

SECURITY IN AN IPv6 WORLD

MYTH & REALITY

AfNOG-15 – Djibouti – June 2014

Chris Grundemann

WHO AM I?

- “DO” Director @ Internet Society
- CO ISOC Founding Chair
- RMv6TF Board
- NANOG PC
- NANOG-BCOP Chair
- IPv6 Author (Juniper Day One Books)
- IETF Contributor (Homenet)

- Past: ARIN, UPnP, DLNA, CEA...
- More: <http://chrisgrundemann.com>



THIS TALK...

- Aims to debunk the most common IPv6 security myths
- Is NOT a comprehensive look at IPv6 security practices

Let's get to busting

SOME MYTHS...

MYTH:
I'M NOT RUNNING IPV6, I DON'T HAVE TO WORRY

MYTH:

I'M NOT RUNNING IPV6, I DON'T HAVE TO WORRY

REALITY:

YOUR APPLICATIONS ARE USING IPV6 ALREADY

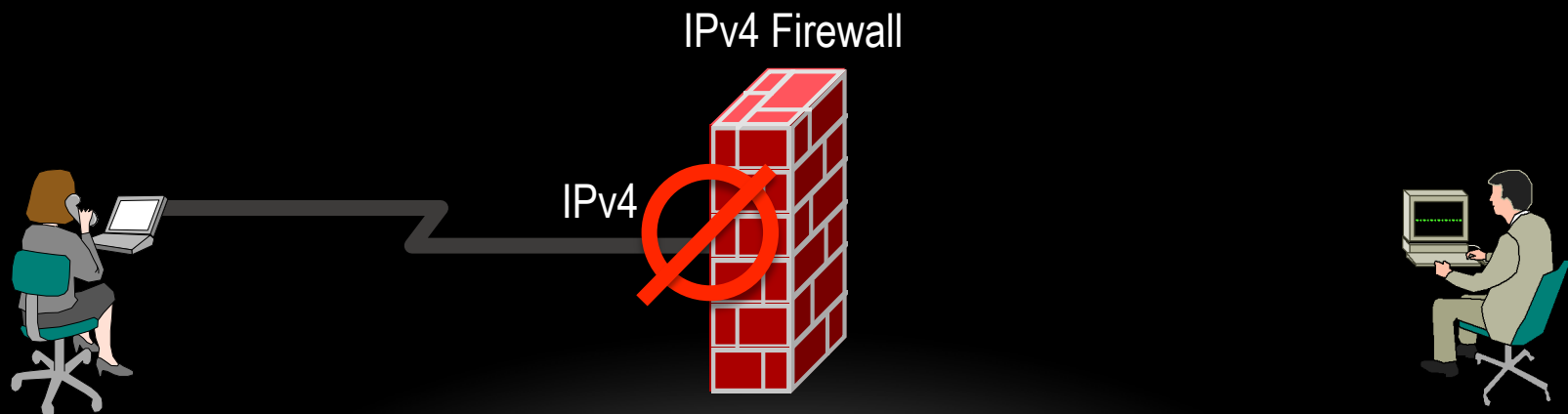
- Linux, Mac OS X, BSD, and Microsoft Vista/Windows 7 systems all come with IPv6 capability, some even have IPv6 enabled by default (IPv6 preferred)
 - They may try to use IPv6 first and then fall-back to IPv4
- If you are not protecting your IPv6 nodes then you have just allowed a huge back-door to exist!

MYTH:

