# **DOCTOR FUN**



Copyright © 2003 David Farley, d-farley@ibiblio.org http://ibiblio.org/Dave/drfun.html

This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.

4 June 2003

The brave new world of IPv6

# Security Implications of IPv6

Michael H. Warfield Internet Security Systems July 18, 2003

# Outline

- IPv6 Introduction and Overview
- State of IPv6 Deployment
- IPv6 Support
- Addressing and Standards
- Tunnels and Tunnel Brokers
- The Internet Underground
- IPv6 Tools and Techniques
- Examples

## Introduction

- IPv6 the "next generation" Internet protocol
- Under development for many years
- Largely ignored in areas rich in IPv4 addresses
- Addresses limitations in IP version 4 (IPv4)
  - Addresses limited to 32 bits
  - Routing tables are taxing routers
  - Networks and subnetworks are ad-hoc
  - Allocations are disorganized
  - Initially no security features on the IP layer

# **IPv6 Overview**

- Expands addresses to 128 bits
- Formalized address boundaries
- IPSec
- Quality of Service (QoS) typing
- Stateless and stateful autoconfiguration
- Dynamic address renumbering
- Transition tunnels
- Robust resistance to brute force scanning

# **IPv6 Deployment**

- Deployment in North America relatively slow
  - Few tunnel brokers
  - Few ISPs provide native support
- Common in Europe
  - Many tunnel brokers and native ISPs
- Widespread adoption in Asia
  - Many IPv6-only networks
  - APNIC already on 2<sup>nd</sup> allocation of top level prefixes
  - An IPv6-only ISP (Hitachi) in China by end of 2003
- Australia is much like North America

## IPv6 and the US Government

- NASA already has some deployment
- US Department of Defense
  - Current interoperability testing
  - Some transition by end of 2003
  - Wide scale conversion beginning in 2005
  - Complete conversion by 2008

## **Transition Mechanisms**

- Intended to promote IPv6 adoption
- Intended to provide interoperability
- Compatibility addresses for IPv4
- SIT (Six in Tunnel)
- 6to4 Automatic SIT tunnels
- Proxy Services
- Protocol Bouncers
- NAT-PT

# Microsoft Windows Support

- Windows XP Native support
- Windows 2003 Server Native support
- Windows 2000 (SP1 and above) Patch from MS
- Windows NT 3<sup>rd</sup> party patches
- Windows 98 3<sup>rd</sup> party support
- Windows 95 3<sup>rd</sup> party support
- Patches and support from Trumpet Software
- Free patches from Hitachi

# Unix / Linux Support

- Linux (most modern distributions)
  - All kernels since 2.2
  - Firewall support for IPv6 in 2.4
  - New USAGI extensions and IPSec in 2.5/2.6
  - Extensive client and server support
- Unix
  - FreeBSD / OpenBSD / NetBSD
  - Solaris / Solaris x86 version 8 and higher
  - AIX 4.3
  - HP/UX 11i

# Other Operating System Support

- Apple MacOS X
- Novell Netware 6
- Routers
  - 3Com
  - Cisco
  - Hitachi
  - Nokia
- No IPv6 support in most low end broadband or xDSL NAT devices or "routers"

# **Application Support**

- Sendmail / Postfix
- OpenSSH
- Bind 8.x and 9.x
- Apache 2.x (not 1.x)
- Mozilla
- Internet Explorer
- Fetchmail
- XInetd
- Zebra (BGP and OSPF)

## Addresses

- IPv4
  - 32 bits 4 billion addresses
  - 4 8-bit decimal octets, 0-255
  - Variable size subnets
  - Network mask runs from /0 to /32
- IPv6
  - 128 bits 3.4 \* 10^38 addresses
  - 8 16-bit hex fields, 0-FFFF
  - Fixed subnets (/64), and networks (/48)
  - Prefix size runs from /0 to /128

## IPv6 Addresses

- IPv4 Compatible:
- IPv4 Mapped:
- Global:
  - Internet6:
  - 6to4:
  - 6Bone:
- Site Local:
- Link Local:
- Multicast

