IPV6 risks and vulnerabilities
Project Report

RP1 Thesis

of

Fred Wieringa
born on the 4th of June 1962 in Amsterdam

February 12, 2012

Supervisors:
Prof. C. de Laat
Mr. R. Visser

University of Amsterdam
Faculty of Natuurwetenschappen, Wiskunde en Informatica
(FNWI)
Institute of System and Network Engineering

Abstract

The last few years worldwide companies started to implement the new Internet Protocol version 6. This paper reviews some of the risks and vulnerabilities associated with the new Internet Protocol version 6, with an emphasis on the vulnerabilities that exist because of the lack of using secure techniques and protocols in combination with IPv6. At the end, it concludes summarizing some of the most common security concerns in the use as a weapon, target or means.

Contents

Chapter 1

Document Information

1.1 Description

This document is the project report for the IPv6 risks and vulnerabilities project. This project has been done as a subproject for National Cyber Security Centre (NCSC) and will be executed as the first research project (RP1) of the System and Network Engineering course.

Chapter 2

Project Information

2.1 Introduction

At the point where Arpanet[1] came with theIPv4 [1] address structure as we know nowadays, it wasn't foreseen that the IPv4 address structure that they come up with would fall short. Due to the rapidly expansion of devices i.e. "wireless devices, IP-telephone etc." that would need IP addressing the IPv4 addresses is almost exhausted. The Internet Engineering Task Force (IETF)[2] realized in 1992 this exhaustion would be imminent and initiated as early as in 1994, the development of a suite of protocols and standards now known as Internet Protocol Version 6 (IPv6) [2]. FOr sure the new IPv6 suite will satisfy the increasingly need of addressing that IPv4 didn't provide. ICANN[3] (Internet Corporation for Assigned Names and Numbers) is responsible for both address systems and has already started to put the IPv6-format on it's root servers to replace the IPv4-standard. Besides the fact that IPv6 will have less boundaries then IPv4, it also will simplify the routing aggregation and automatic address configuration.

2.2 Problem

Because the world starts to adopt IPv6 more and more they will also run into the security problems involved with any type of migration/adaptation. Ofcourse IPv6 has built-in security, compliance with IPSec [3] [4] is mandatory in IPv6, and IPSec is actually a part of the IPv6 protocol. IPv6 provides header extensions that ease the implementation of encryption, authentication, and Virtual Private Networks (VPNs). IPSec functionality is basically identical in IPv6 and IPv4, but one benefit of IPv6 is that IPSec can be utilized along the entire route, from source to destination. This protocol has some security but it can be assumed that only enforcing the use of IPSec within IPv6 isn't solving all security problems.

2.3 Position

Upon starting this project I have searched the net to find information about IPv6 and the security issues with it in general. As a starting point I searched for papers about IPv6 and security flaws. A lot of papers that turned up in prelimanery search so it was hard to get a stating point. I decided to start from the scratch and downloaded the rfc 2460 for IPv6. With this in hand i continued my search and ran into a lot of rfc´s that were linked to this rfc. The project has been been executed as a literature research.

[1] http://www.let.leidenuniv.nl/history/ivh/chap2.htm
[2] www.ietf.org
[3] http://www.icann.org/

2.4 Questions

2.4.1 Main

Which vulnerabilities and risks arise if IPv4 and IPv6 coexist on the network and the use of IPv6 tunneling through the IPv4 network

2.4.2 Subquestions

The central question is answered through the following subquestions:

1. *Which security techniques / protocols are build-in within IPv4?*
2. *Which security techniques / protocols are build-in within IPv6?*
3. *What are the vulnerabilities of IPv4?*
4. *What are the vulnerabilities of IPv6?*
5. *Which type of tunnneling methods for IPv6 on the IPv4 network exists?*
6. *What are the vulnerabilities of the tunnelling methods?*
7. *What possibility is there to detect if IPv6 is used as a weapon or targeted.*

2.5 Goal

Surely there will be many more threats around but for the sake of time this project will focus itself on threats that have a strong simmilarity within IPv4 and IPv6. For this project the risks has been classified in target, weapon or means. Computersystems can be:

- A direct target of criminals;
- Be used as a weapon to commit cybercrime;
- As means to collect information.

2.6 Scope

The study consists of a literature research to see what the vulnerabilities and risks are during the use of IPv6. This research is focussed on the vulnerabilities that exist because of the lack of using secure techniques and protocols when IPv4 coexist with IPv6 on the network. It consists of the answers to the questions stated before.

