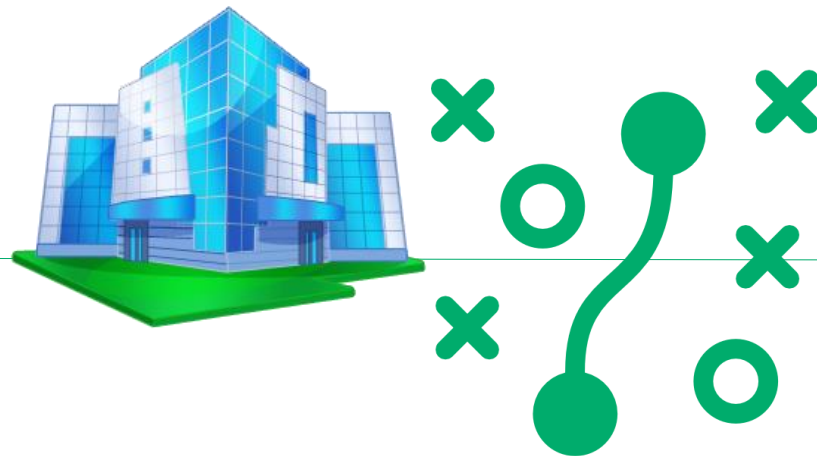# Enterprise IPv6 Security Strategy

Enno Rey, erey@ernw.de

@enno_insinuator

Who Am I

¬ Founder (2001) and head of ERNW, a company providing vendor-independent security assessment & consulting services.

¬ Old-school network guy involved with IPv6 since 1999.

WELCOME
to the IPv6 Security Summit

Day1 – March 14, 2016

Time	Day 1 Track 1	Day 1 Track 2
🕐 09:30	**Developing an Enterprise IPv6 Security Strategy** – Enno Rey	**Basic IPv6 Attacks & Defenses. Hands-On Workshop** – Rafael Schaefer, Christopher Werny
🕐 11:00		Break
🕐 11:15	**The Impact of Extension Headers on IPv6 Access Control Lists - Real Life Use Cases** – Antonios Atlasis	**Basic IPv6 Attacks & Defenses. Hands-On Workshop Part 2** – Rafael Schaefer, Christopher Werny
🕐 12:00	**Security Aspects of IPv6 Multi-Interface and Source/Destination Routing** – Eric Vyncke	**Basic IPv6 Attacks & Denfenses. Hands-On workshop Part 3** – Rafael Schaefer, Christopher Werny
🕐 12:45		Lunch

🕐 12:45

🍺🍔 Lunch

🕐 13:45   **NATTED - A Field Report**   **Advanced IPv6 Network Reconnaissance**

     – Gabriel Müller   – Fernando Gont

🕐 15:15

☕ Break

🕐 15:30   **IPv6 First Hop Security Features on HP Devices**   **Security Assessment of Microsoft DirectAccess**

     – Christopher Werny   – Ali Hardudi

🕐 16:15   **IPv6 First Hop Security Features on HP Devices continued**   **Anonymization IPv6 in PCAPs - Challenges and Wins**
🏳 17:00

     – Christopher Werny   – Jasper Bongertz

Day2 – March 15, 2016

Time	Day 2 Track 1	Day 2 Track 2	Day 2 Track 3
🕐 09:30	**Building a Reliable and Secure IPv6 WiFi Network** – Christopher Werny	**Automating IPv6 Deployments** – Ivan Pepelnjak	**IPv6 in Wireshark Workshop** – Jeff Carrell
🕐 10:15	**Building a Reliable and Secure IPv6 WiFi Network** – Christopher Werny	**Protecting Hosts in IPv6 Networks** – Enno Rey	**IPv6 in Wireshark Workshop** – Jeff Carrell
🕐 11:00		☕ Break	
🕐 11:15	**Remote Access and Business Partner Connections** – Enno Rey	**Recent IPv6 Standardization Efforts** – Fernando Gont	**IPv6 in Wireshark Workshop** – Jeff Carrell
🕐 12:00	**Remote Access and Business Partner Connections continued** – Enno Rey	**Recent IPv6 Standardization Efforts continued** – Fernando Gont	**IPv6 in Wireshark Workshop** – Jeff Carrell
🕐 12:45		🍔 Lunch	

