Security issues in IPv6

R Radhakrishnan
KIET, Ghaziabad, UP,India
radhakrishnan@kiet.edu

Majid Jamil
Jamia Millia Islamia, New Delhi , India
majidjamil@hotmail.com

Shabana Mehfuz
Jamia Millia Islamia, New Delhi , India
mehfuz_shabana@yahoo.com

Moinuddin
NIT Jalandhar,
Prof_Moinuddin@yahoo.com

Abstract

The current generation of IP, version 4 (IPv4), has been in use for more than 20 years, since its inception in 1980 and has supported the Internet's rapid growth during that time. IPv4 has proven to be robust, easily implemented and interoperable. This is a tribute to its initial design. However, the current Internet has grown much bigger than was anticipated. There are several problems such as impending exhaustion of the IPv4 address space, configuration complexities, and poor security at the IP level and inadequate QoS support for real-time delivery of data. To address these and other concerns, the Internet Engineering Task Force (IETF) has developed a suite of protocols and standards known as IP version 6 (IPv6). The new features introduced such as Auto-address configuration, End to End connectivity, mandatory support for security and mobility pose a great challenge on security for future networks based on IPv6. This paper identifies and examines security threats relating to the new features introduced in IPv6.

Key words: IPv6, TCP/IP, NAT, IPSec, IKE, CGA, PKI

1. Introduction

Industry stakeholders and Internet experts generally agree that IPv6-based networks would be technically superior to the commonly installed base of IPv4-based networks [1]. The vastly increased IP address space available under IPv6 could potentially stimulate a plethora of new innovative communications services. The potential development of new classes of networked applications (*e.g.,* widely available networked computing in the home, the office, and industrial devices for monitoring, control, and repair) could result in rapid increases in demand for global IP addresses [2].

Over time, IPv6 could become (as compared to IPv4) a more useful, more flexible mechanism for providing user communications on an end-to-end basis. The redesigned header structure in IPv6 and the enhanced capabilities of the new protocol could also simplify the configuration, and operation of certain networks and services. These enhancements could produce operations and management cost savings for network administrators. In addition, auto-configuration and mobility features of IPv6 could make it easier to connect computers to the Internet and simplify network access for mobile Internet users. However, along with the new features are also new security concerns, which need to be addressed. There are many groups world over, studying the security holes in IPv6. These security threats relating to new features of IPv6 goals are discussed in following sections. The security implications of new features of IPv6 are examined along with other legacy threats encountered in present IPv4 based inter-network.

In section 2, important features introduced in IPv6 are outlined. In sections 3, these features are discussed along with the emerging security issues and current work, if any, to handle the threats. Section 4 outlines threats, which are common with IPv4. Finally the document is summarized with the features of IPv6, which require strengthening for security.

Third International Conference on Networking and Services(ICNS'07)
0-7695-2858-9/07 $20.00 © 2007 IEEE

2. Important features introduced in IPv6

The problem of addressing was the main motivation for creating IPv6. However this is not the only change made in IP and the protocol has been updated in a number of other respects as well, to ensure its viability. Some of the important features of IPv6 are outlined below [3]: -

2.1 Larger Address Space

IPv6 has 128-bit (16-byte) source and destination IP addresses compared to 32 bit for IPv4. IPv6 thus provides 3.4 x 1038 addresses compared to 2.94 x 109 provided by IPv4. Over 1027 globally unique addresses to every individual on the earth in the year 2050 can be made available by the increased address apace.

2.2 Better Management of Address Space

It was desired that IPv6 not only include more addresses, but also for efficient routing in our current Internet and with the flexibility for the future with a more capable way of dividing the address space and provide better support for multicasting.

2.3 Elimination of "Addressing Kludges"

Technologies like NAT are effectively "kludges" that make up for the lack of address space in IPv4. IPv6 eliminates the need for NAT and similar work-around, allowing every TCP/IP device to have a public address.

2.4 Easier TCP/IP Administration

The designers of IPv6 hoped to resolve the difficulties in configuring IP addresses in IPv4. Even though tools like DHCP eliminate the need to manually configure many hosts, it only partially solves the problem. Neighbor discovery protocols allow an IPv6 node to engage in stateless auto address configuration.

2.5 Better Support for Security

IPv4 was designed at a time when security wasn't much of an issue. But today, security on the public Internet is a big issue, and the future success of the Internet requires that security concerns be resolved. IPSec is a mandatory feature in IPv6.

2.6 Better Support for Mobility

When IPv4 was created, there really was no concept of mobile IP devices. The problems associated with computers that move between networks led to the need for Mobile IP. IPv6 builds on Mobile IP and provides mobility support within IP itself.