Chapter 3

Build-in techniques / protocols

3.1 Techniques / protocols build-in IPv4 and IPv6

To find out which techniques are build-in into The Internet Protocol (IP) one have to see how the IP protocal has been build up. The protocol on itself is a network-layer protocol in the OSI model that contains addressing information and some control information to enable packets being routed in a network. It is part of the Transmission Control Protocol(TCP) [5]TCP/IP protocol suite. The IP protocol is the heart of the Internet protocols and is suited for both LAN and WAN communications. It has two primary responsibilities: to provide a connectionless and best-effort delivery of datagrams through a network, and secondly providing fragmentation and reassembly of datagrams to support data links with different maximum-transmission unit (MTU) sizes. The IP addressing scheme is integral to the process of routing IP datagrams through an internetwork. Each IP address has specific components and follows a basic format. These IP addresses can be subdivided and used to create addresses for subnetworks. Each device on a TCP/IP [6] network is assigned an unique address (32-bit in IPv4 or 128-bit in IPv6) that consists of two main parts: the network number and the host number. The network number identifies a network and must be assigned by the Internet Network Information Center (InterNIC)[1] if the network is to be part of the Internet. The host number identifies a host on a network and is assigned by the local network administrator.
The difference in IP-packets within IPv4 and IPv6 are shown below.

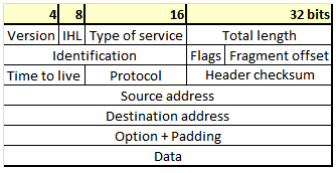

Figure 3.1: IPv4 Packet

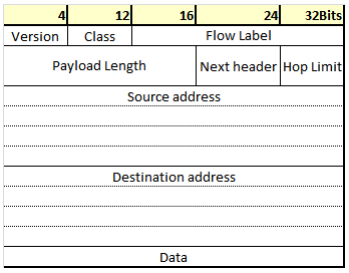

Figure 3.2: IPv6 Packet

[1] http://www.internic.net/

A brief explanation of the fields in the different IP-packages

Version	the version of IP currently used.
IP Header Length	datagram header length.
Type-of-Service	Indicates the quality of service desired.
Total Length	Specifies the length of the entire IP packet
Identification	Identifies the current datagram.
Flags	A 3-bit field which control fragmentation.
Fragment Offset	13 bits field indicates the position of the fragment's data.
Time-to-Live	A counter that decrements down to zero, at which point the datagram is discarded.
Protocol	Indicates which upper-layer protocol receives incoming packets after IP processing is complete.
Header Checksum	To ensure IP header integrity.
Source Address	Specifies the sending node.
Destination Address	Specifies the receiving node.
Options	Allows IP to support various options, such as security.
Data	Contains upper-layer information.

Table 3.1: Field explanations IPv4

Version	The version of the IP used in the packet. 4-bit in IP version 6.
Traffic class	8-bits field determining the packet priority.
Flow label	20-bits specifying the QoS management. Currently unused.
Payload length	16-bits determining the payload length in bytes. When zero, the option is a "Jumbo payload"[a].
Next header	This 8-bits field specifies the next encapsulated protocol.
Hop limit	This is an 8-bits field replacing the time to live field of IPv4.
Source Address	128-bits field with the logical address of the sending host.
Destination Address	128-bits field with the logical address of the receiving host.

Table 3.2: Field explanations IPv6

[a]The payload can be a size of up to 64KB in standard mode, or larger with a "jumbo payload" option

Optional headers for a IPv6 packet are:

- Hop-by-Hop Options header
- Routing header
- Fragment header
- Destination Options header
- Authentication header
- Encrypted Security Payload header

So as you can see there is no security build in the Internet Protocol. To get more security the system will have to rely on other protocols and layers. Encryption and authentication are there but these features aren't part of IP. Since IP datagrams must usually be routed between two devices over unknown networks, any information in them is subject to being intercepted and even possibly changed. With the increased use of the Internet for critical applications, security enhancements were needed for IP. To this end, a set of protocols called IP Security or IPSec was developed. This protocol is supported for both internet protocols, except IPSec is optional in IPv4, but mandatory in IPv6.

