INTRODUCTION TO
IPV6 SECURITY

Harith Dawood
Computer Science Dept.
Cihan University
Erbil - IRAQ.

E-mail: harith.dawood@hotmail.com
E-mail: alwathiq2007@gmail.com
Agenda

1. Motivation for this presentation
2. Introduction.
3. IPv6 Key Features.
5. Some Common Attacks.
6. IPv6 Transition plan (Security Policy)
7. Conclusion.
8. Questions and Answers
Motivation for this presentation
1) This talk is about ongoing work to identify IPv6 security considerations & how to mitigate those problems.


3) Much of this is “work in progress” → your input is welcome!
INTRODUCTION
Introduction

• On 22 March 2008, the US government’s Office of Management and Budget (OMB) issued a memorandum requiring that by June 2008 “all agencies” infrastructure (network backbones) must be using IPv6.

• Emerging Standards, Published by the IEEE Computer Society, 1540-7993/07 © 2007 IEEE
Introduction

Sooner or later you will need to deploy IPv6

- In fact, you have (at least) partially deployed it, already
- IPv6 represents a number of challenges: What can we do about them?

Option #1

Option #2

Suicide is always an option

Option #3

With help comes hope
NATIONAL
SUICIDE PREVENTION
LIFELINE
1-800-273-TALK
Help is available for you or someone you care about, 24-7

Harith Dawood
This means that:

STOP IPv4 ...

&

START IPv6 ...
We Must Start Now !!

Harith Dawood
No doubt some will suffer headaches from having to stuff new knowledge into their heads, but trust me, it's worth it.
Introduction

With millions of new digital devices becoming IP aware, the need for increased addressing and plug & play networking is only met with the implementation of IPv6

IPv6 – Internet for everything!
Broadband Home – A necessity for IPv6!

- **Home Networking**
  - At the heart of the digital home sits the Broadband access point distributing a host of enhanced content and services throughout the home.

- **Wired Devices**
  - Internet access
  - Multiple voice lines
  - Wireless printing
  - Wireless IP Phone
  - Streaming Video/Audio
  - Print/file sharing

- **Wireless Devices**
  - Wireless Laptop
    - Distance learning
    - Video calls
    - MP3 downloads
  - IP Phone
  - PDA
  - Broadband Internet Access
  - Wireless Gaming
  - Triple Play Services
    - Multiple devices served in a Home
    - Commercial download
    - TV guide
  - Broadband Access Point
    - Multiplayer gaming
    - Video on demand
    - Home security
    - Digital audio
    - Domestic appliances
IPv6 KEY FEATURES
IPv6 Key Features

- Improved Network Performance
- Integrated Security (IPSec)
- Larger Address Space
- Standardized Quality of Service (QoS)
- Device auto-configuration

- **variable header size**
  - Improve business performance
- **128 bit address**
  - Business continuity
- **device “plug and play”**
  - Business flexibility/dynamic

- **mandatory IPSec**
  - Secure Business
- **better audio/video transmission**
  - Improve Business QoS
IPv6 Key Features

Header Format Simplification

Multicast

Additionally, others IPv6 features

Jumbograms

Mobility
1. Larger Address Space

IPv4
- 32 bits or 4 bytes long
  - 4,200,000,000 possible addressable nodes

IPv6
- 128 bits or 16 bytes: four times the bits of IPv4
  - $3.4 \times 10^{38}$ possible addressable nodes
  - $340,282,366,920,938,463,374,607,432,768,211,456$ addresses per person
2. Simple and Efficient Header

A simpler and more efficient header means:

• 64-bit aligned fields and fewer fields
• Hardware-based, efficient processing
• Improved routing efficiency and performance
• Faster forwarding rate with better scalability
## IPv4 and IPv6 Header Comparison

