modify packets destined for other nodes. While this may be protected with an IPsec AH, RFC 375613 (IPv6 ND Trust Models and Threats) also defines the type of networks in which the secure IPv6 ND mechanisms are expected to work. The three different trust models can roughly corresponding to secured corporate intranets, public wireless access networks, and pure ad hoc networks. Moreover, the Secure Neighbor Discovery (SEND) protocol is developed to provide an alternate mechanism for securing neighbor discovery with a cryptographic method.

Neighbor discovery, as well as router solicitation in the IP network (v4 or v6) uses ICMP. While ICMPv4 is a separate protocol on the outside of IPv4, ICMPv6 is an integral protocol running directly on the top of the IPv6 protocol, which again could lead to security problems.

Exchanging ICMPv6 messages on the top of the IPv6 protocol for vital "network health" messages and environment solicitations are crucial for IPv6 communication. However,
this, could be abused by sending fake, carefully crafted response messages for denial of service, traffic re-routing or other malicious purposes. For security reasons, the IPv6 protocol recommends that all ICMP messages use an IPsec AH, which is able to offer integrity, authentication and anti-relay functions. It may be better to specify critical systems as static neighbor entries to their default router, instead of using ND, this would avoid many typical neighbor-discovery attacks.

4.3 Attacks

4.3.1.Multicast

Via certain multicast messages an attacker can very fast do a reconnaissance attack on a local network. Simply pinging the all-nodes multicast address ff02::1 shows several machines that are alive. Additionally, some NMAP scripts can be used to reveal almost all IPv6 clients on the network via forcing them to generate new (temporary) IPv6 addresses via SLAAC. The corresponding Multicast Listener Discovery messages from the clients, which are sent via multicast, reveal their interface IDs.

4.3.2. Extension Headers

Inside extension headers an attacker can send information that remain undetected if the intermediary firewalls do not fully check the options of these headers. This kind of attack is called "covert channel". For example, inside the Hop-by-Hop extension header, the PadN option which according to the standard must contain zeros, can be filled with any characters. That means, hidden information can be sent via the network without touching the upper layer protocols.

Vulnerability arises with the routing header 0 (RH0). With its usage, a Denial-of-Service (DoS) attack between two nodes or firewall bypassing strategies can be performed. But since RFC 5095 deprecated the overall usage of RH0 in 2007, these attacks are not explained here one more time

4.3.3. Attacks against ICMPv6

ICMPv6 plays a key role in the proper usage of IPv6. Especially the Neighbor Discovery messages such as Router Advertisements (RAs) and Neighbor Solicitation/Advertisements (NS/NA) are needed for the straightforward usage of the new Internet Protocol.

4.3.3(a). Router Advertisement Spoofing

If an attacker sends spoofed Router Advertisements inside a subnet, all IPv6 nodes will immediately change their routing tables and store the attacker as one of the default routers. If they send traffic to the Internet, this new default router will be used. This leads to a situation in which the attacker can fully see (and even modify) all outgoing traffic from the IPv6 nodes to the Internet. This is called a Man-in-the-Middle (MITM) attack. Meanwhile the attacker cannot see the returning traffic from the Internet since he is not able to spoof the real default router on the network. See Figure 1 below for an illustration of this attack.

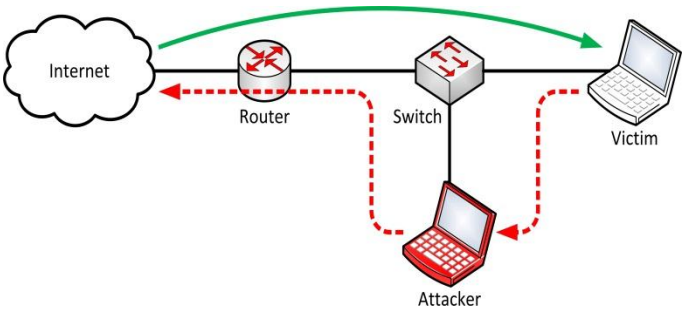


Figure 1: Router Advertisement Man-in-the-Middle Attack

4.3.3(b). Router Advertisement Flooding

The attacker can also flood many thousand RAs which immediately freezes all Microsoft Windows computers since they are completely overloaded with that many SLAAC processes. This bug is known for many years but still exploitable. That means: If an attacker has access to a local network and is not stopped by the intermediary switch while sending spoofed RAs, the complete Windows environment will be frozen!