Chapter 4

Vulnerabilities

4.1 Vulnerabilities of IPv4

Because of its end-to-end model, IPv4 hasn't any security implemented. It completely relies on the hosts to provide security. As a result of this implementation it has a nummerous amount of security threats which has become well known over the years. The most common and well known threats are:

- Viruses, Trojans and Worms [7]: These types of malicious programs can spread themselves from one infected hosts to another. Although the words Virus, Trojan and worm are used interchangeably, they are not the same thing. A virus attaches itself to a file enabling it to spread from one computer to another, leaving infections as it travels. In a way the worm is similar to a virus and also spread from computer to computer but it has the capability to spread without human action. A Trojan will appear to be useful software but will do damage once installed or run on the computer. It is mostly known to make a backdoor to the infected computer. Trojans are not automatically spread from computer to computer.

- Port scanning and reconnaissance [8]: This is the process of scanning a host to determine which TCP and UDP ports are accessible. Open ports can be used to exploit the specific hosts further.

- Fragmentation attacks[1]: The basic modus operandi of IP fragmentation attacks is to use varied IP datagram fragmentation to disguise its TCP packets from a target's IP filtering devices. For example the 'ping of death' attacks. This attack uses many small fragmented ICMP packets which when reassembled at the destination exceed the maximum allowable size for an IP datagram which can cause the victim host to crash, hang or even reboot.

- Man-in-the-middle attacks (MITM)[2]: It is a form of active eavesdropping where the the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

- Denial of Service Attacks (DoS)[3]: DoS attacks are implemented by either forcing the targeted computer to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Many techniques or method had been developed to overcome the abovementioned security issues. For instance, the use of 'IPSec' to aid the use of encrypted communication between hosts, but this is still optional and continues to be the main responsibility of the end hosts.

[1] http://www.bukisa.com/articles/7931_fragmentation-attacks/
[2] http://en.wikipedia.org/wiki/Man-in-the-middle_attack/
[3] http://en.wikipedia.org/wiki/Denial-of-service_attack/

4.2 Vulnerabilities of IPv6

As we all know IPv6 is also called IPng. And this protocol surely will be here for the next generation but just like any new system or protocol there has to be close attention to it from a security perspective. There sure will be heaps more but below i give the 4 most common vulnerabilities that create a risk to the security of the system.

- One of the first vulnerabilities that exist with using IPv4 next to IPv6 is the fact that network managers need new education on IPv6. IPv6 will be on the networks under their control and it's essential that they they are educated at the basics of IPv6, especially where it comes to the addressing scheme and use of protocols to be able to perform incident handling. Time has told us that this is a part that has been heavely underestimated.
- IPv6 creates addressing complexity and autoconfiguration allows devices to automatically receive a network address without any physical intervention of the administrator. IPv6 supports two different techniques in autoconfiguration. The first is Stateful autoconfiguration, a simple upgrade to the current DHCP protocol and doesn't difference much from the old system in the way of a security perspective. The second technique is Stateless autoconfiguration, this allow the systems to hand out their own IP addresses and does a check to avoid address duplication. This is a nice and easy system but sure gives security issues in the way of tracking abuse of the network.
- Security tools need to be upgraded. The regular hard- and software that is used to route traffic and perform the security analyses won't just work with IPv6 traffic but mostly have to be upgraded to support the protocol. A lot of manufacturers have these upgrades available.
- The equipment that does support IPv6 should treat it as a separate protocol. Therefore, all the security measurments as access control lists(ACL) and other security parameters have to be reevaluated and changed into a system that supports the IPv6 environment.

Chapter 5

Tunnneling methods for IPv6

5.1 Which type of tunnneling methods for IPv6 on the IPv4 network exists?

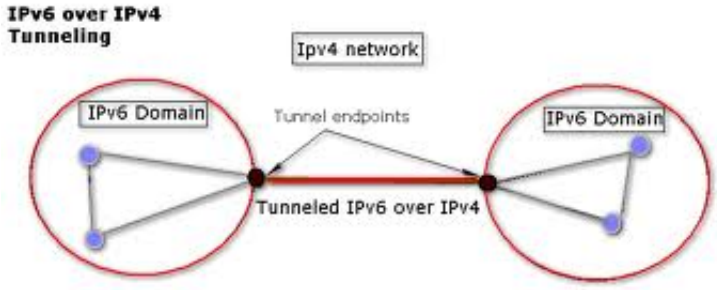

Figure 5.1: IPv6 Tunnel
[1] [2]

Although most operating systems in any business or home network can use the IPv6 protocol on their network, IPv6 does'nt have interoperability features with IPv4. In essence it creates an independent network that coexist parallel to the IPv4 network. To exchange any traffic between the 2 networks one has to implement a translator gateway, but most operating systems have implemented a dual-protocol software to give transparent access between the two networks. This can be done natively or with the use of a tunneling protocol [9] such as 4in6, 6to4 [10], 6in4, or DS-Lite and Teredo [11]. At this moment in time there are a nummerous amount of tunneling methods available to allow one to use IPv6 on the IPv4 network. Each of the tunneling protocols has its own mechanism to make this possible. Because of the short time available for this project i will lift only one out to show what the vulnerabilities are.