<table>
<thead>
<tr>
<th>IPv4 Header</th>
<th>IPv6 Header</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version</strong></td>
<td><strong>Version</strong></td>
</tr>
<tr>
<td><strong>IHL</strong></td>
<td><strong>Traffic Class</strong></td>
</tr>
<tr>
<td><strong>Type of Service</strong></td>
<td><strong>Flow Label</strong></td>
</tr>
<tr>
<td><strong>Total Length</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Identification</strong></td>
<td><strong>Payload Length</strong></td>
</tr>
<tr>
<td><strong>Flags</strong></td>
<td><strong>Next Header</strong></td>
</tr>
<tr>
<td><strong>Fragment Offset</strong></td>
<td><strong>Hop Limit</strong></td>
</tr>
<tr>
<td><strong>Time to Live</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Header Checksum</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Source Address</strong></td>
<td><strong>Source Address</strong></td>
</tr>
<tr>
<td><strong>Destination Address</strong></td>
<td><strong>Destination Address</strong></td>
</tr>
<tr>
<td><strong>Options</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Padding</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Legend
- Field’s Name Kept from IPv4 to IPv6
- Fields Not Kept in IPv6
- Name and Position Changed in IPv6
- New Field in IPv6
3. IPv6 Extension Headers

Simpler and more efficient header means:

- IPv6 has extension headers.
- IPv6 handles the options more efficiently.
- IPv6 enables faster forwarding rate and end nodes processing.
IPv6 SECURITY CONSIDERATIONS
Problem
Problem

Does IPv6 solve all the security problems of IPv4?
IPV6 SECURITY CONSIDERATIONS

1. Ipv6 Address Spoofing (Mac Address Spoofing).
2. Large Address Space Consideration.
5. Extension Header Consideration.
1. IPV6 ADDRESS SPOOFING (MAC ADDRESS SPOOFING) SECURITY CONSIDERATION

• In today's IPv4-based Internet, a typical Internet user connects to an Internet service provider (ISP) and obtains an IPv4 address using the Point-to-Point Protocol (PPP) and the Internet Protocol Control Protocol (IPCP). Each time the user connects, a different IPv4 address might be obtained. Because of this, it is difficult to track a dial-up user's traffic on the Internet on the basis of IP address.
• For IPv6-based dial-up connections, the user is assigned a 64-bit prefix after the connection is made through router discovery and stateless address auto-configuration. If the interface identifier is always based on the EUI-64 address (as derived from the static IEEE 802 address), it is possible to identify the traffic of a specific node regardless of the prefix, making it easy to track a specific user and their use of the Internet.
The conversion of a universally administered, unicast IEEE 802 address to an IPv6 interface identifier

IEEE administered company ID

Manufacturer selected extension ID

IEEE 802 Address:

cccccc00 cccccc00 cccccc00

xxxxxxx xxxxxxxx xxxxxxxx

48 Bit Interface Identifier

EUI-64 Address:

cccccc00 cccccc00 cccccc00 11111111 11111110

xxxxxxx xxxxxxxx xxxxxxxx

IPv6 Interface Identifier:

cccccc10 cccccc10 cccccc10 11111111 11111110 xxxxxxxx xxxxxxxx xxxxxxxx

64 bits

0xFF 0xFE

Harith Dawood
Tracking the user’s moves

At Work
IP: 2001:db8:2::200:baff:febe:0
MAC
0000.BABE.0000

Email Server

Internet

At Home
MAC
0000.BABE.0000

At Wireless Hotspot
IP: 2001:db8:33::200:baff:febe:0
MAC
0000.BABE.0000

Harith Dawood
Because of IPv6 address depends on MAC address which in a sense the MAC address is a computer's true name on a LAN.

Therefore, many people changing their MAC address in different operating systems (Window XP/Vista, Linux & Mac OS X) either manually or by software. Unfortunately, this is privacy risk, because anyone who has your MAC address also has your IP address!!
2. LARGE ADDRESS SPACE SECURITY CONSIDERATION

- Port scanning is one of the most common techniques in use today.
- Default subnets in IPv6 have $2^{64}$ addresses. $10 \text{ Mpps} = \text{more than 50,000 years}$
- In IPv6 networks, IPv6 subnets use 64 bits for allocating host addresses. Scanning such a large address space ($2^{64}$) is not absolutely impossible [Szigeti, S.; Risztics, P. Ref. no.8].
- Many of IPv6 attack tools are already available and relatively easy to install and operate. Tools such as Scapy6 and the Hacker's Choice IPv6 Toolkit.
IPv6 Address Format

- **Network Prefix**: Identifies the address range assigned to a site.
- **Subnet ID**: Identifies a link within a site.
- **Host ID**: Interface ID, 64 bits.