🕐 12:45

🍺🍔 Lunch

🕐 13:45   **Advanced IPv6 Attacks Using Chiron Training**   **Tools for Troubleshooting and Monitoring IPv6 Networks**   **Security Evaluation of Dual-Stack Systems**

– Patrik Fehrenbach

– Antonios Atlasis, Rafael Schaefer   – Gabriel Müller

🕐 15:15

☕ Break

🕐 15:30
🚩 17:00   **Advanced IPv6 Attacks Using Chiron Training continued**   **Tools for Troubleshooting and Monitoring IPv6 Networks continued**

– Antonios Atlasis, Rafael Schaefer   – Gabriel Müller

Agenda of This Talk

¬ Threat & Risk Analysis IPv4 vs. IPv6

¬ Mitigating controls, infrastructure level

¬ Notes on the transformation of IPv4 sec architectures

IPv6 Security Strategy

¬ Within the organization's network, what are the main threats & risks once IPv6 gets deployed, both on the network and the system level?

¬ Which mitigating controls could be put in place?

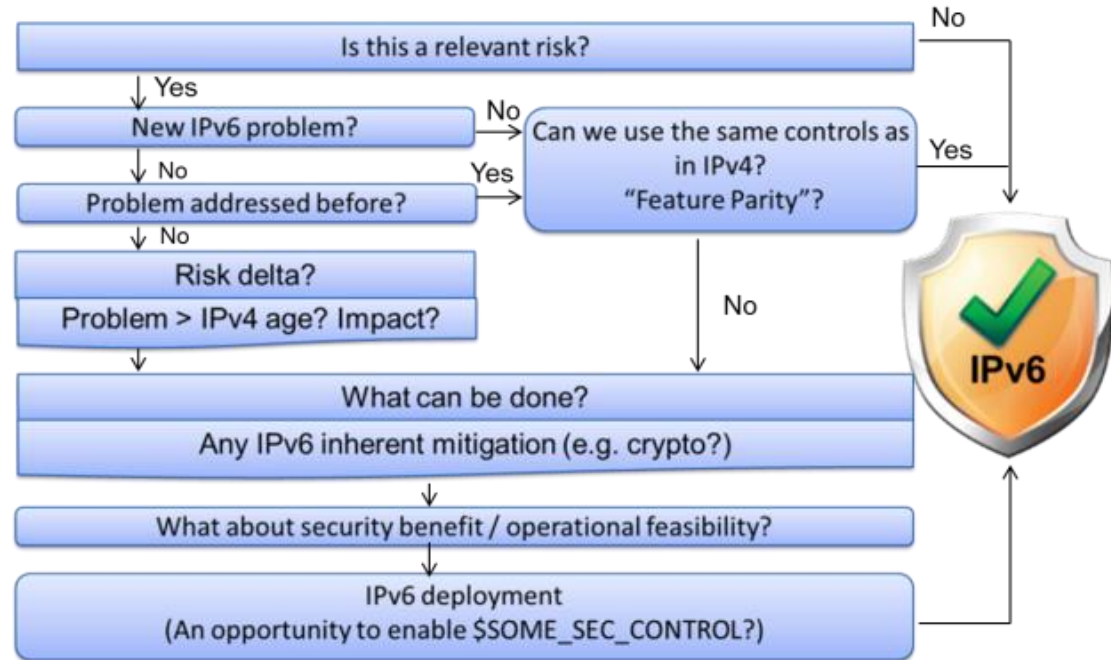– IPv6-specific/new ones

– Existing ones

IPv6 Security Strategy

Typical Steps

¬ Baseline threat analysis (IPv4)

¬ Threat analysis IPv6/DS

¬ Mitigating controls, infrastructure level

¬ Mitigating controls, system level
– To be covered in talk tomorrow

IPv4 / IPv6 Security

Old approach of looking at threats & risks

Baseline Threat Analysis

Main attack classes

[Ranking of associated risks to be displayed later]

