Security concerns and solutions with IPv6

Tomáš Podermański, tpoder@cis.vutbr.cz

IPv6 security

- IPv6 provides better security than IPv4 for applications and networks

- How does IPv6 provide a solution?

  In IPv6, **IPSec** is a major protocol requirement and is one of the factors in ensuring that IPv6 provides better security than IPv4.

  The large address space also prevents networks against **address scanning**.

Source: http://www.ipv6.com/

Scanning

- The huge address space prevents scanning
  - Brute force scanning on a network with prefix /64 would take 28 years until the first active address found. That means 1 mln tests per second and traffic 400Mb/s.
  - RFC 5157 IPv6 - Implications for Network Scanning
  - Privacy extension for Stateless Address Autoconf. (RFC 4941)
- New ways to find active IPv6 addresses
  - DNS, whois, logs, Flow, NI Query (RFC 4620), well known MAC address, existing IPv4 address, transition mechanisms
  - vanHauser – Ministry of Truth (http://www.youtube.com/watch?v=c7hq2q4jQYw)
  - 2000 active addresses were found in 20 seconds !!
- Scanning on the local network
  - Ping FF02::1
  - Information obtained from neighbor cache (or sniffing on FF02::1)

ICMPv6 (RFC 2463)

- Completely differed comparing to IPv4
- IPv6 can not work without ICMPv6
  - Neighbor Discovery (NDP)
  - Stateless Autoconfiguration (RS, RA)
  - Working with multicast groups (MLD)
  - Diagnostics (PING)
  - Signalization
    - Destination Unreachable
    - Time exceeded
    - **Packet to Big**
    - Redirection
  - …

Neighbor Discovery

- Neighbor cache spoofing
  - Very similar to ARP spoofing
  - The spoofed address can be kept in the NC longer
- DoS - Duplicate Address Detection (DAD)
  - Nodes usually create own address (EUI 64, Privacy Extensions)
  - Optimistic DAD – “sorry, the address is mine, choose another one”
- Neighbor Cache table overload
  - Big address space (64 bits – 1.8e+19 address)
  - Many records in the NC for non existing clients
- Fake Router Advertisement
  - I am a router for this network – use me as a default router
  - The real router is not a valid anymore – zero lifetime
- Fake DHCPv6 Server
  - I am a DHCPv6 sever for this network. Use my options (DNS)

IPv6 Attack Tools

- **Scanners** – Nmap, halfscan6, Scan6, CHScanner
- **Packet forgery** – Scapy6, SendIP, Packit, Spak6
- **DoS Tools** – 6tunneldos, 4to6ddos, Imps6-tools

- **THC IPv6 Attack Toolkit** – parasite6, alive6, fake_router6, redir6, toobig6, detect-new-ip6, dos-new-ip6, fake_mld6, fake_mipv6, fake_advertiser6, smurf6, rsmurf6

  http://freeworld.thc.org/

It is not a problem

There are not enough services available on IPv6.
We have plenty of time to solve it and implement proper solution.

