Available online at www.sciencedirect.com

ScienceDirect

Procedia Social and Behavioral Sciences 2 (2010) 5285–5291

Procedia
Social and Behavioral Sciences

WCES-2010

IPV4/IPV6 security and threat comparisons

Emre Durdağı[a], Ali Buldu[b] *

[a] *Technical Education Faculty, Marmara Üniversity, İstanbul, 34722, Turkey*

Received November 15, 2009; revised December 3, 2009; accepted January 25, 2010

Abstract

Internet using is increasing rapidly. İnternet occured as a result of commincating nodes with each. New internet users are joining to this structure and development of it is going on. In such a big structure, communication of two nodes is possible only if they find each other. Various addressing protocols have been developed to obtain this. The well-known is called Internet Protocol (IP). Currently IP is used IP Version 4 (Ipv4).Ipv4 has limited address. This limited addresses does not meet the growth of internet.Because of inadequate internet address, IP Version 6 (IPV6) was developed in 1995. Ipv6 brings many enhancement. Ipv6 was designed with security in mind. It is bringing security enhancments into modern IP network. This paper analyses Ipv6 and Ipv4 Threat Comparisons on two stage. First part focuses on the attacks with Ipv4 and Ipv6 similarities.Second part is focuses on the attacks with new considirations in Ipv6.

Keywords: IPv6; IPv4; IP security; Ipv6 security performance; IP threats; IP attacks; security comparision

1. Introduction

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

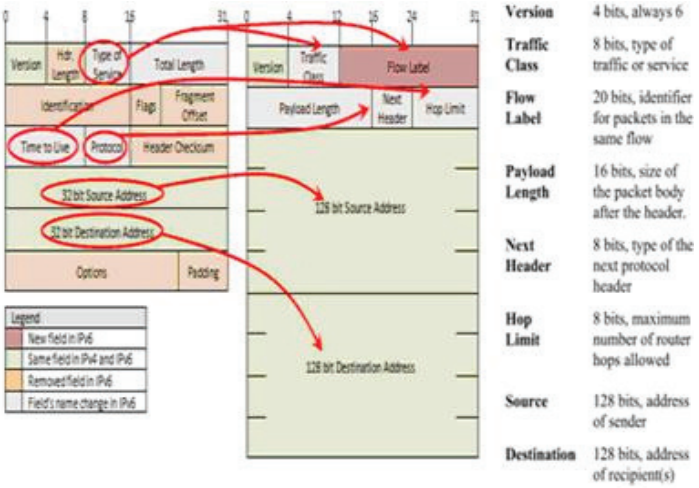
Restrictions parameters (IETF RFC 791, 1981) Aware of the limitations of the current Internet infrastructure, which is based on the Internet Protocol version 4 (IPv4) suite of protocols, the Network Working Group of the Internet Engineering Task Force (IETF) proposed a new suite of protocols called the Internet Protocol version 6 (IPv6). As a result of this, the IETF has been working on the IPv6 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 2460 (Deering & Hinden, 1998). IPv6 Protocol, RFC4861 (Narten et al., 2007) IPv6 Neighbour Discovery, RFC 4862 (Thomson, Narten, & Jinmei, 2007) IPv6 Stateless Address Auto-Configuration, RFC 4443 (Conta, Deering & Gupta, 2006) Internet Control Message Protocol for IPv6 (ICMPv6), RFC 4291(Hinden & Deering, 2006) IPv6

* Ali Buldu. Tel.: +90-216-336-5770; fax: +90-216-337-8987
E-mail address: alibuldu@marmara.edu.tr

1877-0428 © 2010 Published by Elsevier Ltd.
doi:10.1016/j.sbspro.2010.03.862

Addressing Architecture, and RFC 4301 (Kent & Seo, 2005) Security Architecture for IP or IPsec. IPv6 is also referred as the Next Generation Internet Protocol (IPng). The differences between IPv6 and IPv4 headers are outlined in the tables below:

Features	IPv4	IPv6
Address	32 bits	128 bits
Checksum in header	Included	No checksum
Header includes options	Required	Moved to IPv6 extension headers
Quality of Services (QoS)	Differentiated Services	Use traffic classes & flow labels
Fragmentation	Done by routers & source node	Only by the source node.
IP configuration	Manually or DHCP	Auto-configuration or DHCP
IPSec support	Optional	Required
Unicast, multicast and broadcast	Use all	Uses unicast, multicast and anycast
Address Resolution Protocol (ARP)	Use to resolve an IPv4 address	replaced by Neighbor Discovery
Internet Group Management Protocol (IGMP)	Use to manage local subnet group.	Replaced with Multicast Listener Discovery (MLD)
Domain Name System (DNS)	Use host address (A) resource records	Use host address (AAAA) resource records
Mobility	Use Mobile IPv4 (MIPv4)	MIPv6 with faster handover, routing and hierarchical mobility



Figüre 1. Comparing Ipv4 and Ipv6

2. Differences between Ipv6 and Ipv4

2.1. Address

Instead of allowing for only 32-bit IP, IPv6 allows for 128-bit IP.With the increased IP address size, up to 2128 or 3.4 x 1038 different IP addresses can be defined. Multicast addresses Increased use of efficient one-to-many communications. Anycast addresses Redundant services using nonunique addresses.

2.2. The IPv6 Header

The IPv6 header itself is always exactly 40 bytes, and contains exactly 8 fields. Unlike the IPv4 header, the IPv6 header cannot vary in size. The figure below shows the header and explains each of the fields, for details consult RFC 2460 (Deering & Hinden, 1998). The checksum field was simply dropped; all checksum computations in IPv6 must be carried out by upper-layer protocols like TCP and UDP. The fragment fields which appear in the IPv4 header were dropped from the main IPv6 header. Fragment information was relegated to an extension header. Also, IPv6 routers are not allowed to fragment packets they forward; only the original sender of an IPv6 packet is permitted to break the packet into fragments. This has significant implications for network security because ICMP control packets that support path maximum transmission unit (MTU) discovery must be permitted through all IPv6 networks (Ziring, 2006). The functionality provided by the “Time to Live” field has been replaced with the “Hop Limit” field. The “Protocol” field has been replaced with the “Next Header Type” field. The “Options” field is no longer part of the header as it was in IPv4. Options are specified in the optional IPv6 Extension Headers. The removal of the options field from the header provides for more efficient routing; only the information that is needed by a router needs to be processed (Hermann & Seton, 2002).

2.3. Enhance QoS support

The IPv6 packet header contains fields that facilitate the support for QoS for both differentiated and integrated services (Sotillo, 2006). To provide better support for real-time traffic (e.g. Voice over IP), IPv6 includes “labeled

flows" in its specifications. By means of this mechanism, routers can recognize the end-to-end flow to which transmitted packets belong (Sailan, Hassan, & Patel, 2009).

2.4. Auto configuration

Autoconfiguration is an important feature of IPv6.For devices such as a PC, laptop, PDA, or cell phone using an IP based network, each interface connected to the network must be assigned an IP address. For this task, IPv4 is limited to stateful protocols such as the Dynamic Host Configuration Protocol, which require a server to store a requesting host's configuration information. In addition to supporting stateful autoconfiguration through DHCPv6, IPv6 introduces a simplified stateless autoconfiguration procedure where a node can configure its IP address based only on local information that is without contacting a server (Caicedo, Joshi & Tuladhar, 2009) Stateless auto configuration occurs without the use of DHCP.

2.5. Enhance mobility support

Main goal of the mobile IP protocol (MIP) is to maintain the IP address of the node while roaming through the different network segments (Davies, 2003). Pv6 provides mechanisms that allow mobile nodes to change their locations and addresses without loosing the existing connections through which those nodes are communicating. This service is supported at the Internet level and therefore is fully transparent to upper-layer protocols.

2.6. Native Security

The term IPsec refers to a suite of protocols from the IETF providing network layer encryption and authentication for IP-based networks (Kanda, 2004). The objective of IPsec is to authenticate and/or encrypt all traffic at the IP level (Radwan, 2005). Although IPSec is also available for IPv4 implementations, it is not mandated but optional. Support for IPSec in IPv6 implementations is not an option but a requirement. IPsec is mandated in the protocol (Sotillo, 2006). In IPv4, widely-used NATs, but IPv6 expands address space and making NAT unnecessary. IPv6 is expected to increase the use of IPsec in end-to-end communications.[16,17].In IPv6, IPSec is implemented using the authentication header (AH) and the Encapsulating Security Payload (ESP) extension header. Additionally,
because most security breaches occur at the application level,even the successful deployment of IPsec with IPv6 does not guarantee any additional security for those attacks beyond the valuable ability to determine the source of the attack (Oh et al., 2006).