¬ Traffic redirection attacks

¬ Attacks against provisioning of configuration information

¬ Denial-of-Service (DoS) by abuse of protocol features

¬ Denial-of-Service exploiting (insufficient) implementation

¬ Denial-of-Service based on load

¬ Unauthorized access over network
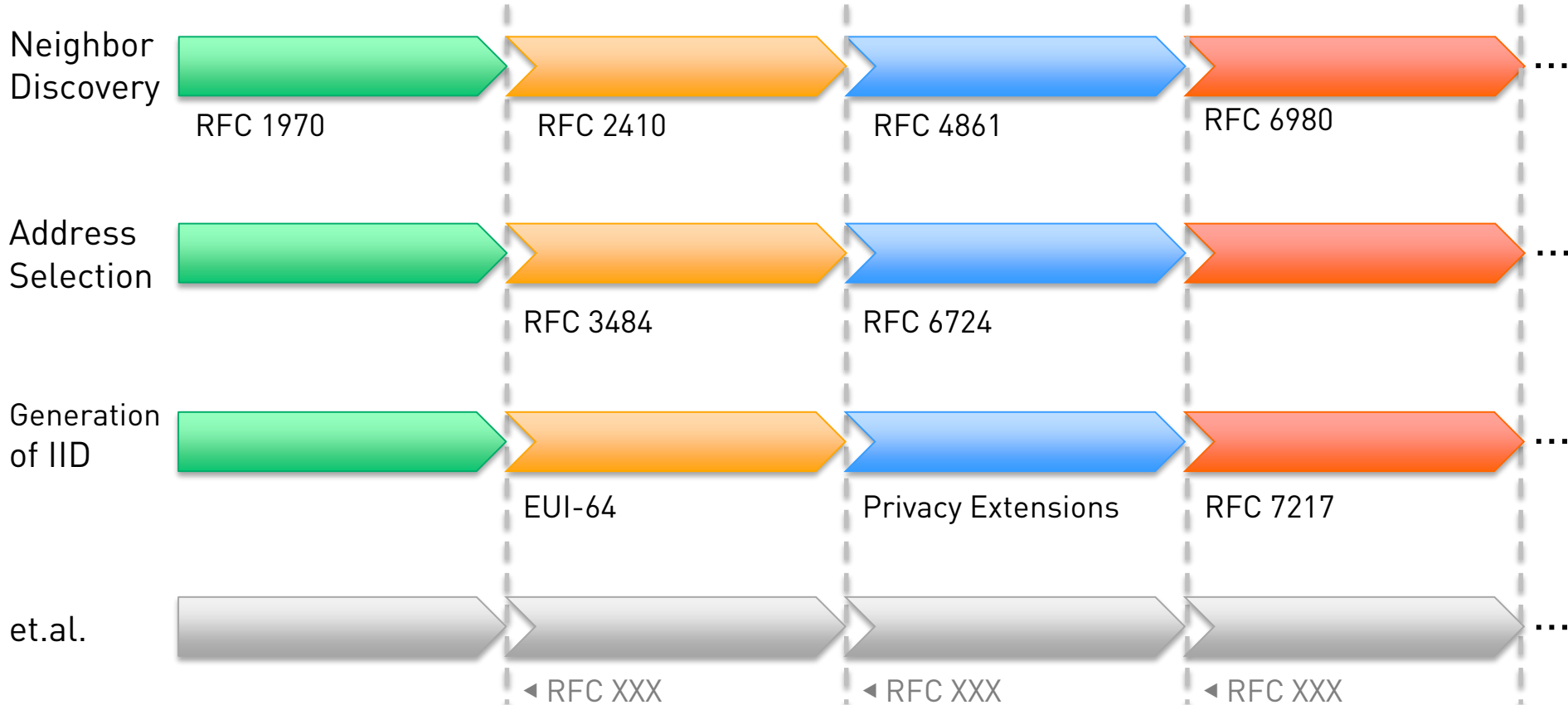
Threat Analysis IPv6

Main technical differences affecting
security posture

See also:
https://www.insinuator.net/2015/06/is-ipv6-more-
secure-than-ipv4-or-less/

¬ Increased complexity

¬ Extension headers

¬ Different provisioning paradigm
  – Plus its trust model

¬ New helper protocol MLD

¬ Different/immature host behavior

¬ Transition technologies

Neighbor Discovery

RFC 1970 | RFC 2410 | RFC 4861 | RFC 6980 | …

Address Selection

| RFC 3484 | RFC 6724 | …

Generation of IID

| EUI-64 | Privacy Extensions | RFC 7217 | …

et.al.

| ◄ RFC XXX | ◄ RFC XXX | ◄ RFC XXX |

What an IPv6 Datagrams Looks Like...