I'M NOT RUNNING IPV6, I DON'T HAVE TO WORRY

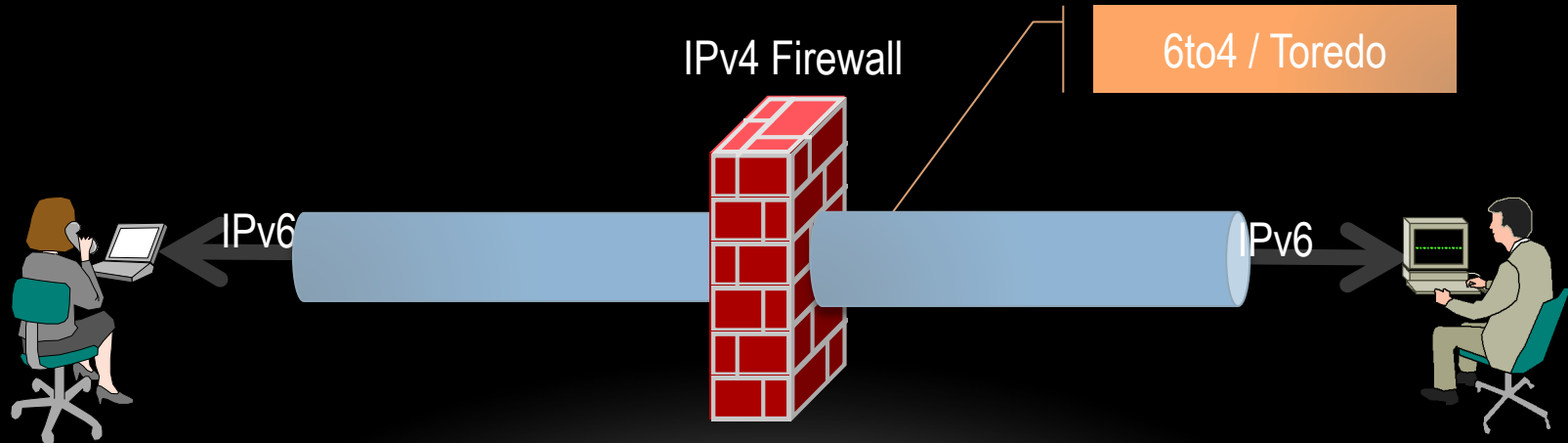
REALITY:

YOUR USERS ARE USING IPV6 ALREADY



MYTH:
I'M NOT RUNNING IPV6, I DON'T HAVE TO WORRY

REALITY:
YOUR USERS ARE USING IPV6 ALREADY



MYTH: IPV6 HAS SECURITY DESIGNED IN

MYTH:
IPV6 HAS SECURITY DESIGNED IN

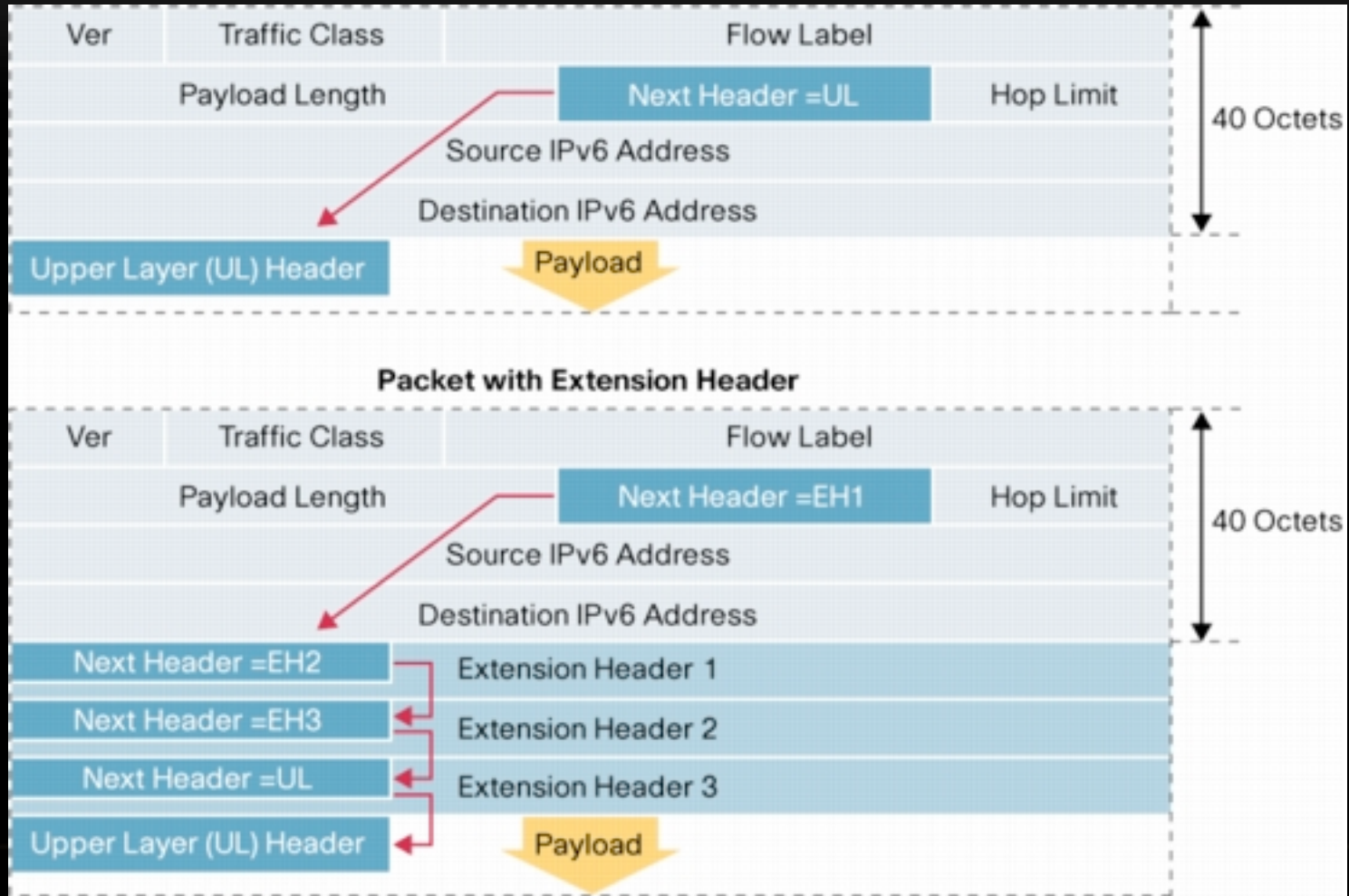
REALITY:
IPSEC IS NOT NEW

- IPsec exists for IPv4
- IPsec mandates in IPv6 are no guarantee of security

MYTH:
IPV6 HAS SECURITY DESIGNED IN

REALITY:
IPV6 WAS DESIGNED 15-20 YEARS AGO

REALITY: EXTENSION HEADERS



MYTH: IPV6 HAS SECURITY DESIGNED IN

REALITY:

- Routing Header Type 0 (RH0) – Source Routing
 - Deprecated in [RFC 5095](#):

The functionality provided by IPv6's Type 0 Routing Header can be exploited in order to achieve traffic amplification over a remote path for the purposes of generating denial-of-service traffic.

MYTH: IPV6 HAS SECURITY DESIGNED IN

REALITY:

- Hop-by-Hop Options Header
 - Vulnerable to low bandwidth DOS attacks
 - Threat detailed in [draft-krishnan-ipv6-hopbyhop](#)

MYTH: IPV6 HAS SECURITY DESIGNED IN

REALITY:

- Extension Headers are vulnerable in general
 - Large extension headers
 - Lots of extension headers
 - Invalid extension headers

MYTH: IPV6 HAS SECURITY DESIGNED IN

REALITY:

- Rogue Router Advertisements (RAs)
 - Can renumber hosts
 - Can launch a Man In The Middle attack
 - Problem documented in [RFC 6104](#)

In this document, we summarise the scenarios in which rogue RAs may be observed and present a list of possible solutions to the problem.

MYTH: IPV6 HAS SECURITY DESIGNED IN

REALITY:

- Forged Neighbor Discovery messages
- ICMP Redirects – just like IPv4 redirects

MYTH:
IPV6 HAS SECURITY DESIGNED IN

REALITY:
MANY ATTACKS ARE ABOVE OR BELOW IP

- Buffer overflows
- SQL Injection
- Cross-site scripting
- E-mail/SPAM (open relays)

MYTH: NO IPV6 NAT MEANS LESS SECURITY

MYTH:
NO IPV6 NAT MEANS LESS SECURITY

REALITY:
STATEFUL FIREWALLS PROVIDE SECURITY

- NAT can actually reduce security

MYTH: IPV6 NETWORKS ARE TOO BIG TO SCAN

MYTH: IPV6 NETWORKS ARE TOO BIG TO SCAN

REALITY:

- SLAAC - EUI-64 addresses (well known OUIs)
 - Tracking!
- DHCPv6 sequential addressing (scan low numbers)
- 6to4, ISATAP, Teredo (well known addresses)
- Manual configured addresses (scan low numbers, vanity addresses)
- Exploiting a local node
 - ff02::1 - all nodes on the local network segment
 - IPv6 Node Information Queries ([RFC 4620](#))
 - Neighbor discovery
 - Leveraging IPv4 (Metasploit Framework "[ipv6_neighbor](#)")
- IPv6 addresses leaked out by application-layer protocols (email)

MYTH:

IPV6 NETWORKS ARE TOO BIG TO SCAN

REALITY:

PRIVACY ADDRESSES ([RFC 4941](#))

- Privacy addresses use MD5 hash on EUI-64 and random number
- Often temporary – rotate addresses
 - Frequency varies
 - Often paired with dynamic DNS (firewall state updates?)
- Makes filtering, troubleshooting, and forensics difficult
- Alternative: Randomized DHCPv6
 - Host: Randomized IIDs
 - Server: Short leases, randomized assignments

MYTH: IPV6 IS TOO NEW TO BE ATTACKED

MYTH:
IPV6 IS TOO NEW TO BE ATTACKED

REALITY:
TOOLS ARE ALREADY AVAILABLE

- [THC](#) IPv6 Attack Toolkit
- IPv6 port scan tools
- IPv6 packet forgery tools
- IPv6 DoS tools