3. Security threats similar in IPv4 and IPv6 network

Some types of attacks have not fundamentally changed by appearance of the IPv6 protocol. Despite security improvements implemented in the new IPv6 protocol, IPv6 networks are still exposed to different types of attacks. Some vulnerabilities still exist, so there are different attack types that could potentially harm IPv6 networks. Some types of attacks known in IPv4 networks did not fundamentally change by appearance of the new IPv6 protocol. That means that they can affect both IPv4 and IPv6 networks.

3.1. The sniffing attacks

A typical example of an attack that affects both IPv4 and IPv6 network is a sniffi ng attack. The sniffing attack involves capturing of the data being transmitted through the network. In case that confidential data are transmitted in a plaintext protocol, they can easily be compromised by an attacker running sniffing attack. A sniffing attack type can be avoided by a proper use of the IPsec security architecture, which is used in IPv4 as an option and in IPv6 as an obligation.

3.2. Application layer attacks

Application layer attacks are the most common attacks today. Here e.g. belong buffer overflow attacks, web application attacks (e.g. CGI attacks), different types of viruses and worms. Unfortunately, transition to the IPv6 protocol will neither prevent computer systems and networks from these attacks nor alleviate their consequences since both IPv4 and IPv6 are protocols of the network layer and these types of attacks are performed at the application layer of the ISO/OSI network model.

3.3. Flooding attacks

One of the most frequent attack types present in IPv4 networks is a flooding attack. It connotes flooding a network device (e.g. a router) or a host with large amounts of network traffic. A targeted device is unable to process such large amount of network traffic and becomes unavailable or out of service. A flooding attack can be local or a distributed denial of service attack (DoS), when the targeted network device is being flooded by network traffi c from many hosts simultaneously. This type of attack can also affect the IPv6 networks, because the basic principles of the flooding attack remain the same. New types of extension headers in IPv6, new types of ICMPv6 messages and dependence on multicast addresses in IPv6 (e.g. all routers must have site-specific multicast addresses) may provide new ways of misuse in flooding attacks.

3.4. Rogue devices

Rogue devices are devices introduced into the network that are not authorized. Although this could most easily be a simple unauthorized laptop, more interesting for 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 somewhat. The 802.1x standard also has the potential to help here, though an undetected rogue device could funnel 802.1x authentication sequences to a compromised node acting as a AAA server while capturing valid credentials.

3.5. Man-in-the-middle attacks

Because the IPv4 and IPv6 headers have no security mechanisms themselves, each protocol relies on the IPsec protocol suite for security. In this fashion IPv6 falls prey to the same security risks posed by a man in the middle attacking the IPsec protocol suite, specifically IKE. Tools that can attack an IKE aggressive mode negotiation and derive a preshared key are documented. With this in mind, we recommend using IKE main mode negotiations when requiring the use of preshared keys. IKEv2 is expected to address this issue in the future (Convery & Miller, 2004). When a node requires the MAC address of another node B, it sends an NS message to the all-nodes multicast address. An attacker on the same link can see the NS message and reply to it with the corresponding NA message, thereby taking over the intended traffic flow between A and B (Caicedo, Joshi & Tuladhar, 2009).

4. IPv6 specific security threats (Zagar, & Grgic, 2006; Zagar, Grgic & Snjezana, 2007):

4.1. Reconnaissance attacks in IPv6 networks

The first phase of the larger attack is usually a reconnaissance attack. An intruder uses reconnaissance attacks to gather some essential data about the victim network that can be misused later in further attacks. For the reconnaissance attack an intruder can use active methods, such as different scanning techniques, or passive data mining. First, an intruder uses ping probes in order to determine which IP addresses are in use in the victim network. After having found an accessible system, an intruder performs the port scan procedure. The subnet size in the IPv6 networks is much larger than in the IPv4 networks (the default subnet size in IPv6 networks is 64 bits). To perform a scan of the whole subnet an intruder should make 264 probes – so that makes it impossible. Owing to this fact, IPv6 networks are much more resistant to reconnaissance attacks than IPv4 networks. Unfortunately, there are some types

of multicast addresses used in IPv6 networks that can help an intruder to identify and attack some resources in the targeted network.