Problem

- ¬ Variable types
- ¬ Variable sizes
- ¬ Variable order
- ¬ Variable number of occurrences of each one.
- ¬ Variable fields

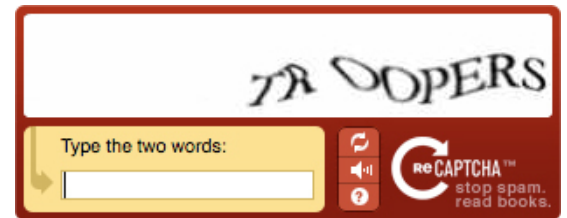IPv6 = f(v,w,x,y,z,)

IPv6 Packet Header

A comparison
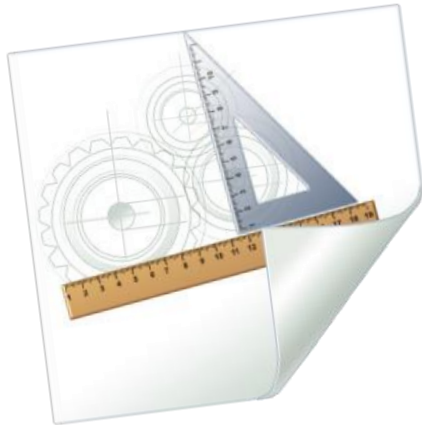

vs.

TROOPERS

vs.

What's a *Router*?

¬ Wikipedia:
  – router = "a **router** is a device that forwards *data packets* between *computer networks*"

¬ RFC 2460:
  – router: "router - a node that forwards IPv6 packets not explicitly addressed to itself."

¬ Is there any issue then?

What's a *Router,* in IPv6?

¬ Looking Closer

¬ RFC 2461: "Routers advertise their presence together with various link and Internet parameters either periodically, or in response to a Router Solicitation message".

¬ In the end of the day, in IPv6 a router is not just a forwarding device but a provisioning system as well.

   – As many other IPv6 guys we generally like the idea.

   – Still, having an operations background in large scale enterprise networks we can tell you quite some of our colleagues have a hard time with this.

   – While we're at it: MANY THANKS TO YOU GUYS OVER THERE AT IETF FOR THE BRILLIANT STATE OF RA & DHCPv6 "INTERACTION".

      – This really helps a lot with widespread IPv6 adoption. Rly!

   – That said we won't further open this can of worms here...

IPv6's Trust Model

¬ On the *local link* we're all brothers.

MLD

See also:
https://www.troopers.de/media/filer_public/7c/35/7c359
67a-d0d4-46fb-8a3b-
4c16df37ce59/troopers15_ipv6secsummit_atlasis_rey_s
alazar_mld_considered_harmful_final.pdf

MLD Considered Harmful

Breaking Another IPv6 Subprotocol

Antonios Atlasis, aatlasis@secfu.net
Enno Rey, erey@ernw.de
Jayson Salazar, jsalazar@ernw.de

www.ernw.de

| Class	Specific Threat	Overall Risk Rating of Attack Type	Delta via IPv6	Priority Weight
Traffic Redirection	ARP/NA Spoofing	high risk	equal risk	7
Traffic Redirection	DNS Spoofing	medium risk	equal risk	6
Traffic Redirection	Spoofing of Default GW through DHCP	high risk	significantly lower risk	6
Traffic Redirection	Route Injection	medium risk	equal risk	6
Traffic Redirection	Attacks against FHRP	medium risk	equal risk	6
Traffic Redirection	Rogue RAs	high risk	significantly increased risk	9
Attacks against Provisioning	Modification of Default GW through DHCP	high risk	significantly lower risk	6
Attacks against Provisioning	Modification of DNS resolver through DHCP	high risk	equal risk	7
Denial-of-Service	Resource Depletion	medium risk	slightly increased risk	7
Denial-of-Service	Flooding of Helper Protocols	low risk	significantly increased risk	7
Denial-of-Service	Traffic blackholing	high risk	significantly increased risk	9
Unauthorized Access over Network	Capability to establish undesired connections	medium risk	significantly increased risk	8

Threat Analysis IPv6

Risk delta in comparison with IPv4 network

Controls / Infrastructure

Main elements
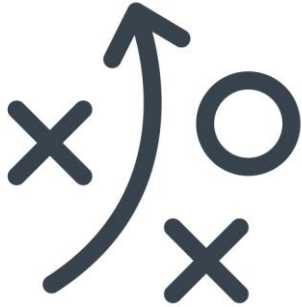
¬ Isolation on the routing layer