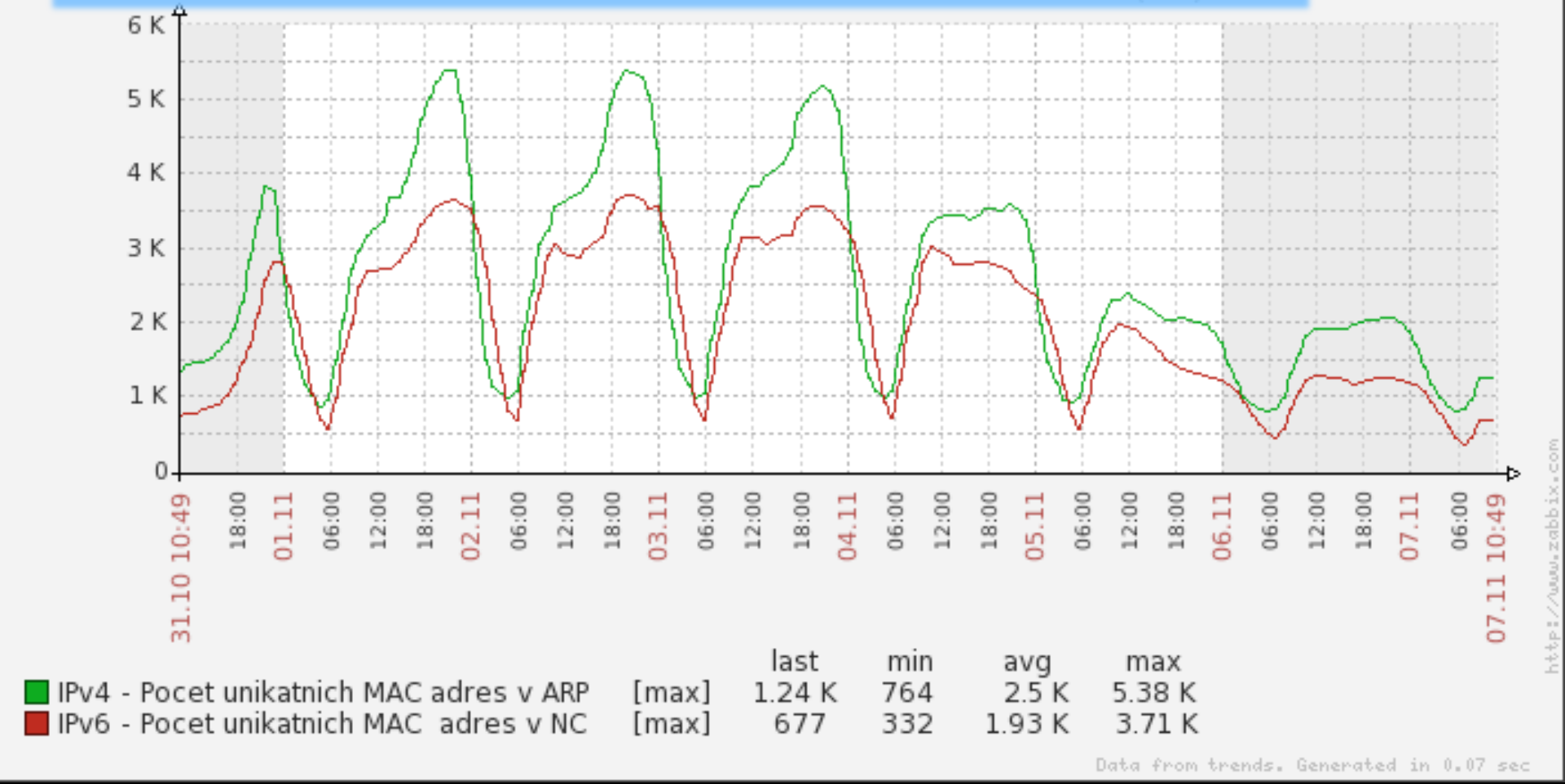
Really ? Do we ?

```
# ./flood_router6 eth0
```

Autoconfiguration – SLAAC, DHCPv6

- SLAAC does not contain addresses of DNS servers
  - Obtain via another protocol (DHCPv4, DHCPv6)
  - Anycast address for recursive DNS servers
  - New option in RA (RFC 6106) – lack of implementation
- DHCP was not planned for IPv6
  - The first RFC 3315 (2003)
  - Coexistence with SLAAC (flags M,O)
  - **Does not contain the address of a default router**
- We have to use both protocols in IPv6-only networks
- Different platforms support different techniques
  - Windows Vista/7 – SLAAC + DHCPv6
  - MAC OS, iOS - SLAAC only
  - Linux, BSD, … – depends on distribution

Number of MAC addresses in NC and ARP table



IPv4 and IPv6 in a network

- More than 50% of PC supports dualstack
  - Most of them use autoconfiguration (SLAAC) to get IP address (MS Vista/7, Linux, Mac OS, iOS, BSD*)
  - IPv6 is preferred protocol by default
- Steps to make an attack:
  - Setup attacker's IP to act as a RA sender
  - Prepare a DHCPv6 server on the attacker's PC; as DNS servers provide attacker's addresses
  - Modify the behavior of DNS server to return A or AAAA records for www.google.com, www.yahoo.com, etc. to your attacker's address
  - Transparent proxy service allows attacker to modify content of webpages

It is not a problem

IPv4 has very similar issues related to autoconfiguration. There is no difference between IPv6 and IPv4.