5.2 6in4

One of the Internet transition mechanism that is used during the migration of IPv4 to IPv6 is 6in4. It encapsulate IPv6 traffic over IPv4 as defined in RFC 4213 and uses a tunneling method to transport the encapsulated IPv6 traffic.

If the endpoint of a tunnel is inside a private network, one can sometimes still use the DMZ feature of a NAT router. The router will forward all packets to the configured host. In certain routers is is even possible to allow a transparent operation of the 6in4 Mechanism.

On itself the 6in4 protocol lacks any type of security, therefore it is easy to inject IPv6 packets and spoof the IPv4 address of a tunnel endpoint and sending it to the other endpoint [12]. This security flaw can partially been solved with the use of IPsec.

5.3 What are the vulnerabilities of the tunnelling methods?

Eventhough your own network doesn't run IPv6 If you have machines that run Vista or Windows 7, then they will run both protocols simultanously. Even if the network isn't using IPv6 there are methods to make the IPv6 stack turned on. This could be done by infecting a machine on the network with some worm that activates IPv6 stack.

In the past the people involved have invested a lot of time and energy to ensure that IPv6 is a security-enabled protocol. However, because of the fact that IPv6 will exsist in a transition state the greatest risks is the use of tunneling protocols to support the transition to IPv6. Tunneling protocols allow encapsulation of IPv6 traffic within IPv4 data streams so they can be routed through non-compliant devices. Because of this it's possible that people on a network can run IPv6 using these tunneling protocols before the network is ready for it and secured.

It turns out if one start to look into the vulnerabilities of IPv6 there are numerous known and yet unknown. one already known and warned for is for instance the

> Routing Loop Attack Using IPv6 Automatic Tunnels [13]

This rfc states that

> Reference [USENIX09][3] pointed out the existence of a vulnerability in the design of IPv6 automatic tunnels. Tunnel routers operate on the implicit assumption that the destination address of an incoming IPv6 packet is always an address of a valid node that can be reached via the tunnel. The assumption of path validity can introduce routing loops as the inconsistency between the IPv4 routing state and the IPv6 routing state allows a routing loop to be formed. Although those loops will not trap normal data, they will catch traffic targeted at addresses that have become unavailable, and misconfigured traffic can enter the loop.

To get all the vulnerabilities together that are already known it would take a much longer time then available for this project.

[3] http://tools.ietf.org/html/rfc6324#ref-USENIX09

Chapter 6

Coexisting Threats

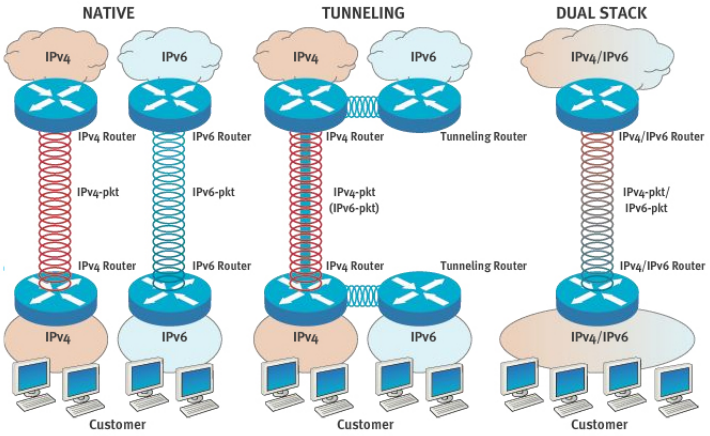

Figure 6.1: Three way's of implementing IPv6
[1]

6.1 Dual Stack

Any network engineer that has dual-stack devices running in the network will have to tackle the shortcomings of either protocol. One has to keep in mind that if the security policies aren't made for either protocol it will give security issues. Imagine a ACL made for IPv4 won't do much good if the IPv6 isn't blocked. This will leave the system open for atacks eventhough the Administrator might think he has ACL's in place. The same thing goes for any other type of firewalling, the all have to be configured to block the risks for both protocols.