¬ Filtering (in transit)

¬ First Hop Security

Infrastructure Controls

Isolation on the Routing Layer

See also:
https://www.insinuator.net/2015/12/developing-an-enterprise-ipv6-security-strategy-part-2-network-isolation-on-the-routing-layer/

¬ Selective announcements
  – Keep "strict filtering" in mind

¬ Null-routing/blackholing of (to-be) protected prefixes at network borders
  – E.g. prefix used for loopback addresses of network devices
  – This is what we see most often (planned).

¬ Reduced *hop limit* in specific segments

The *Strict Filtering* Issue

- An organization might want to split the (PA) address space received into smaller parts to be "handled individually", on the routing level
  - For network topology reasons
    - "regional network hubs/data centers"
  - For organizational reasons
    - different administrative domains
  - For security reasons
    - "selective announcements", e.g. DMZ-only
    - See also http://www.insinuator.net/2014/12/security-implications-of-using-ipv6-guas-only/

- Other organizations ("traditional ISPs") might not like this, for a variety of reasons.
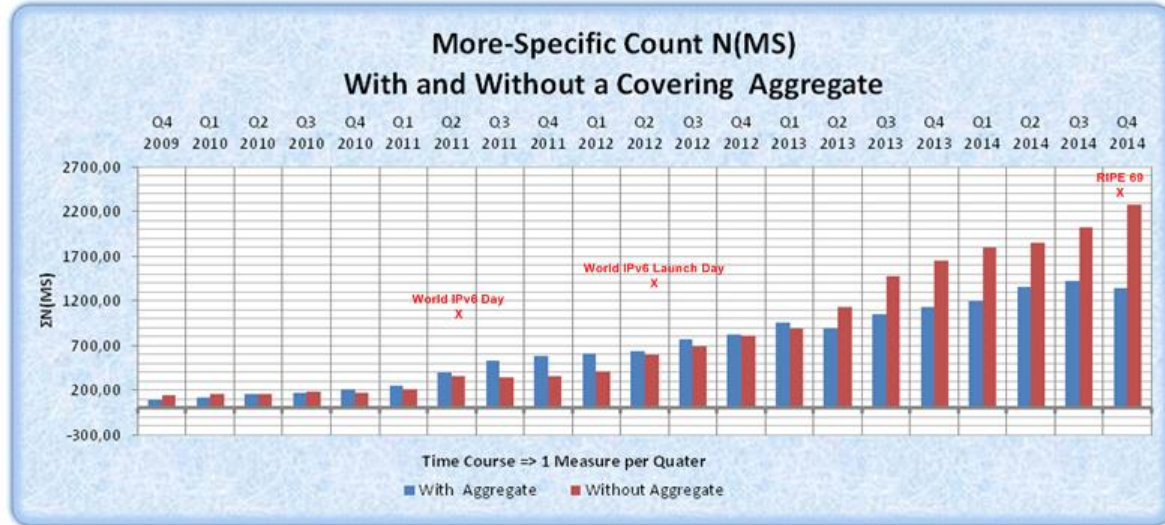 - They then perform *strict filtering*.

Is this really a Problem?

¬ Well, some providers (still) do this.

¬ Overall routing table statistics seem to suggest they become fewer in numbers.

– "The market will fix it".

¬ But keep this topic in mind, and consider including it in carrier selection process.

Strict Filtering

Some Numbers

See also:

https://www.troopers.de/media/filer_public/8
a/6c/8a6c1e42-f486-46d7-8161-
9cfef4101ecc/tr15_ipv6secsummit_langner_r
ey_schaetzle_slash48_considered_harmful_u
pdate.pdf