3. Security issues relating to features of IPv6

There are great expectations about the features of the IPv6 protocol, one of which is better network security. IPv6 provides network level security via IPSec. While this is an obvious improvement in security, its universal usability is still questionable. Other features outlined above also open up windows of new threats. Following sections discuss in detail the features and security issues arising due to them.

3.1 Larger Address Space

In the late 1970s when the IPv4 address space was designed, it was unimaginable that it could be exhausted. However, due to changes in technology and an allocation practice that did not anticipate the recent explosion of hosts on the Internet, it was clear by 1992 itself that a replacement for IPv4 would be necessary. The 128-bit address will solve address space problem for at least next 50 years even with the present explosive growth of Internet.

First category of security attack relating to address is Reconnaissance [4], by which an adversary attempts to learn as much as possible about the victim network. Reconnaissance is carried out by Ping sweeps and Port scans. While this is relatively easier in the case of IPv4 where the number of subnet addresses are in the range of hundreds or thousands, the task is made very difficult in the case of IPv6 since the subnet addresses on which scan are to be carried out are of the order 2^{64}. For example, if the scanning rate were one million addresses per second, for an adversary it would take more than 500,000 years to scan the subnet. Hence the larger address space is a deterrent for reconnaissance. Large address space can make the work of an intruder hard; it may interfere with countermeasures.

Security scanners and IDS tools can suffer from this problem. Hence, large address range may also make detection of rogue hosts difficult [5].

3.2 Better Management of Address Space

The relatively large size of the IPv6 address is designed to be subdivided into hierarchical routing domains that reflect the topology of the modern-day Internet. The use of 128 bits allows for multiple levels of hierarchy and flexibility in designing hierarchical addressing and routing that is currently lacking on the IPv4-based Internet [6]. An IPv6 host and router can have multiple unicast and multicast addresses. When the use of these address ranges is combined with the routing system, the network designer can limit access to IPv6 end nodes through IPv6 addressing and routing. For instance, the network designer can assign global unicast addresses only to devices that need to communicate with the global Internet while assigning site-local addresses to devices that need to communicate only within the organization. Likewise, if a device needs to communicate only within a particular subnet, only the link-local address is needed. Additionally, the use of IPv6 privacy extensions also becomes a limiting factor for any single IPv6 address to be accessible and exposed to a security threat [4].

IPv6 supports new multicast addresses that can enable an adversary to identify key resources on a network and then attack them. These addresses have a node, link, or site-specific domain of use as defined in RFC 2375 [7]. For example, all routers (FF05::2) and all DHCP servers (FF05::3) have a site-specific address. Although this setup clearly has a legitimate use, it is in effect handing the adversary an official list of systems to further attack with simple flooding attacks or something more sophisticated designed to subvert the device.

3.3 Elimination of NAT

When IPv4 addresses were allocated for the Internet it was carried out in such a manner that North America had enough, while Europe and Asia had less addresses. When the address shortage was realized a workaround called Network Address Translation (NAT) was defined in which NAT gateways would modify the addresses in packets and thus be able to hide a network behind a single official address. While NATs promote reuse of the private address space, they do not support standards-based network layer security [8].

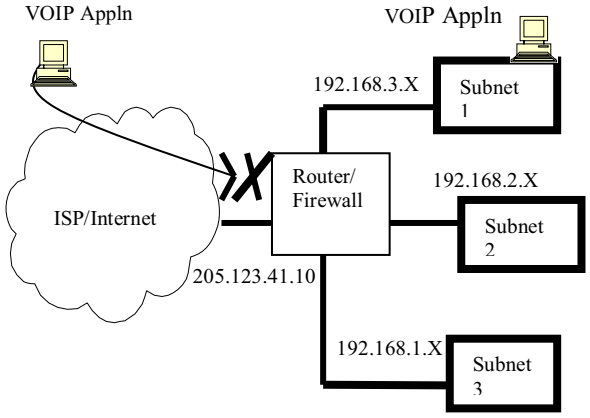

Figure 1. NAT

NAT breaks end-to-end connectivity, so it has drawbacks. As shown In figure 1, VOIP application between two private addresses cannot take place [9]. The operation of NAT has the security byproduct of hiding the internal network and preventing connection attempts from outside. This is also considered as an advantage of NAT.

