Information **S**ecurity **S**olutions **E**urope, 7-9 Oktober 2003 Vienna Austria, Franjo Majstor, Cisco Systems, Inc.

Does IPv6 protocol solve all security problems of IPv4?

Franjo Majstor
Cisco Systems, Inc.
franjo.majstor@cisco.com

Abstract

Network security specialists familiar with IPv4 protocol would gladly hope that the IPv6 protocol would easily solve the security problems we are having today in networks based on the IPv4 protocol. Well, the truth is as always somewhere in between. IP Security protocol or shortly IPsec, is the protocol which was developed for IPv6 protocol and is certainly adding significant level of security to it, but isn't solving all existing network security problems and it is at the same time with its flexibility introducing some new ones. Mobile IP protocol is built in the IPv6 protocol, however security solutions for it are still under development. Dynamic configuration flexibility of IPv6 is, if not properly used, enemy of it as well. This paper is after quick primer of the IPv6 protocol, listing and explaining few security issues to which we are exposed in IPv6 network environments.

Keywords: Network security, IPv6, IPsec, neighbor discovery, authentication, mobility

1. Introduction

Internet protocol version four or shortly IPv4, which was developed almost about three decades ago, is the most dominant communication protocol used in any data network today. It evolved out of the Defense Advance Research Project Agency (DARPA) project which had a major goal of survivability of the network connectivity. In its origin, the IPv4 protocol was used in a trusted closed environment and as such didn’t require any security mechanisms for protecting hosts or network elements from external hostile attacks or attacks to the hosts from each other. Throughout the history, growth and commercialization of the global network best known today as the Internet, the IPv4 protocol became the most popular protocol used in the open, non trusted, unsecured, external network environments as well, including all of its inherited flexibility and insecurity as it was initially developed. In parallel with the exponential growth of the Internet based on the IPv4 protocol, there was a foreseen problem of the luck of address space for the all possible devices and services which could potentially connected to it, which has initiated the development of the new modernized communication protocol, today known as Internet Protocol version six or shortly IPv6 [3,4]. IPv6, as the follow up protocol to IPv4, has addressed several missing points of the IPv4 protocol. One of them is certainly the security aspect of the protocol.

2. Quick primer of the IPv6 protocol

The features which IPv6 protocol brings to plate are described in several RFCs (Request for Comments) and Intermet drafts could be summarized as follows:

- New header format
- Large address space
- Efficient and hierarchical addressing and routing infrastructure
- Stateless and stateful address configuration
- Security
- Better Quality of Service (QoS) support
- New protocol for neighboring node interaction
- Extensibility

The IPv6 header has a new format that is designed to minimize header overhead. The IPv6 header is only twice the size of the IPv4 header, even though the number of bits in IPv6 addresses is four times larger than IPv4 addresses.This is achieved by moving both nonessential and optional fields to extension headers that are placed after the IPv6 header. Therefor is the streamlined IPv6 header more efficiently processed at intermediate routers. Differences between IPv4 and IPv6 protocol headers are illustrated in Figure 1.