4.3.3©. Neighbor Discovery Spoofing

When the attacker spoofs certain Neighbor Advertisements, he can execute a MITM attack. By answering falsified Neighbor Advertisements to the issued Neighbor Solicitations from the victims, he redirects all IPv6 traffic over his "routing instance" in the same subnet (see Figure 2).

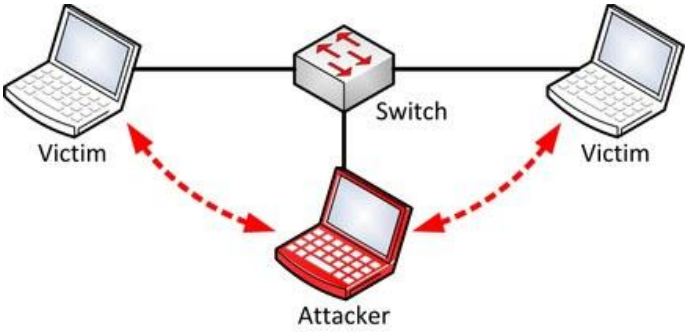


Figure 2: Neighbor Advertisement Man-in-the-Middle Attack

4.3.3(d) Duplicate Address Detection

A DoS attack is executed if the attacker answeres to all Duplicate Address Detection messages (DADs) from a new IPv6 node (with a not yet assigned IPv6 address). The node always believes that this address is already in use and will never get an available IPv6 address and is therefore unable to access the network. This situation remains until the attacker stops the attack.

4.3.4. Attacks against DHCPv6

4.3.4(a). Address Space Exhaustion

If the concept of stateful DHCPv6 is used, an attacker can exhaust the IPv6 address pool on the server, similar to a DHCPv4 server. Even though the DHCPv6 server could provide enough IPv6 addresses, it has to store a small binding for each address and the corresponding DUID from the client which will at least exhaust the memory of the server if it is flooded with many requests.

4.3.4(b). Rogue DHCPv6 Server

An attacker can also place his own DHCPv6 server inside a network and distribute falsified values, e.g. a spoofed DNSv6 server address. If the clients accept this DNS server, they will get falsified DNS responses from now on if the attacker also owns the spoofed DNS server. With this attack, internal IPv6 users can be redirected to other (web-) servers than they intended to access. The picture below shows the basic attack in the local network.

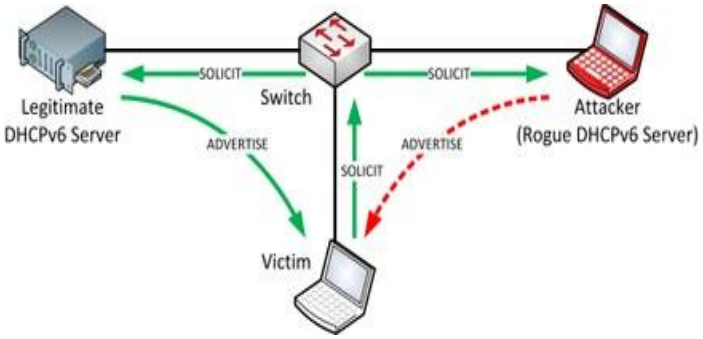


Figure 3: Rogue DHCPv6 Server

4.4. Attack Toolkits

In order to test own equipment and security appliances, the following IPv6 attack toolkits can be used:

- THC-IPv6: The toolkit from Marc Heuse provides many easy to use tools which require almost only the specification of the network interface.
- SI6 Networks' IPv6 Toolkit: This package of tools from Fernando Gont can be used in a more precise manner since it can be fine-tuned with many options. Likewise it is more complicated to use compared to the THC-IPv6 toolkit.
- Scapy: To send completely crafted IPv6 packets, the packet manipulation tool Scapy from Philippe Biondi can be used.