IPv6 does not support NAT. IPv6 with this large 128 bit address space IPv6 can offer end-to-end (E2E) connectivity to all hosts. Though this feature is a boon it is also a bane at the same time from security point of view. The present internet makes use of NAT which provides a single point entry into networks and security mechanisms such as Firewalls can be set up at entry, as shown in figure 1. Firewalls protect a not-so-secure point inside a perimeter from the rest of the (big bad) world. Firewalls enforce uniform policy at perimeter, stop outsiders from performing dangerous operations and provide a choke point which is scalable and with centralized control. End-to-end connectivity, tunneling, and encryption may conflict with this policy. Traffic that cannot be checked at the firewall can bring unpleasant things to desktops in the network. With E2E connectivity, there will be no such entry point security and the onus of security will lie with the hosts. All hosts may not have the required computing resources for providing security.

3.4 Easier TCP/IP Administration

With IPv6, ARP is gone, and stateless auto-configuration as well as Neighbor Discovery is built into ICMPv6. The purpose of IPv6 Neighbor Discovery (ND) [10] is to provide IPv6 nodes with a means to discover the presence and link-layer addresses of the other nodes on the local link. Additionally, it provides methods for discovering routers on the local link, for detecting when a local node becomes unreachable, for resolving duplicate addresses, and for routers to inform nodes when another router is more appropriate (redirect).

Neighbor Discovery starts with a Neighbor Solicitation (NS) multicast query to which anyone can respond by Neighbor Advertisement (NA), as shown in figure 2. A rogue node can send NA and cause failure of ND. ND can be attacked in various ways by forging ND packets. These packets can interfere with neighbor discovery, resulting in causing unreachability for certain nodes. Fake reply to duplicate address detection(DAD) can result in failed DAD, and as a result, failed auto-configuration. Spoofed router advertisements can divert traffic to the attacker to perform man-in-the-middle, etc, attacks, or to another host, resulting in denial of service by flooding with

Auto-Configuration allows any rogue host to get an IPv6 address without authentication or administrative configuration, thereby, providing IPv6 access to any system with physical network access [11]. The security implications of this are serious because sometimes just getting on a LAN implies certain privileges, e.g., access to certain proprietary applications.

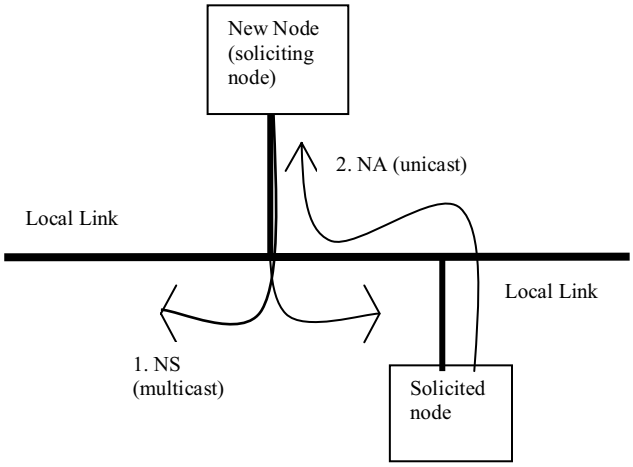

Fig 2. NS and NA messages

The original ND protocol specifications called for the use of IPSec to protect NDP messages. However, the RFCs do not give detailed instructions for using IPsec to do this. There is no simple mechanism for determining which neighbors are authorized to respond.

However, the way ND operates; these attacks may only be performed by nodes on the same network segment, which mitigates their effect. Operators of such networks, where nodes are not trusted, should apply some kind of protection against these attacks. There are currently schemes such as Secure ND (SeND) [12] which describe a methodology to counter the threats to ND.

3.5 Better Support for Security

IPSec [13] is mandatory for IPv6 and it is definitely a security enhancement in IPv6. IPSec provides IP level authentication of the packets and encryption of individual packets or traffic. The cryptography algorithms may be used in a plug-in fashion in the IPSec framework. Current IPSec implementations are better suited for tunnel mode operation (such as VPN) than for arbitrary end-to-end communication [5]. The main reason behind this is the problem of key management. Traffic protection with AH [14] or ESP[15] is not too useful without key management. Manual key distribution does not scale well, so an automated system, i.e., IKE [16], is needed. IKE has limitations [17] in that it is, as of now, a unicast UDP protocol. IKE is not useful when the messages address ranges include multicast and anycast.

We note that, in fact, the IPv6 RFCs say to use IPSec AH to protect ICMPv6. The question is, “How?” To use IPSec one needs a Security Association, which depends on the address learned through Neighbor Discovery, security keys, a lifetime, and so forth. If Security Associations are pre-established, how many are needed? The bigger questions can be phrased as, “If one already has IPSec set up, why is discovery needed?” or “How can a Security Association be pre-established to communicate

securely with someone one still needs to discover?" So the reasoning is circular.

3.6 Better Support For Mobility

IPv6 mobility feature allows a mobile node to keep the same IP address visibility even when moved to a foreign network. This feature is integrated in IPv6.