Security issues for dual stack

- The IPsec protocol won't work across relays. So the security there goes to zero.
- If one makes use of DNS proxies and they modify the Recource Record (RR) it is impossible to verify the DNSsec signatures.
- Like a SMTP open relay, Transport Relay Translator(TRT) [14] can be abuses by any malicious user, the so called Service Theft.
- It is also not recommended to use TRT for the protocols that use an authentication based on a source IP address.
- 6to4 architecture that is used to take part in reflected DoS or DoS makes an attack hard to trace

- Denial-of-Service (DoS) attacks
- Reflection Denial-of-Service (DoS) attacks

some other security problems are:

- 6to4 routers not being able to identify whether relays are legitimate
- Wrong or impartially implemented 6to4 router or relay security checks
- 6to4 relays being subject to “administrative abuse”

Similar Threats

This section SHORTLY outlines attacks wich are the same for IPv4 and IPv6 end aren’t changed by the use of IPv6

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

Chapter 7

Conclusion

Intro

The goal of this project was to research to see what the vulnerabilities and risks are because of the lack of using secure techniques and protocols when IPv4 coexist with IPv6 on the network. Some of the objectives were achieved while some were not. This was due to the short time frame of the project. This chapter concludes the findings from this research project. The main descriptive question was: Which vulnerabilities and risks arise if IPv4 and IPv6 coexist on the network and the use of IPv6 tunneling through the IPv4 network? The research and analysis has been performed purely with literature as a source.

conclusion

The conclusion is that because of coexistence of the IPv6 protocol on the network the ammount of vulnerabilities hasn't become less, but instead it gave quite a few extra vulnerabilities and risks. The real ammount of risks can't be yet said as only time will be able to tell us how many of the vulnerabilities will be discovered. The main thing we can say now is that it will be a time consuming to be able to cover all vulnerabilities and risks. Time has been too short to really give an answer to the main question and it will be advised to research each vulnerability on it's own to be able to tell if it can be used as a weapon, target or a means to discover information or a combination of the three. For the time being it can be said training is essential because the engineers who grew up with IPv4 need a fresh education because IPv6 is quite different and plays with different tools. Also the security policies between IPv4 and IPv6 aren't consistent.

Last but not least i reccomend the people that are ready to run IPv6 to get there system prepared for it and try to protect yourself at least against the now known weaknesses.

Bibliography

[1] J. Postel, "Internet Protocol", RFC 791 (Standard), Sept. 1981, Updated by RFC 1349.

[2] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460 (Draft Standard), Dec. 1998, Updated by RFCs 5095, 5722, 5871, 6437.

[3] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401 (Proposed Standard), Nov. 1998, Obsoleted by RFC 4301, updated by RFC 3168.

[4] S. Kent and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301 (Proposed Standard), Dec. 2005, Updated by RFC 6040.

[5] J. Postel, "Transmission Control Protocol", RFC 793 (Standard), Sept. 1981, Updated by RFCs 1122, 3168, 6093.

[6] T.J. Socolofsky and C.J. Kale, "TCP/IP tutorial", RFC 1180 (Informational), Jan. 1991.

[7] Daniel Minoli and Jake Kouns, *Security in an IPv6 environment*, CRC Press, Boca Raton, 2009, ID: 231581313.

[8] Scott Hogg and Eric Vyncke, *IPv6 security*, Cisco Press, Indianapolis, IN, 2009, ID: 234444830.

[9] W. Simpson, "IP in IP Tunneling", RFC 1853 (Informational), Oct. 1995.

[10] B. Carpenter and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056 (Proposed Standard), Feb. 2001.

[11] C. Huitema, "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", RFC 4380 (Proposed Standard), Feb. 2006, Updated by RFCs 5991, 6081.

[12] L. Colitti, G. Di Battista, and M. Patrignani, "Discovering ipv6-in-ipv4 tunnels in the internet", 2004.

[13] D. Eastlake 3rd and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234 (Informational), May 2011.

[14] J. Hagino and K. Yamamoto, "An IPv6-to-IPv4 Transport Relay Translator", RFC 3142 (Informational), June 2001.

List of Figures

List of Tables