5. APPROACHES

5.1 IPv6 with Firewalls

A possible solution we opted to consider with respect to IPv6 security is the use of firewalls. The first line of

defenceof most enterprise networks is a firewall that aims to prevent attacks from the public Internet to the enterprise network, and limits how local users can access the public Internet. As IPv6 is rolled out on enterprise networks, IPv6 firewalls will be deployed so that the same security policies that are currently being enforced in IPv4 are enforced in IPv6. While IPv6 and IPv4 are very similar in terms of the service they provide -- a best-effort datagram service -- there are some subtle differences between these two protocols that have larger implications on firewall design and operation. This article discusses some of those differences and highlights how they affect the design and operation of IPv6 firewalls. It then explains how these differences might be leveraged for malicious purposes and offers ways to mitigate and eliminate security holes in the IPv6 firewall.

5.2 Security implications on theIPv6 firewall

The IPv6 header chain structure allows for more flexibility than IPv4, in the sense that there is no limit on the number of options that any packet can include. However, this flexibility comes at a price.

Any system willing to obtain upper-layer information, such as TCP port numbers, will need to process the entire IPv6 header chain. And since the current protocol specifications allow for an arbitrary number of extension headers, including multiple instances of the same extension header type, it results in a number of implications for devices like firewalls:

- A firewall may need to parse multiple extension headers in order to perform deep packet inspection (DPI), which could result in degraded WAN performance, denial of service (DoS) or firewall circumvention.
- The combination of extension headers and fragmentation may prevent deep packet inspection.

Since the current protocol specifications allow for an arbitrary number of extension headers, including multiple instances of the same extension header type, a firewall must be prepared to gracefully handle packets that contain an unusually large number of IPv6 extension headers. This could be exploited by attackers who could intentionally include an arbitrarily large number of extension headers in their packets so that firewalls employ more resources when processing the aforementioned packets. Eventually, this could result in reduced firewall performance, or a DoS of the firewall itself. Additionally, some poorly implemented firewalls might fail to process the entire IPv6 header chain when trying to enforce a filtering policy, possibly allowing attackers to leverage extension headers to circumvent the corresponding firewall.

IPv6 fragmentation can also be leveraged for malicious purposes in similar ways to its IPv4 counterpart. For example, to circumvent a firewall's filtering policy, an attacker may send overlapping fragments to confuse how these fragments would be reassembled by the destination host. IPv6 exacerbates this problem, since the combination of multiple IPv6 extension headers and fragmentation might result in fragments that, despite their "normal" packet size, could manage to hide even basic information usually needed for enforcing filtering policies, like TCP port numbers. That is, the first fragment of a packet could contain a number of IPv6 options so large that the upper-layer protocol header would belong to some other fragment than the first one.

5.3 Possible IPv6 security mitigations

Clearly, in order to enforce an IPv6 packet filtering policy, firewalls should at the very least support processing of the entire IPv6 header chain. Such firewalls should ideally also support IPv6 transition technologies, so that the same filtering policies that are applied on native IPv6 traffic can be applied on transition traffic. That said, firewalls should implement a **"default deny" policy**, so that the firewall blocks traffic you didn't take into account, like transition traffic.

Potential resource exhaustion attacks, which leverage the use of multiple extension headers, could be mitigated by enforcing a limit on the maximum number of extension headers that the firewall will allow in any given IPv6 packet. A sensible limit could be to allow one instance of each of the currently defined extension headers. However, some other limit such as “16” could be enforced -- for instance, OpenBSD enforces such a limit. The limit should allow legitimate traffic, while not allowing a ridiculously large number of extension headers. Packets that exceed this limit should be dropped. While this would degrade performance, it would also prevent DoS.

Finally, firewall circumvention techniques that employ fragmentation could be mitigated by requiring the first fragment of an IPv6 datagram to contain the full packet headers needed to enforce a packet filtering policy. That is, if a firewall receives the first fragment of a datagram that fails to contain the full upper-layer header, such as the TCP header, the corresponding packet should be dropped. Firewall circumvention techniques could also be mitigated by having the firewall reassemble fragmented datagrams before applying its filtering policy.