Really ? Isn’t there ?

Autoconfiguration – IPv4

- IPv4 autoconfiguration = DHCP
- Protection mechanisms on L2 devices
  - **DHCP snooping**
    - Blocking DHCP responses on access ports
    - Prevents against fake DHCP servers
  - **Dynamic ARP protection**
    - MAC-IP address database based on DHCP leases
    - Checking content of ARP packets on client access port
    - Prevents against ARP spoofing
  - **Dynamic lock down**
    - The MAC-IP database is used for inspection of client source MAC and IP address.
    - Prevents against source address spoofing

Possible solutions for IPv6

- SeND (RFC 3971, March 2005)
  - Based on cryptography CGA keys
  - Requires PKI infrastructure
  - Can not work with
    - Manually configured, EUI 64 and Privacy Extension addresses
- RA-Guard (RFC 6105, February 2011)
  - Dropping fake RA messages on access port (RA Snooping)
  - Cooperation with SeND (send proxy) – learning mode
- SAVI (draft-ietf-savi-dhcp-07, November 2010)
  - Complex solution solving
    - fake RA, DHCPv4 an DHCPv6

These solutions have not been widely implementation yet.

Either is not possible to buy a device supporting any kind of this protection or implementations are available on devices that are more expensive.

But things going to be better:

Cisco Catalyst 2960

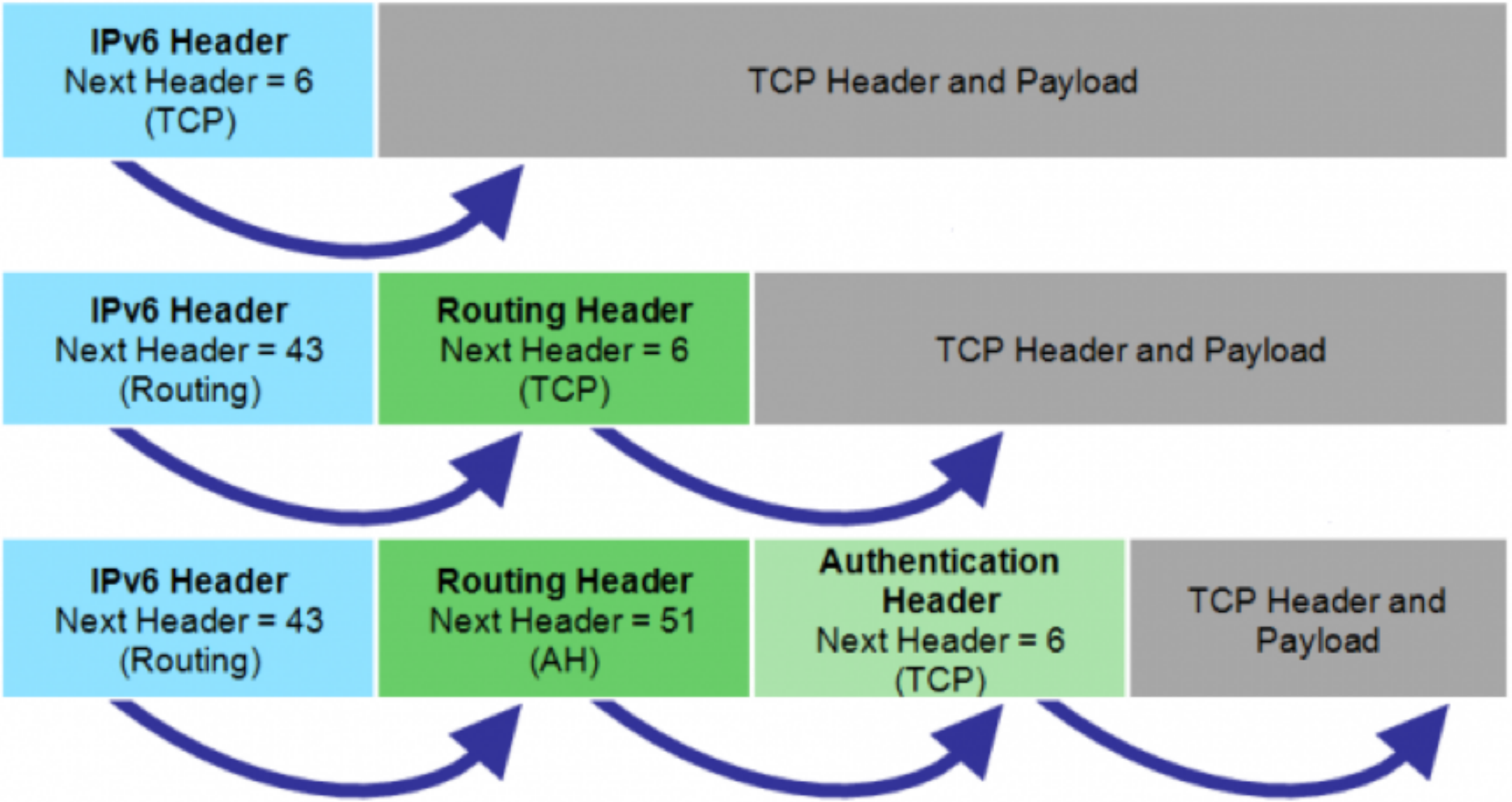
H3C (HP) 4800

How to mitigate impact of those attacs

- Setup an native connectivity into network
- Prefix monitoring and sending alerts
  - ramond - http://ramond.sourceforge.net/
  - rafixd - http://www.kame.net/
  - ndpmon - http://ndpmon.sourceforge.net/
  - scapy6 - http://hg.natisbad.org/scapy6/
- Blocking unwanted traffic on access ports
  - Taken from:http://www.cesnet.cz/ipv6/wg/p/1006-detekce-routeru.pdf

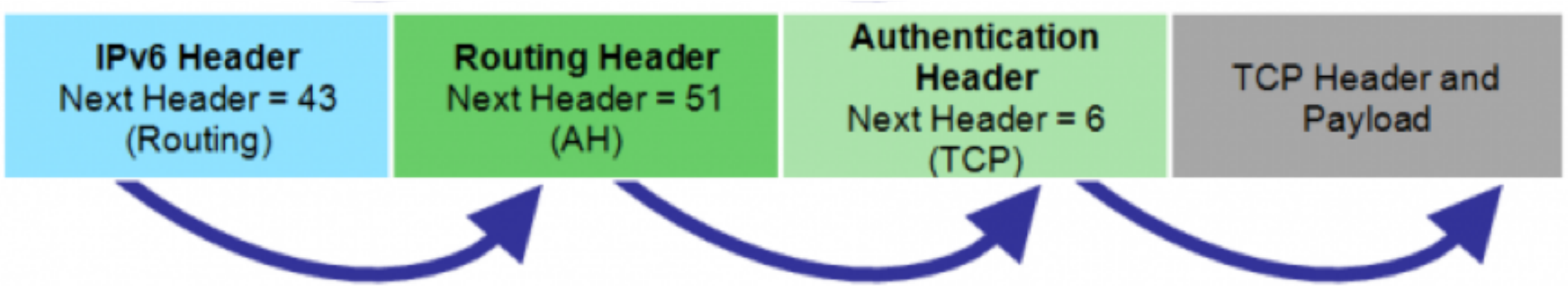
```
ipv6 access-list block-ra-dhcp
     10 deny icmp any any 134 0
     20 deny udp any eq 547 fe80::/64 eq 546
     30 permit ipv6 any any
     exit
interface 1-44
ipv6 access-group block-ra-dhcp in
```

Extension headers



Extension headers

- Mechanism allows to add new features into IPv6
- Chain of headers
  - Protocol:
    - TCP, UDP, ICMPv6, OSPFv3, EIGRP, PIM-SM, …, NULL
  - Extension header:
    - ESP, AH, Hop-by-Hop, Destination, Routing, Fragmentation
- Experimental headers
- Required order