Mobility is a complex function of IPv6, involving several entities (mobile host, home agent etc.)[18]. Even the normal operation of mobility raises several security questions, such as authentication and authorization of the mobile host in a foreign network. Because mobility uses option headers to store the "real" address of a mobile host, while using the "mobile" address in the IPv6 header, it may be involved in address spoofing attacks. By supplying false information to the home agent, legitimate traffic may be diverted.

IPSec puts a secure pipe between two secure points. It is hard for a firewall between networks to do its job if it does not understand the application or cannot parse the payload.

4. Security threats common to IPv4 and IPv6

This section outlines attacks that are not altered by new features of IPv6 [4]:

- Sniffing
- Application layer attacks
- Rogue devices
- Man-in-the-middle attacks
- Flooding

IPv6 provides fundamental technology to prevent sniffing with IPSec, but until the key management issues (among others) are resolved, deployment of IPSec will be stalled and sniffing attacks will continue to be possible.

Both IPv4 and IPv6 are vulnerable to application attacks. If host to host traffic is secured using IPSec, firewalls or IDS cannot provide security when it sees encrypted traffic. All security protections will be responsibility of the hosts.

An adversary would be a rogue wireless access point, DHCP or DNS server, router, or switch. These attacks are fairly common in IPv4 networks and are not substantially changed in IPv6. If IPSec were ever used in a more comprehensive way in the IPv6 protocol (including device bootstrap), authentication for devices could mitigate this attack.

IPv6 falls prey to the same security risks posed by a man in the middle attacking the IPSec protocol suite, specifically IKE, as in the case for IPv4. There are tools that can attack an IKE aggressive mode negotiation and derive a pre-shared key.

IPv6 network is equally vulnerable as IPv4 network for DoS attacks. Though certainly the increase in IP addresses that can be spoofed may make flooding attacks more difficult to trace, the core principles of a flooding attack remain the same in IPv6.

5. Summary

To summarize, IPv6 has several new features that have an effect on network security. IPv6 does not provide radically new security measures, but there are small improvements, that, if used appropriately, can change the security in a positive way. Because IPv6 is still at the very early stages on introduction, it is still too early to tell, if IPv6, just by itself will enhance IP security. The IETF is still working on IPv6 security for ICMPv6, IPv6 firewalls, mobility, transition, etc. On the long term we expect IPv6 to have an overall better security then IPv4 has.

6. References

[1] IPv6 on everything: 3G Mobile Communication Technologies, 2001. Second International Conference on (Conf. Publ. No. 477) 26-28 March 2001 Pages:317 – 322

[2] IPv6 Tutorial. Florent Parent, Régis Desmeuleshttp://www.viagenie.qc.ca13 march 2000

[3] Introduction to IP Version 6. Microsoft Corporation Published: September 2003 Updated: March 2004

[4] IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0) Sean Convery (sean@cisco.com),Darrin Miller (dmiller@cisco.com) presentation at the 17th NANOG, May 24, 2004

[5] Will IPv6 Bring Better Security? Szabolcs Szigeti, Dr. Péter Risztics Proceedings of the 30th EUROMICRO Conference (EUROMICRO'04) IEEE computer society
[6] Internet Protocol Version 6 (IPv6) Addressing Architecture, R. Hinden Nokia, S. Deering Cisco Systems, April 2003. Request for Comments: 3513.
[7] R Hinden, S Deering, "IPv6 Multicast Address Assignments" (July 1998), RFC 2375 at http://www.ietf.org/rfc/rfc2375.txt
[8] NAv6TF Response NTIA IPv6 RFC Jim Bound and Latif Ladid 1 march 2004
[9] IPv6 Security from point of view firewalls, Janos Mohácsi 09/June/2004, Information societ technologies, 6net.
[10] Neighbor Discovery for IPv6 [RFC-2461]
[11] A secure and efficient solution to the IPv6 address ownership problem.Steffano M.Faccin and Franck Lee, IEEE 2000
[12] [RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "Secure Neighbor Discovery (SEND)",RFC 3971, March 2005.
[13] Security Architecture for the Internet Protocol [RFC-2401]
[14] IP Authentication Header [RFC-2402]
[15] IP Encapsulating Security Payload (ESP) [RFC-2406].
[16] The Internet Key Exchange (IKE), D. Harkins, D. Carrel, cisco Systems November 1998 Request for Comments: 2409.
[17] Security with IPv6 explored. Richard Graveman – RFG Security Renée Esposito – B | A | H North American IPv6 task force. Dec 2003
[18] "Inter-domain security in Mobile IPv6" by Maryline Laurent-Maknavicius, Francis Dupont, IEEE 2000