6 RECOMMENDATIONS

Below are some best practices for reference in building and maintaining secure IPv6 networks:

- Use standard, non-obvious static addresses for critical systems;
- Ensure adequate filtering capabilities for IPv6;
- Filter internal-use IPv6 addresses at border routers;
- Block all IPv6 traffic on IPv4-only networks;
- Filter unnecessary services at the firewall;
- Develop a granular ICMPv6 filtering policy and filter all unnecessary ICMP message types;
- Maintain host and application security with a consistent security policy for both IPv4 and IPv6;
- Use IPsec to authenticate and provide confidentiality to assets;
- Document the procedures for last-hop traceback;
- Pay close attention to the security aspects of transition mechanisms.

7 REFERENCES

[1] Al-Radhi, A, A. 2011. *IPv6 Promised Role in Mitigating Cyber Attacks: Really it's Time!.* Swiss Cyber Storm-International IT Security Conference, Switzerland.

[2] Khaldoun, B. Khaled, B. Amer, A. 2011. *THE NEED FOR IPv6*. International Journal of Academic Research,Vol. 3. No. 3. II Part. PP.431-448, Azerbaijan.http://www.ijar.lit.az

[3] Minoli, D. Kouns, J. 2009. *Security in an IPv6 Environment.* CRC Press, USA.

[4] Davies, J. 2008. *Understanding IPv6***.** 2nd edition. Microsoft Press, USA.

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

[6] White Paper, (Published: September 2003 & Updated: January 2008). *Microsoft Windows Server 2008, Introduction to IP Version 6*, Microsoft Corporation, USA.

[7] White paper 2004. *IPv6 and IPv4 Threat Comparison and Best Practice Evaluation(v1.0)* , Cisco Press, USA.

[8] Szigeti, S.; Risztics, P. 2004. *Will IPv6 bring better security?. Proceedings 30th Euromicro Conference*, vol., 532- 537, 31 Aug.-3 Sept.

[9] Sotillo, S. 2006. *IPv6 Security Issues***.** East Carolina University, USA.

[10] Choudhary, A. R. Sekelsky, A. 2010. *Securing IPv6 Network Infrastructure: a New Security Model*. *IEEE Conference*, USA.

[11] Blanchet, M. 2006. Migrating to IPv6. *John Wiley & Sons Ltd, England.*

[12] Hagen, S. 2006. *IPv6 Essentials*, 2nd edition. O'Reilly Media.

[13] Popoviciu, C. Abegnoli, E. L. Grossetete, P. 2006. *Deploying IPv6 Networks*. Cisco Press, USA.

[14] Karlsson, B. 2003. *Cisco Self-Study: Implementing IPv6Networks (IPV6).* Cisco Press, USA.

[15] Li, Q. Jinmei, T. Shima, K. 2009. *Mobile IPv6: Protocols and Implementation*, Elsevier Inc. USA.

[16] Hauser, V. 2008. *Attacking the IPv6 Protocol Suite*, TheHacker's Choice, http://www.thc.org/thc-ipv6.

[17] Cisco IOS Learning Services. 2002. *The ABCs of IP Version* 6, Cisco Press, http://www.cisco.com/go/abc**.** White Paper, October 2011, *IPv6 Security Brief*, CiscoPress.

[18] Yoo, H. S. Cagalaban, G. A. Kim, S. H. 2009, *A Study on the Connectivity of IPv6 to IPv4 Domains and Its Security Issues*, International Journal of Advanced Science and Technology, Vol. 10, Korea.

[19] Merike, K. Green D. Bound, J. and Pouffary, Y. July 2006. *IPv6 Security Technology Paper.* North American IPv6 Task Force (NAv6TF) Technology

[20] O'Reilly Media, "**IPv6 Essentials**," July 2002

8 AUTHORS

Varsha Alangar is currently pursuing her B.E in Computer Science Engineering at Meenakshi Sundararajan Engineering College which is affiliated to the Anna University of Chennai, Tamil Nadu, India. She has presented several papers on networking including "Resource allocation in Wireless Mesh networks" and other papers related to Operating systems and Cloud computing . She will intern at University Sains Malaysia for her final year project where she will be working on IPv6 and its related security issues.

Anusha Swaminathan is also pursuing her B.E in Computer Science Engineering at Meenakshi Sundararajan Engineering College which is affiliated to the Anna University of Chennai, Tamil Nadu, India. She has presented several papers and also won many accolades for the same. She specializes in Algorithms and programming. She will also intern at University Sains Malaysia for her final year project where she will be working on IPv6 and its related security issues.