Extension headers

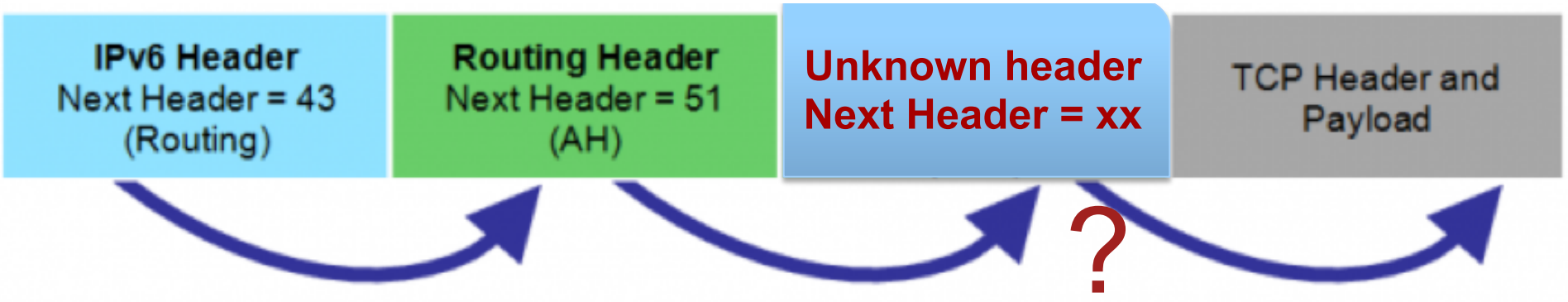
- Routing header (RH0, deprecated by RFC 5095)
- Fragmentation (VRF)
- Extension header manipulation (reorder, long chains of headers)
  - Poor possibility of filtration
  - (do not)try *isic6* – generator of random headers
    - http://isic.sourceforge.net/

```
# ./isic6 -s 2001:2:3:4::1  -d 2001:a:b::1
```

Extension headers or protocol ?

- What happen when a new protocol or header appears ?
  - Expect that header is a protocol an stop processing
    - Drop packet
  - Expect that header is extension header and try to guess next header – process until known header is found

```
config-ipv6-acl# deny ipv6 any any log undetermined transport
```



Implementation Vulnerabilities in IPv6 so far

- IPv6 was meant to be easy to process and easy to implement.
- Programmers have learned their lessons with IPv4.

Hey, then what can probably go wrong?

Taken from: http://freeworld.thc.org/papers.php

Implementation Vulnerabilities in IPv6 so far

- Python getaddrinfo Function Remote Buffer Overflow Vulnerability
- FreeBSD IPv6 Socket Options Handling Local Memory Disclosure Vulnerability
- Juniper JUNOS Packet Forwarding Engine IPv6 Denial of Service Vulnerability
- Apache Web Server Remote IPv6 Buffer Overflow Vulnerability
- Exim Illegal IPv6 Address Buffer Overflow Vulnerability
- Cisco IOS IPv6 Processing Remote Denial Of Service Vulnerability
- Linux Kernel IPv6_Setsockopt IPv6_PKTOPTIONS Integer Overflow Vulnerability
- Postfix IPv6 Unauthorized Mail Relay Vulnerability

Implementation Vulnerabilities in IPv6 so far

- Microsoft Internet Connection Firewall IPv6 Traffic Blocking Vulnerabilityn Microsoft Windows 2000/XP/2003 IPv6 ICMP Flood Denial Of Service Vulnerability
- Ethereal OSI Dissector Buffer Overflow
- Vulnerabilityn SGI IRIX Snoop Unspecified
- Vulnerabilityn SGI IRIX Snoop Unspecified
- Vulnerabilityn SGI IRIX IPv6 InetD Port Scan
- Denial Of Service Vulnerabilityn Apache Web
- Server FTP Proxy IPv6 Denial Of Service
- Vulnerabilityn Sun Solaris IPv6 Packet Denial of Service Vulnerability
- Multiple Vendor HTTP Server IPv6 Socket IPv4 MappedAddress