MYTH:
IPV6 IS TOO NEW TO BE ATTACKED

REALITY:
BUGS AND VULNERABILITIES PUBLISHED

- Vendors
- Open source software

MYTH:
IPV6 IS TOO NEW TO BE ATTACKED

REALITY:
SEARCH FOR “*SECURITYFOCUS.COM INURL:PID IPV6*”

MYTH:
96 MORE BITS, NO MAGIC (IT'S JUST LIKE IPV4)

MYTH:

96 MORE BITS, NO MAGIC (IT'S JUST LIKE IPV4)

REALITY:

IPV6 ADDRESS FORMAT IS DRASTICALLY NEW

- 128 bits vs. 32 bits
- Hex vs. Decimal
- Colon vs. Period
- Multiple possible formats (zero suppression, zero compression)
- Logging, grep, filters, etc.

MYTH:

96 MORE BITS, NO MAGIC (IT'S JUST LIKE IPV4)

REALITY:

MULTIPLE ADDRESSES ON EACH HOST

- Same host appears in logs with different addresses

MYTH:

96 MORE BITS, NO MAGIC (IT'S JUST LIKE IPV4)

REALITY:

SYNTAX CHANGES

- Training!

MYTH: CONFIGURE IPV6 FILTERS SAME AS IPV4

MYTH:

CONFIGURE IPV6 FILTERS SAME AS IPV4

REALITY:

DHCPV6 && ND INTRODUCE NUANCE

- Neighbor Discovery uses ICMP
- DHCPv6 message exchange:
 - Solicit: [your link local]:546 -> [ff02::1:2]:547
 - Advertise: [upstream link local]:547 -> [your link local]:546
 - and two more packets, both between your link locals.

REALITY: EXAMPLE FIREWALL FILTER (MIKROTIK)

Flags: X - disabled, I - invalid, D - dynamic

0 ;;; Not just ping - ND runs over icmp6.

```
chain=input action=accept protocol=icmpv6 in-interface=ether1-gateway
```

1 chain=input action=accept connection-state=established in-interface=ether1-gateway

2 ;;; related means stuff like FTP-DATA

```
chain=input action=accept connection-state=related in-interface=ether1-gateway
```

3 ;;; for DHCP6 advertisement (second packet, first server response)

```
chain=input action=accept protocol=udp src-address=fe80::/16 dst-address=fe80::/16  
in-interface=ether1-gateway dst-port=546
```

4 ;;; ssh to this box for management (note non standard port)

```
chain=input action=accept protocol=tcp dst-address=[myaddr]/128 dst-port=2222
```

5 chain=input action=drop in-interface=ether1-gateway

MYTH: IT SUPPORTS IPV6

MYTH:
IT SUPPORTS IPV6

REALITY:
IT PROBABLY DOESN'T

- Detailed requirements (RFP)
 - [RIPE-554](#)
- Lab testing
- Independent/outside verification

MYTH:
THERE ARE NO IPV6 SECURITY BCPS YET

MYTH:

THERE ARE NO IPV6 SECURITY BCPS YET

REALITY:

THERE ARE!

- Perform IPv6 filtering at the perimeter
- Use RFC2827 filtering and Unicast RPF checks throughout the network
- Use manual tunnels (with IPsec whenever possible) instead of dynamic tunnels and deny packets for transition techniques not used
- Use common access-network security measures (NAC/802.1X, disable unused switch ports, Ethernet port security, MACSec/TrustSec) because SEND won't be available any time soon
- Strive to achieve equal protections for IPv6 as with IPv4
- Continue to let vendors know what you expect in terms of IPv6 security features

MYTH: THERE ARE NO IPV6 SECURITY RESOURCES

MYTH:

THERE ARE NO IPV6 SECURITY RESOURCES

REALITY:

THERE ARE!

- [IPv6 Security](#), By Scott Hogg and Eric Vyncke, Cisco Press, 2009
- [Guidelines for the Secure Deployment of IPv6](#)
[Recommendations of the National Institute of Standards and Technology](#)
- Search engines are your friend!

THE REALITY OF DUAL-STACK

- Two sets of filters
- Two sets of bugs



THANK YOU!

Gratitude and Credit:

- [Scott Hogg](#) – My IPv6 Security Guru
- Rob Seastrom – For the Mikrotik example
- The Internet – Lots of searching
- You – Thanks for listening!

[@ChrisGrundemann](#)

<http://chrisgrundemann.com>

<http://www.internetsociety.org/deploy360/>