::n.n.n.n ::FFFF:n.n.n.n 2000::/3 2001::/16 2002::/16 3FFE::/16 FEC0::/10 FE80::/10 **FF00::/8** 

# TLA / NLA / SLA / EUI

- TLA: Top Level Aggregator
  First 16 bits
- NLA: Next Level Aggregators
  - Second and third 16 bit fields
  - Variable field spliting between ISPs
- SLA: Site Level Aggregator IPv6 subnet ID
  - Fourth 16 bit field
- EUI: End Unit Identifier Host identifier
  - Lower 64 bits
- tttt:nnnn:nnn:ssss:eeee:eeee:eeee

# The 6Bone

- 3FFE::/16 Prefix
- Uses TLA / NLA / SLA / EUI scheme
- The Experimental IPv6 backbone
- Scheduled for decommissioning (years away)
- /48 network spaces readily available anywhere
- Uses static SIT tunnels from tunnel brokers
- Some difficulties with reverse DNS lookups

## Internet6

- 2001::/16 Prefix
- Uses TLA/NLA/SLA/EUI scheme
- Production IPv6 Internet Deployment
- Available from numerous ISPs
- Free subnets (/64) and networks (/48) available
- Uses static SIT tunnels from tunnel brokers
- Reverse DNS lookups delegated and stable

## 6to4 Addresses

- 2002::/16 Prefix
- Uses TLA/NLA/SLA/EUI scheme
- An IPv6 network assigned to each IPv4 address
- Automatic SIT tunnels
- No tunnel broker required
- 2002:{IPv4\_ADDR}::/48 Network
- Gateway IPv4 address is the NLA
- Autorouted on IPv4 by the NLA address
- 192.88.99.1 Anycast Gateway to other TLAs

# EUI-64

- Lower 64 bits of autoconfigured address
- Remains constant over renumbering
- Remains constant across subnets
- Based on interface MAC address
- Potential privacy and tracking issues
- Potential network mapping issues
- ::mmMM:MMff:feMM:MMMM (M=Mac address)
  - Invert one bit
  - Split address in half and insert "fffe"

#### Well Known Addresses

- 6to4 addresses
  - Linux: 2002:{IPv4}::1
  - Windows: 2002:{IPv4}::{IPv4}
- Routers
  - Trivial EUI addresses
  - Static Configurations
- Site Local Aggregators
  - Simple subnet numbers
- Easy to guess means easy to scan

# **Stateless Autoconfiguration**

- Allows for auto configuration of IPv6 addresses
- Allows for dynamic renumbering of prefixes
- Subnets may have multiple perimeter routers
  - Different prefixes
  - Different lifetimes
  - Different preferences
- Interfaces may have multiple global addresses
- Rogue routers may inject IPv6 routes on IPv4 nets
- Rogue routers may interfere with IPv6 routers

# SIT Tunnels

- Simple Internet Transition
- Six In Tunnel
- Protocol 41 (ipv6) in IPv4
- IPv4 "protocol" field = 41
- Operates over IPv4 infrastructure
- Static SIT tunnels use preconfigured endpoints
- Tunnel Brokers provide IPv6 through SIT tunnels
- Some tunnel brokers adapt to dynamic addresses

# **Tunnel Brokers**

- Provide IPv6 access across IPv4 networks
- North America
  - FreeNet6 (CA) 6Bone
  - Hurricane Electric (US) Internet6
- Europe
  - SixXS and others
- Asia
  - Many easy to find
- Australia
  - Difficult to find

# 6to4 Autotunnels

- Autoconfigured SIT tunnel
- Protocol 41
- 2002::/16 TLA Prefix
- IPv4 gateway determined by IPv6 address
- No Tunnel Broker required
- Each IPv4 host has an entire IPv6 network
  - 65536 subnets (SLAs) with 1.84 \* 10^19 addresses
  - Total 1.2 \* 10^24 IPv6 addresses for each IPv4 address
- No infrastructure support required