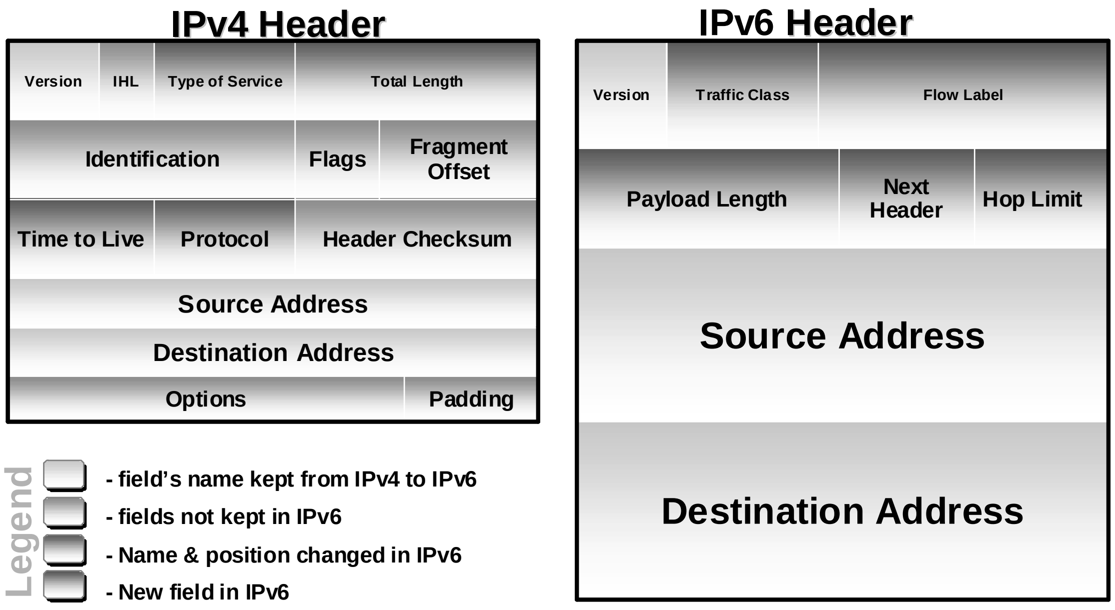

Figure 1: IPv4 and IPv6 header fields compared

3. Security mechanisms built into the IPv6 protocol

IPv6, as the follow up protocol to IPv4 has addressed several missing points of the IPv4 protocol. One of them is the security aspect of the protocol. Security features which are developed for IPv6 are known under the name of IP Security or shortly IPsec. IPsec is today most commonly used in IPv4, where it is optional, while it is mandatory to use it in the IPv6 protocol. IPsec consists of enhancements to original IP protocol which provide authenticity, integrity, confidentiality and access control to each IP packet through usage of the two new headers: AH (authentication header) and ESP (Encapsulations Security Payload) as it is illustrated on the Figure 2:

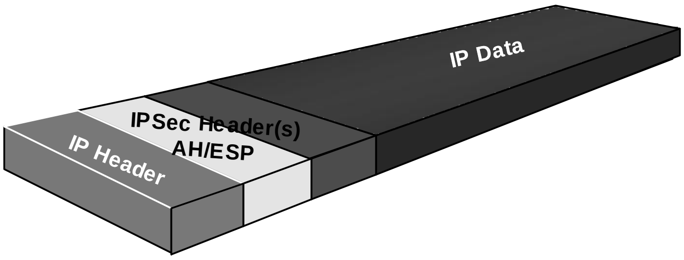

Figure 2. AH and ESP headers in IPv4 and IPv6 protocols

IPsec is, if properly used, certainly changing security paradigm of IP (v4 and v6) communications and is very well known and interoperable in multiple vendor implementations so far, however it is not the topic of this paper.

4. Security exposures in IPv6 protocol and comparison to IPv4

One of the greatest flexibilities of the IPv4 protocol is that its layer two (L2) address is not statically bound to the layer three (L3), IP address, hence it could run easily on top of any layer two media without significant changes in the protocol. Connection between the L2 and L3 address is established with a protocol named Address Resolution Protocol (ARP) which is dynamically establishing mapping between the L2 and L3 addresses on the local network segment. ARP protocol has its own security exposures, but as it is tight to IPv4 protocol only, it is out of the scope of this paper. In IPv6 protocol, there is no need for ARP protocol because the interface identifier (ID) portion of L3 IPv6 address is directly derived from device L2 address [7]. The L3 IPv6 address together with its locally derived interface ID portion is than used on the global level in the whole IPv6 network. Due to that we have the following security considerations.

4.1 Privacy and duplicate IP address detection

First security consideration with L3 addressing in IPv6 is concerning privacy. Each of the devices in the network which is using IPv6 protocol instead of IPv4 could be uniquely traced by using ID portion of its IPv6 address [5]. Secondly, duplicate address detection (DAD) in IPv4 as well as IPv6 has no real good security protection mechanism for assuring the service to particular device with a duplicate IP address. The privacy problem within IPv6 protocol has luckily been taken care of in time of the protocol development and is resolved by the usage of temporarily assigned randomly generated interface ID to provide certain level of anonymity. So IPv6 device privacy problem if properely implemented, used and configured is solved by privacy extensions for stateless address autoconfiguration in the IPv6 protocol.