4.2. Security threats related to IPv6 routing headers

According to IPv6 protocol specification, all IPv6 nodes must be capable of processing routing headers. Unfortunately, routing headers can be used to avoid access controls based on destination addresses. Such behavior can produce some security problems. There is a possibility that an intruder sends a packet to a publicly accessible address with a routing header containing a ‘‘forbidden’’ address (address on the victim network). In that case the publicly accessible host will forward the packet to a destination address stated in the routing header (‘‘forbidden’’ address) even though that destination address is filtered. By spoofing packet source addresses an intruder can easily initiate a denial of service attack by using any publicly accessible host for redirecting attack packets.

4.3. Fragmentation related security threats

According to IPv6 protocol specification, packet fragmentation by intermediary nodes is not allowed. Since in IPv6 networks the usage of the path MTU discovery method (based on ICMPv6 messages) is an obligation, packet fragmentation is possible only at the source node. The minimal recommended MTU size for IPv6 networks is 1280 octets. For security reasons it is highly recommended to discard all fragments with less than 1280 octets unless the packet is the last in the flow. Using fragmentation an intruder can achieve that port numbers are not found in the first fragment and in that way bypass security monitoring devices (which do not reassemble fragments) expecting to find transport layer protocol data in the first fragment. By sending a large number of small fragments an attacker can cause an overload of reconstruction buffers on the target system potentially implying a system to crash (a type of a denial of service attack). To avoid such problems it is a recommended security practice to limit the total number of fragments and their allowed arrival rate.

4.4. Security threats related to ICMPv6 and multicast

In IPv4 networks it was possible to block most of ICMP messages without a direct influence to the proper network functionality. Therefore, blocking ICMP messages was common practice for improving security in IPv4 networks. On the other hand, in IPv6 networks some important mechanisms (e.g. neighbour discovery and path maximum transmission unit discovery mechanisms) are dependent on some types of ICMPv6 messages. Consequently, some ICMPv6 messages must be allowed because of proper network operation (e.g. a ‘‘packet too big’’ message is required for the procedure of path maximum transmission unit discovery or a ‘‘parameter problem’’ message is necessary if an unrecognized option occurs in the IPv6 packet header). ICMPv6 specification also allows an error notification response to be sent to multicast addresses (if a packet was targeted to a multicast address). That fact can be misused by an attacker. By sending a suitable packet to a multicast address an attacker can cause multiple responses targeted at the victim (the spoofed source of the multicast packet).

3.4.1SEND and CGAs

The Secure Neighbor Discovery protocol can counter some of the threats against the ND protocol when IPSec is not used.4,6 SEND uses cryptographically generated addresses to verify the sender’s ownership of a claimed address. CGAs 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 the public key and a node’s address. By default, a SEND-enabled node should use only CGAs for its own addresses. The basic purpose of CGAs is to prevent the stealing or spoofing of existing IPv6 addresses (Caicedo, Joshi Tuladhar, 2009).

4.5. Security issues related to transition mechanisms

Since the transition from the IPv4 to the IPv6 protocol will not be rapid (prior due to enormous size of the global IPv4 network) for a certain period of time both protocols will coexist, and the transition will be gradual. To ensure a smooth transition to a new version of the protocol different transition mechanisms are developed. The most important transition mechanisms are tunnelling and dual-stack configurations (supporting both IPv4 and IPv6 protocols). These transition mechanisms can introduce some new, previously unknown security threats. Thus, it is very important for network designers and administrators to understand security implications of transition mechanisms in order to apply proper security mechanisms, such as firewalls and intrusion detection mechanisms.