More-Specific Count N(MS)
With and Without a Covering Aggregate

World IPv6 Day
World IPv6 Launch Day
RIPE 69

Time Course => 1 Measure per Quater

■ With Aggregate   ■ Without Aggregate

Number	Category	Requirement	XY Expectation	Weight	Provider's Answer	Comment
1	General	IPv6 service level agreements (SLAs) meet or exceed existing/IPv4 SLAs.	Yes	Very high	No	
2	General	IPv6 circuit bandwidth, latency, packet loss, and jitter specifications meet or exceed existing/IPv4 specifications/properties.	Yes	Very high	No	
3	QoS	The QoS policies (queuing/discard) applicable to both IPv4 and IPv6 traffic are identical.	Yes	Very high	No	
4	Metrics	IPv6 performance metrics of $PROVIDER's network will be made available.	Yes	Medium	No	
5	Monitoring	$PROVIDER hosts and provides access to a "looking glass" IPv6 BGP router and/or similar functionality (e.g. an access-controlled monitoring portal) for troubleshooting purposes.	Yes	High	No	
6	MPLS	Full support of MPLS 6VPE (RFC 4659) throughout $PROVIDER's MPLS network.	Yes	High	No	
7	Internet Access	$PROVIDER is willing to accept IPv6 prefix advertisements from XY's RIPE PA space allocation up to /48 _without_ a covering aggregate, provided appropriate route6 objects exist.	Yes	Very high	No	
8	Internet Access	In case answer to previous question is "No", what would be the maximum prefix length that XY can advertise without a covering aggregate?	/48	Very high	No	
9	Internet Access	$PROVIDER does not impose any restrictions on IPv6 prefixes accepted as long as their length is shorter or equal /48 and appropriate route6 objects have been created (that means: "strict filtering" like described in http://www.space.net/~gert/RIPE/ipv6-filters.html will _not_ be applied to XY's IPv6 prefixes).	TRUE	Very high	No	
10	Internet Access	XY's IPv6 own address space can be used in the transit network between $PROVIDER's and XY's BGP router(s)?	Yes	Medium	No	
11	MTU	What is the maximum MTU of IPv6 packets that can be transported without fragmentation through $PROVIDER's network? Different for MPLS network?	Pls specify	Very high	No	
12	MTU	All network devices/hosts under $PROVIDER's control originate ICMPv6 PTB messages when needed.	Yes	Very high	No	
13	MTU	All network devices under $PROVIDER's control pass any ICMPv6 PTB messages in transit which are originated from other devices/hosts.	Yes!	Very high	No	

Evaluate Carriers
Sample

See also:
http://docwiki.cisco.com/wiki/What_To_Ask_From_Your_Service_Provider_About_IPv6

Infrastructure Controls

Traffic Filtering

¬ On network boundaries of the corp_nw and potentially intersection points within corporate network

– Border gateways, business partners, WAN interconnection points

¬ IPv6-specific filtering rules to apply to prevent IPv6-specific threats

– Do! Extension headers and/or fragments

– Filtering of specific address ranges (multicast and un-assigned by IANA)

– Apply specific rules wrt filtering ICMPv6.

– Keep performance impact (in particular from logging) in mind!

Infrastructure Filtering

Discussion from a case study org

See also:
https://www.insinuator.net/2015/12/developing-an-enterprise-ipv6-security-strategy-part-3-traffic-filtering-in-ipv6-networks-i/

¬ Balance between
- Visibility (of "bad stuff")
- Speed

¬ ACL processing in itself shouldn't have too much performance impact on ASR 1K platforms.
- Disable sending ICMPv6 Type1 might be required for hardware-only processing.
- Protocol type-code access lists always on RP?
- Optimized ACL Logging (OAL) might help. Supported for IPv6 and on specific platform?

¬ Logging desired/required? – For high speed Internet facing devices going with "drop only" might be preferable.

Filtering ICMPv6

Our recommendation for Internet border gateways

See also:

https://www.insinuator.net/2015/12/developing-an-enterprise-ipv6-security-strategy-part-4-traffic-filtering-in-ipv6-networks-ii/

```
permit icmp any any unreachable
permit icmp any any packet-too-big
permit icmp any any hop-limit
permit icmp any any parameter-problem
permit icmp any any echo-request
permit icmp any any echo-reply
permit icmp any any nd-ns
permit icmp any any nd-na
deny icmp any any log-input (?)
```

Infrastructure Controls

Filtering Extension Headers, Cisco

```
deny ipv6 any any routing
deny ipv6 any any hbh
[deny ipv6 any any fragments]
[deny ipv6 any any undetermined-transport]
deny ipv6 any any dest-option
deny ipv6 any any mobility
```