The problem of duplicate addressing, unfortunatelly has not changed much from IPv4 to IPv6 world. In the IPv4 world there is simple no standardized mechanism for detecting and reacting at the moment of duplicate address appearance on the network segment, but it is rather left to a particular device or IP stack implementation how to handle it. In the IPv6 world the problem is more serious, as the interface ID portion of the L3 IPv6 address is directly derived from L2 device address. Within RFC 2462 it is defined that if during the neighbour discovery process IPv6 device which received response that some other particluar device is already using its proposed address - it ***must not*** use it. It is fairly easy for a mallicious user to craft the address which already exists on the local segement and hence achieve Denial of Service (DoS) attack on particlaur IPv6 device trying to initally obtain the statless IPv6 address and start the IPv6 communication.

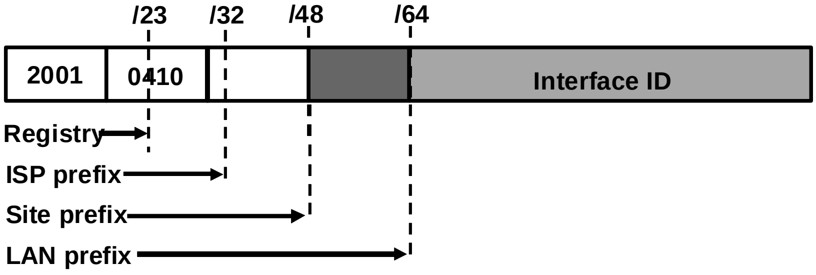

Figure 3. IPv6 address format

4.2 Neighbor discovery and router solicitation

Neighbor discovery and stateless address auto configuration are yet two other powerful flexibilities in the world of IPv6 protocol [1]. However flexibility and security are just the opposite requirements. The neighbor discovery as well as the router solicitation in the IP network (v4 or v6) is using the Internet Control Messaging Protocol (ICMP). While the ICMPv4 is a separate protocol on a side of IPv4, the ICMPv6 is the protocol which runs directly on the top of the IPv6 protocol, which might cause a security problem. As you might guess, depending on the practical implementations of the IPv6 protocol stacks, it actually does. Exchanging the ICMPv6 messages on the top of the IPv6 protocol for the vital “network health” messages and environment solicitations are crucial for IPv6 communication. However it could also be abused with sending the fake, crafted response messages for the purpose of the denial of service, traffic re-routing or any other malicious purpose. For security reasons, the IPv6 protocol definition recommends that all ICMP messages use the IPsec AH (Authentication Header) and its functionality of integrity, authentication and anti-replay. Unfortunately in practice and early commercial implementations we do face that very few IPv6 implementations support IPsec or support it in very limited fashion, which opens the ICMPv6 messages to potential security attacks.

4.3 Header extensions

IPv6 header is simpler compared to IPv4 header as we have seen briefly in the IPv6 primer at the beginning. Simplicity is achieved due to additional header chaining which allows routing devices to process only IPv6 header while the other headers are processed only by the end nodes. Examples of chained extension headers are illustrated in Figure 4.