64 Bit Sub-Network prefix

64 Bit Host
3. MULTIPLE ADDRESSES SECURITY CONSIDERATION

- IPv6 assigns multiple addresses to an interface which challenges the filtering rules in the firewalls & access control lists [10]. In such cases, a firewall will need to learn all the addresses dynamically and the filtering rules will need to be automatically generate-able using sophisticated policy rule sets. And such capabilities are not available.
4. MULTICAST SECURITY CONSIDERATION.

• IPv6 has no broadcast method of packet forwarding and instead uses multicast for all one-to-many communications.
4. MULTICAST SECURITY CONSIDERATION.

• If an attacker could send traffic to these multicast groups and all the systems that are part of these groups respond, that would give the attacker information that could be used for further attacks.

• Multicast could not only be used for reconnaissance but also as a way to amplify traffic volumes for DoS attacks.
5. EXTENSION HEADER SECURITY CONSIDERATION

- The figure shows the structure of an extension header and describes how they form a linked list of headers before the packet payload.
5. EXTENSION HEADER SECURITY CONSIDERATION

• An attacker could perform header manipulation on the extension headers to create attacks. Someone could create an IPv6 packet that meets the protocol specification and has an unlimited number of extension headers linked together in a big list.

• Chaining lots of extension headers together is a way for attackers to avoid firewalls and Intrusion Prevention Systems (IPS).
6. FRAGMENTATION SECURITY CONSIDERATION
6. FRAGMENTATION SECURITY CONSIDERATION

• In IPv6, fragmentation is never performed by the intermediary routers but by the end nodes themselves. So, only the end hosts are allowed to create and reassemble fragments.

• This process can be used by attackers to either hide their attacks or to attack a node. By putting the attack into many small fragments, the attacker can try to bypass filtering or detection.

• Fragmentation attacks are typically used by hackers with tools such as: Whisker, Fragrouter, Teardrop, and Bonk [5].
7. NEIGHBOR DISCOVERY AND SOLICITATION SECURITY CONSIDERATION.

- In IPv4, subnets are generally small, made just large enough to cover the actual number of machines on the subnet.
- In contrast, the default IPv6 subnet size is a /64, a number so large it covers trillions of addresses, the overwhelming number of which will be unassigned.
7. NEIGHBOR DISCOVERY AND SOLICITATION SECURITY CONSIDERATION.

• Consequently, simplistic implementations of Neighbor Discovery can be vulnerable to denial of service attacks whereby they attempt to perform address resolution for large numbers of unassigned addresses.

• Such denial of service attacks can be launched intentionally (by an attacker), or result from legal operational tools that scan networks for inventory and other purposes.
SOME COMMON ATTACKS
Viruses and Worms in IPv6

Viruses and email worms: IPv6 brings no change

Other worms:

IPv4: dependence on network scanning.
IPv6: not so easy => will use alternative techniques.

Worm developers will adapt to IPv6
IPv6 Attacks with Strong IPv4 Similarities

- **Sniffing**
  Without IPSec, IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4

- **Application layer attacks**
  Even with IPSec, the majority of vulnerabilities on the Internet today are at the application layer, something that IPSec will do nothing to prevent

- **Flooding**
  Flooding attacks are identical between IPv4 and IPv6
SOME COMMON ATTACKS

- Internet (DMZ, web pages, pop-ups).
- Header manipulation, session hijacking, man-in-the-middle.
- Buffer overflows, SQL injection, cross-site scripting.
- Email (attachments, phishing, hoaxes)
- Distributed denial of service (DDoS)
- Macros, Trojan horses, spyware, malware, key loggers
- VPN, business-to-business (B2B)
- Chat, peer-to-peer (P2P)
- Malicious insider, physical security, rogue devices, dumpster diving.
By the Way:

It Is Real IPv6 Hacking Tools?

the hacker's choice presents:

Attacking the IPv6 Protocol Suite

van Hauser, THC
vh@thc.org
http://www.thc.org
IPv6 Hacking Tools

- **parasite6**: icmp neighbor solicitation/advertisement spoofer, puts you as man-in-the-middle, same as ARP mitm (and parasite)
- **alive6**: an effective alive scanning, which will detect all systems listening to this address
- **fake_router6**: announce yourself as a router on the network, with the highest priority
- **redir6**: redirect traffic to you intelligently (man-in-the-middle) with a clever icmp6 redirect spoofer
- **toobig6**: mtu decreaser with the same intelligence as redir6
- **detect-new-ip6**: detect new ip6 devices which join the network, you can run a script to automatically scan these systems etc.
- **dos-new-ip6**: detect new ip6 devices and tell them that their chosen IP collides on the network (DOS).

[Link to THC-IPv6 Toolkit Attacking the IPv6 Protocol](http://www.darknet.org.uk/2010/07/thc-ipv6-toolkit-attacking-the-ipv6-protocol/)

Harith Dawood
IPv6 Hacking Tools

- **fake_mld6**: announce yourself in a multicast group of your choice on the net
- **fake_mipv6**: steal a mobile IP to yours if IPSEC is not needed for authentication
- **fake_advertiser6**: announce yourself on the network
- **smurf6**: local smurfer
- **rsmurf6**: remote smurfer, known to work only against Linux at the moment
- **sendpees6**: a tool by willdamn(ad)gmail.com, which generates a neighbor solicitation requests with a lot of CGAs to keep the CPU busy.

The Hacker's Choice

IPv6 Hacking Tools

- **dnsdict6**: paralyzed dns ipv6 dictionary brute forcer
- **trace6**: very fast traceroute6 with supports ICMP6 echo request and TCP-SYN
- **flood_router6**: flood a target with random router advertisements
- **flood_advertise6**: flood a target with random neighbor advertisements
- **fuzz_ip6**: fuzzier for ipv6
- **implementation6**: performs various implementation checks on ipv6
- **implementation6d**: listen daemon for implementation6 to check behind a FW

# Other IPv6 Hacking Tools

**Sniffers/packet capture**
- Snort
- TCPdump
- Sun Solaris snoop
- COLD
- Ethereal
- Analyzer
- Windump
- WinPcap
- NetPeek
- SnifferPro

**Scanners**
- IPv6 Security Scanner
- Halfscan6
- Nmap
- Strobe
- Netcat

**DoS Tools**
- 6tunneldos
- 4to6ddos
- Imps6-tools

**Packet forgers**
- SendIP
- Packit
- Spak6
Problem

What are the alternatives to avoid IPv6 in your business?

IPv6 is the only future—proof solution that can satisfy the expected user needs. Therefore, there are no plans to avoid or delay the deployment of IPv6.

Harith Dawood
The Solution?

Providing native IPv6 services in your business.
IPv6 Security Summary

• IPv6 is no more or less secure than IPv4
  – Lack of knowledge of IPv6 is an issue
• There aren’t as many security products that support IPv6 yet
• IPv6 will change traffic patterns (p2p, MIPv6)
• IPv6 larger addresses makes worms and scanning less effective but there are still ways to find hosts
• IPv6 hierarchical addressing and no NAT should reduce the anonymity of hackers and allow for full IPSec
• LAN-based attacks exist in IPv6, Physical Security, Ethernet port security, NAC, 802.1X, SEND can help
• Perform IPv6 filtering at the perimeter
• Use RFC2827 filtering and Unicast Reverse Path Forwarding (uRPF) checks throughout the network
• Use manual tunnels instead of dynamic tunnels
• Remember physical security
Creating an IPv6 Security Policy

When creating an organization-wide security policy, you need to make sure that it has the following critical characteristics. If any one of these is missing, the security policy is doomed to fail:
Creating an IPv6 Security Policy

• It must be written down.
• It must be approved by management.
• It must be agreed upon by everyone and have universal participation.
• It must be well publicized.
• It must be monitored and enforced.
• It must be regularly reviewed and updated.
The policy development process

Anyone can participate

OPEN

Need

Discuss

Evaluate

‘BOTTOM UP’

Internet community proposes and approves policy

TRANSIENT

Consensus

Implement

All decisions & policies are documented & available

Harith Dawood
• How much will it cost?