Implementation Vulnerabilities in IPv6 so far

- Cisco IOS IPv6 Processing Arbitrary Code Execution Vulnerabilityn Cisco IOS IPv6 Processing Arbitrary Code Execution Vulnerability
- Linux Kernel IPv6 Unspecified Denial of Service Vulnerabilityn HP Jetdirect 635n IPv6/IPsec
- Print Server IKE Exchange Denial Of Service Vulnerabilityn
- 6Tunnel Connection Close State Denial of Service Vulnerability
- HP-UX DCE Client IPv6 Denial of Service Vulnerability
- Multiple Vendor IPv4-IPv6 Transition Address SpoofingVulnerability
- ZMailer SMTP IPv6 HELO Resolved Hostname Buffer Overflow Vulnerability
- Linux Kernel IPv6 FlowLable Denial Of Service Vulnerability
- Linux Kernel IP6_Input_Finish Remote Denial Of Service Vulnerability

Implementation Vulnerabilities in IPv6 so far

- Linux Kernel IP6_Input_Finish Remote Denial Of Service Vulnerability
- Sun Solaris 10 Malformed IPv6 Packets Denial of Service Vulnerability
- Sun Solaris Malformed IPv6 Packets Remote Denial of Service Vulnerability
- Windows Vista Torredo Filter Bypass
- Linux Kernel IPv6 Seqfile Handling Local Denial of Service Vulnerability
- Linux Kernel Multiple IPv6 Packet Filtering Bypass Vulnerabilities
- Cisco IOS IPv6 Source Routing Remote Memory Corruption Vulnerability

Implementation Vulnerabilities in IPv6 so far

- Linux Kernel IPv6_SockGlue.c NULL Pointer Dereference Vulnerability
- Multiple: IPv6 Protocol Type 0 Route Header Denial of Service Vulnerability
- Linux Kernel Netfilter nf_conntrack IPv6 Packet Reassembly Rule Bypass Vulnerability
- Sun Solaris Remote IPv6 IPSec Packet Denial of Service Vulnerability
- Linux Kernel IPv6 Hop-By-Hop Header Remote Denial of Service Vulnerability
- KAME Project IPv6 IPComp Header Denial Of Service Vulnerability
- OpenBSD IPv6 Routing Headers Remote Denial of Service Vulnerability

Implementation Vulnerabilities in IPv6 so far

- Linux Kernel IPv6_Getsockopt_Sticky Memory Leak Information Disclosure Vulnerability
- Linux Kernel IPv6 TCP Sockets Local Denial of Service Vulnerability
- Juniper Networks JUNOS IPv6 Packet Processing Remote Denial of Service VulnerabilityCisco IOS Dual-stack Router IPv6 Denial Of Service Vulnerability
- Multiple Platform IPv6 Address Publication Denial of Service Vulnerabilities
- Microsoft IPv6 TCPIP Loopback LAND Denial of Service Vulnerability
- Handling Vulnerabilityn BSD ICMPV6 Handling
- Routines Remote Denial Of Service Vulnerability

Implementation Vulnerabilities in IPv6 so far

Vulnerability data from June 2008

47 bugs

some multi operating systems

many silently fixed

Taken from: http://freeworld.thc.org/papers.php

Conclusion

- IPv6 have all security issues that IPv4, also have
  - DDoS, Address spoofing, (RH0), Fragmentation, …
- Some attacks are more difficult to perform
  - Scanning
  - Better network filtration
- Some are easier to perform
  - RA, DHCPv6 spoofing, …
  - ICMPv6 – more complex, needs more attention to secure
  - Header reorder, overflow, …
  - Lack of knowledge how to secure the network
- Transition techniques are a new way to perform attacks
  - Avoiding firewalls, probes, IDS, IPS
  - Address behind NAT can be accessible from anywhere
- IPSec is NOT complex solution to solve security issues

What we can do about it ?

- Start using IPv6 immediately
  - We have been waiting 15 years for perfect IPv6 - it does not work
  - Until IPv6 is used we will not discover any problem
- Prefer native IPv6 connectivity (anywhere you can)
  - It is a final solution for future (IPv4 will be switched off later)
  - Native IPv6 is more secure than unattended tunneled traffic !
- Ask vendors and creators of standards to fix problems
  - More requests escalate troubles on the vendor side
  - Standardization of IPv6 is not enclosed process. Anyone can contribute or comment the standards
- Stop pretending that IPv6 do not have any troubles
  - IPv6 have many problems
  - Problems can not be solved by covering them
  - Unreliable information led to broken trust amongst users. The naked truth is always better than the best dressed lie