# Teredo

- IPv6 over UDP
- Intended to provide tunnels over IPv4 NAT
- Development driven by lack of IPv6 support by low end router/nat device manufacturers
- Enabled automatically with IPv6 in Windows XP
- Disabled in Windows XP when part of a domain
- Potentially bypasses most firewalls
- Requires a Teredo enabled server on IPv4
- Still in draft stage at IETF

#### Alternate Tunnels

- IPv6 tunnels over PPP
  - PPP tunneled over stunnel
  - PPP tunneled over ssh
  - PPP tunneled over UDP (CIPE)
- IPSec
- GRE (Generic Routing Encapsulation) tunnels

## The Internet Underground

- Elite are already active on IPv6
- IPv6 only IRC channels
- IPv6 only FTP sites
- IPv6 only Web sites
- Many IRC bots have IPv6 patches
- IPv6 has been used for communications tunnels
- IPv6 can be used to hide backdoors
- IPv6 can be used to bypass firewalls

# IPv6 Tools

- Protocol Bounders
  - Relay6
  - Netcat6
  - 6tunnel
  - XInetd
- Scanners
  - halfscan6
  - nmap
- DoS / DDoS
  - 6to4DDoS

# **Hiding Backdoors**

- Backdoors can listen on specific IPv6 addresses
- Cannot be scanned for by IPv4 scanners
- Communications may evade IPv4-only IDS
- SLA and EUI (80 bits) must be exact to connect
- Traffic can be detected by IDS and sniffers



## Firewalls

- Not all firewalls configured to block protocol 41
- IPv4 firewalls can not see TCP or UDP in SIT
- IPv6 firewalls can not see protocol 41 on IPv4
- Teredo (UDP) will bypass most firewalls
- Tunnels should terminate at firewall or perimeter
- SIT tunnels should be controlled to the perimeter
- 6to4 tunnels should be limited to external sites
- Teredo should be prohibited

#### Example - Stealth ssh Backdoor

- Simple, unmodified sshd
- sshd\_config: ListenAddress: 2002:{IPv4}:...
- Pick EUI and SLA at random
- Add and configure IPv6 6to4 to systems
- Add address 2002:{IPv4}:SLA:EUI
- Add ssh authorized keys to accounts & restart
- Client must know and match SLA:EUI
- Can't be scanned for by IPv4 network scanner

## Example - Controlling VMware

- Three ports used by VMware GSX
  - 902: Remote Console
  - 8222: Management User Interface (web)
  - 8333: Secure Management User Interface (ssl web)
- Remote console auth forks from inetd
  - No IPv6 mods necessary on server
  - Client needs netcat6 to bounce protocol
- MUI uses standard browsers
  - Server requires netcat6 to bounce protocols
  - Client uses netcat6 to keep names straight

## **IPv6 Enhanced Traceroute**

- 6to4 UDP with variable payload
- IPv4 TTL expired until protocol gateway or block
- ICMP unreachable
  - IPv4 Protocol Unreachable No IPv6
  - IPv6 Network Unreachable Try other SLA values
  - IPv6 Host Unreachable IPv6 Network Identified
- Vary SLA to determine subnetworks
- Vary well known trivial EUI values
- Traceroute down IPv6 paths

# Conclusion

- IPv6 carries a number of advantages
  - Improved addressing
  - Improved security
  - Improved routing
- IPv6 advantages can be used against networks
  - Backdoors hidden
  - Communications channels hidden
  - Security mechanisms bypassed
- Time for ignoring IPv6 is past
- Time for understanding and using IPv6 is now INTERNET

SECURITY SYSTEMS

#### **DOCTOR FUN**



The brave new world of IPv6

INTERNET SECURITY SYSTEMS

And he didn't even know it was IPv6 enabled...

4 June 2003

This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.

ave/drfun.html

http://ibiblio.org/l

# Security Implications of IPv6

Michael H. Warfield Internet Security Systems July 18, 2003