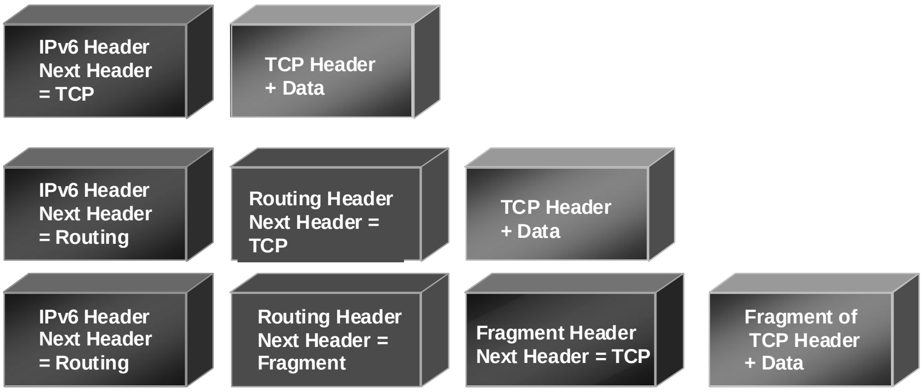

Figure 4. IPv6 Header and Extension Headers

Routing header in IPv6 is comparable to IPv4 source-route option. Source route in the header of the IPv4 packet defines the hop-by-hop path from the source of the packet to the destination of the packet throughout the whole network. Source-routing is from the security perspective very unwelcome feature in IPv4 networks, as it could be abused for spoofing attack and hence has to be used with care or disabled on the portions of the network where it is not needed. In the IPv6 world there is no source-routing option in the IP header. This functionality is instead achieved with a routing header, with the same security consequence, however it couldn’t be always easily turned off or filtered. If there is a need for using mobile IP (MIP) functionality within the IPv6 network, than the routing header must be used. While some more detailed description of the MIP is following later, it is important to mention here that MIP is natively build into IPv6 protocol stack and it requires routing header to work.

4.4 Mobile IPv6

Main goal of the mobile IP protocol (MIP) is to maintain the IP address of the node while roaming through the different network segments [4]. MIP consists of several elements and tunneling mechanism to achieve IP roaming functionality. In the IPv4 protocol there are Home Agent (HA) and a Foreign Agent (FA), while in the IPv6 world, MIP concept requires only HA, while the FA role is natively built in to a plain IPv6 router on the foreign link. In both versions of the MIP protocol (v4 and v6) there are strong security requirements for tunnel authentication and optional tunnel confidentiality of the re-routed traffic from the mobile device to its home network. Most of the security requirements could be achieved by applying IPsec AH and ESP headers, however industry standardization body (IETF) is still deciding of how to use it [2].

4.5 Dual stacks

IPv4 headers and IPv6 headers are not interoperable. IPv6 is not a superset of functionality that is backward compatible with IPv4 but rather a new protocol with its own specific requirements for filtering at the perimeter of the network. This opens the whole new area of the statefull perimeter security for the native IPv6 communication. In the transition towards the complete native IPv6 networks there will be a period where devices on the network will need to run both IPv4 and IPv6 protocols and process or recognize both header formats. This mixed environments would certailny be just another area where devices would be exposed to bothe IPv4 as well as IPv6 protocol security issues.

5. Conclusion

It is obvious and easy to say that two decades younger protocol, IPv6 is bringing security enhancements into a modern IP network. It brings a lot of flexibility which also opens the security problems. IPv6 mandates usage of the IPsec protocol and also has flexible extension header options. In practice that could help, however does not solve all the security problems for the all requirements. This paper has exposed just a few of them. As security is a journey and not a destination, it is also yet to be seen what are the additional security exposures we could have in the IPv6 based network environment.

References

[1] Arko J., and others, Secure Neighbor Discovery, <*www.ietf.org/internet-drafts/draft-ietf-send-ipsec-00.txt*>, IETF draft, February 2003

[2] Johnson, D., Perkins, C., Arko J.,, Mobility Support in IPv6, <*www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-21.txt*>, IETF draft, February 2003

[3] Brown S., and others, Configuring IPv6 for Cisco IOS, Syngress Publishing, Inc 2002

[4] Davies J., Understanding IPv6, Microsoft Press 2003

[5] Narten, T., Draves, R., Privacy Extensions for Stateless Address Autoconfiguration in IPv6, IETF RFC 3041 standard, January 2001.

[6] Solomon, D. J. Mobile IP, The Internet Unplugged, PTR Prentice Hall, 1998.

[7] Tomson, S., Narten, T., IPv6 Stateless Address Autoconfiguration, IETF RFC 2462 standard, December 1998.

Speaker Biography:

Franjo Majstor holds an University Graduate Engineering degree from Faculty of Electrical Engineering at University of Zagreb, Croatia and Master of Science degree from Faculty of Computer Sciences at KUL University of Leuven, Belgium, obtained in 1989 and

2002 respectively. He started his industry career back in 1990 in Ljubljana, Slovenia, joined Cisco Systems in 1995 in Brussels Belgium, where he is currently working as a senior consulting engineer, focusing on security related products, feature and solutions across technologies. He is involved as a trusted adviser in designs of security related projects in Europe, Middle East and Africa. He holds a CISSP and CCIE industry certifications and is a member of several professional associations: CSI, ISSA, IEEE and IETF. He is a frequent speaker on security topics at public technical conferences around a world.