5. Conclusions

The IPv6 protocol will replace the IPv4 protocol. Every day the IPv6 protocol becomes more accepted and used throughout the global network. Without doubt, IPv6 represents a considerable improvement if compared to the old IPv4 protocol stack. The new suite of protocols provides innumerable features

that improve both the overall functionality as well as some specific security functions into a modern IP network. It brings a lot of flexibility which also opens the security problems.Despite numerous improvements some potential security problems are still present and require consideration. Certain vulnerabilities and misuse possibilities known in IPv4 networks persist, and some new transition-related and IPv6 specific security issues emerged. Successful solving of these security issues will certainly contribute to wider acceptance and usage of IPv6 protocol. Because of the existence of some security issues in IPv6 networks, it is necessary to undertake all possible steps for achieving the highest possible security level. 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. Although IPv6 offers better security (larger address space and the use of encrypted communication),the protocol also raises new security challenges.It is far from being a panacea. For an improved protection in IPv6 networks it is recommended to implement security mechanisms for packet filtering (firewalls) and intrusion detection. All unneeded services should be filtered at the firewall. Nevertheless, security of IPv6 protocol and IPv6 networks can still be improved, but this fact should not be an obstacle to its acceptance,usage and further development.

References

IETF RFC 791 (September 1981).

Deering, S., & Hinden, R. (December1998). Internet Protocol Version 6 (IPv6) Specification*, IETF RFC 2460*.

Narten, T., Nordmark, E., Simpson, W., & Soliman, H. (September 2007). Neighbor Discovery for IP version 6 (IPv6*),IETF RFC 4861*.

Thomson, S., Narten, T., & Jinmei, T. (September 2007). IPv6 Stateless Address Autoconfiguration, *IETF RFC 4862* .

Conta, A., Deering, S., & Gupta, M. (March 2006). Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*),IETF RFC 4443*.

Hinden, R., & Deering, S. (February 2006). IP Version 6 Addressing Architecture, *, IETF RFC 4291*.

Kent, S., & Seo, K. (December 2005). Security Architecture for the Internet Protocol *, IETF RFC 430*1.

Ziring N. (May 2006). Router Security Configuration Guide Supplement - Security for IPv6 Routers. [Online]. Available: *www.nsa.gov/ia/_files/routers/I33-002R-06.pdf*

Hermann, P.-Seton (2002). Security Features in IPv6. [Online]. Available: *www.sans.org/reading_room/whitepapers/.../security_features_in_ipv6_380*

Sotillo, S. (2006). IPv6 Security Issues. [Online]. Available: *www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf*

Sailan, M.K., Hassan, R., & Patel, A. (2009). A Comparative Review of IPv4 and IPv6 for Research Test Bed. *2009 International Conference on Electrical Engineering and Informatics, Selangor, Malaysia.*

Caicedo, C.E., Joshi, J.B.D., & Tuladhar, S.R.(2009). IPv6 Security Challenge*. Computer,* 42, 36-42.

Davies, J. (2003). Understanding IPv6, *Microsoft Press*.

Kanda, M. (2004). IPsec: a basis for IPv6 security. [Online]. Available*:http://www.ipv6style.jp/en/tech/20040707/index.shtml.*

Radwan, A.M. (2005). Using IPSec in IPv6 Security. [Online]. Available*:http://www.uop.edu.jo/csit2006/vol2%20pdf/pg471.pdf*

Saito, Y. (December 2003). IPv6 and New Security Paradigm. *NTT Communications*, Doc. No. 79

Cisco Systems Report (2004). IPv6 SECURITY Session Sec-2003.

Oh, H., Chae, K., Bang, H., & Na, J. (February 2006). Comparisons analysis of Security Vulnerabilities for Security Enforcement in IPv4/IPv6. *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference* .

Convery, S., & Miller, D. (2004). IPv6 and IPv4 ThreatComparison and Best-Practice Evaluation (v1.0). Cisco Systems. [Online]. Available: *http://seanconvery.com/v6-v4-threats.pdf*

Zagar, D., & Grgic, K. (2006). IPv6 Security Threats and Possible Solutions. *Automation Congress, 2006. WAC '06. World*, 1-7.

Zagar, D., Grgic, K., & Snjezana, R. (2007). Security aspects in IPv6 networks implementation and testing. *Computers and Electrical Engineering*, 4, 425-437.