• How long will the testing take?
  Router: 4-5 weeks
  Layer 3/Optical Switch: 3-4 weeks
  Server: 2-3 weeks
  Host/Workstation: 2-3 weeks
  Security Device: 3-4 weeks
  Network Appliance: 2-5 weeks
• What if my device fails testing? 
  Retesting or conformance regression testing is an easy option.
• Will there be an IPv6 Information Assurance (IA) Testing Certification?
• Does my software need to be production or modified?
• How long will the training staff take?
Conclusion
Defiantly, before deploying IPv6 you should be aware of the following aspects of security for IPv6 traffic:

- *Protection host from scanning and attacking.*
- *Protection of IPv6 packets.*
- *Protecting & Controlling of what traffic is exchanged with the Internet.*
- *Authorization for automatically assigned addresses and configurations.*
- *Prevention systems (firewalls and intrusion detection).*
Conclusion

- IPsec is not the answer to every IPv6 security issues.
- IPv6 is not a panacea for IP-layer/network-layer security concerns. A new protocol brings new security issues & challenges with it.
  (Solve one problem, create another)
- Mobile IPv6 brings also many security challenges with it.
- The lack of IPv6 training for network and security staff is probably the biggest threat.
• At first I must thank my lovely wife and my family, for their support.

• I would also like to thank (my teacher) Mr. Alaa Al-Din Al-Radhi for providing me such good guidance.
REFERENCES


REFERENCES


Web sites

- www.6deploy.org
- www.6diss.org
- www.cisco.com/ipv6
- http://www.ipv6tf.org
- http://www.cisco.com/ipv6
- http://www.microsoft.com/ipv6
Web sites

- NSA SNAC Guide for IPv6
  http://www.nsa.gov/snac/downloads_cisco.cfm?MenuID=scg10.3.1
• IPv6 Security
  • Scott Hogg & Eric Vyncke
  • Cisco Press,
  • Copyright © 2009,
IPv6 Books

- **Security in an IPv6 Environment.**
- Daniel Minoli & Jake Kouns,
- CRC press,
IPv6 Books

• *Understanding IPv6*
  
• 2nd edition,
• Joseph Davies,
• Microsoft Press,
• Copyright © 2008,
• ISBN: 0735624461
IPv6 Books

- **IPv6 Essentials**,  
  - 2nd Edition,  
  - Silvia Hagen,  
  - O’reilly Press,  
  - May, 2006,  
IPv6 Books

• *Running IPv6*,
  • Iljitsck Van Beijnum,
  • Apress
IPv6 Books

• *Deploying IPv6 in Broadband Access Networks.*

• Adeel Ahmed & Salman Asadullah

• Wiley Press, USA.
IPv6 Books

- *Deploying IPv6 Networks*,
- Ciprian Popoviciu,
- Cisco Press
IPv6 Books

• *An IPv6 Deployment Guide*

• Editor: Martin Dunmore

• The 6NET Consortium, Sep. 2005,
IPv6 Books

- **IPv6 Network Programming.**
  - Jun-ichiro itojun Hagino,
  - Elsevier Digital Press,
  - Copyright © 2004,
IPv6 Books

- *Cisco Self-Study: Implementing Cisco IPv6 Networks (IPv6).*
  - *Cisco Press.*
IPv6 Books

- **Mobile IPv6: Protocols and Implementation.**
  - Elsevier Inc.
  - Copyright © 2009,
  - ISBN 13: 978-0-12-375075-4
Thank you ...
Any Questions?

Have a Nice Day ...