Infrastructure Controls

Filtering unallocated space

```
deny 0400::/6 any
deny 0800::/5 any
deny 1000::/4 any
deny 2d00::/8 any
deny 2e00::/7 any
deny 3000::/4 any
deny 4000::/3 any
deny 6000::/3 any
deny 8000::/3 any
deny a000::/3 any
deny c000::/3 any
deny e000::/4 any
deny f000::/5 any
deny f800::/6 any
deny fe00::/9 any
```

See also:
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml

http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml

Infrastructure Controls

Filtering *Martians*


```
deny ipv6 host ::1 any log-input
deny ipv6 fc00::/7 any
deny ipv6 fec0::/10 any
deny ipv6 2001:db8::/32 any
deny ipv6 2001:2::/48 any
```

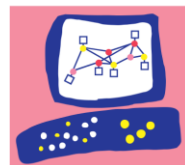See also https://tools.ietf.org/rfc/rfc6890.txt

Infrastructure Controls

Alternative approach wrt address space filtering

```
deny ipv6 2001:db8::/32 any
permit ipv6 2000::/3 any
permit ipv6 fe80::/10 any
[permit ipv6 :: any]
deny ipv6 any any
```

Infrastructure Controls

Filtering Extension Headers, Check Point

From: sk39374

By default, Check Point Security Gateway drops all extension headers, except fragmentation. This can be adjusted by editing the `allowed_ipv6_extension_headers` section of `$FWDIR/lib/table.def` file on the Security Management Server.

Furthermore, as of R75.40 there is an option to block type zero even if Routing header is allowed. It is configurable via a kernel parameter `fw6_allow_rh_type_zero`. The default of 0 means it is always blocked. If the value is set to 1, then the action is according to `allowed_ipv6_extension_headers`.

Do not touch `table.def`!

First Hop Security

Overview

¬ Term initially coined by Cisco but concept available on devices of other vendors (HP), too.

¬ Set of approaches (& their commands) meant to mitigate risks on the *local-link* (= "IPv6's Achilles' heel").

¬ Main use cases
  – Access layer
  – Data center, physical infrastructure (?)
  – Data center, virtualized infrastructure (?)

First Hop Security

"Generations" (Cisco)

¬ # 1st generation

– Prevent rogue router advertisements and allow for ACLs.

– Simple commands which can be applied on port or VLAN level

→ Easy integration into templates.

– Mature and available on the vast majority of access layer platforms.

– Lack of support in virtualized DC
(as of Jan 2016 → Cisco road map).

– Can be circumvented by attacker & there's no fix for this (except RFC 6980).

RFC 6980

Unfortunately, as of Jan 2016 pretty much only Linux supports this.

Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery

Abstract

   This document analyzes the security implications of employing IPv6
   fragmentation with Neighbor Discovery (ND) messages. It updates RFC
   4861 such that use of the IPv6 Fragmentation Header is forbidden in
   all Neighbor Discovery messages, thus allowing for simple and
   effective countermeasures for Neighbor Discovery attacks. Finally,
   it discusses the security implications of using IPv6 fragmentation
   with SEcure Neighbor Discovery (SEND) and formally updates RFC 3971
   to provide advice regarding how the aforementioned security
   implications can be mitigated.

First Hop Security

Cisco Land

¬ 2nd/3rd generation

– These features address some other
(in most organizations: risk-wise less relevant)
scenarios.

– Usually based on "IPv6 snooping" framework
→ Config becomes more complex, with "policy"
statements.

– In other environments (and the lab) we've
observed a lot of teething problems (see also
cisco-sa-20150923-fhs).
→ Most features not considered mature for prod.

– Ratio of operational cost vs. actual security
benefit has to be kept in mind!

First Hop Security

Cisco

¬ Sample:

```
ipv6 snooping logging packet drop

interface GigabitEthernet1/0/1
  switchport mode access
  ipv6 nd raguard
  ipv6 dhcp guard
```

¬ (Only!) this is what we usually recommend.

One More Note on
RA Guard

¬ **It might make sense to use it in (presumed) IPv4-only networks, too.**

– Alternatively one can filter IPv6 packets at the switch port, based on their *IEEE 802.3 Ethertype* (0x86DD).
Not many (namely industrial) switches support this though.

FHS Availability, Cisco

Feature/Platform	Catalyst 6500 Series	Catalyst 4500 Series	Catalyst 2K/3K Series	ASR1000 Router	7600 Router	Catalyst 3850	Wireless LAN Controller (Flex 7500, 5508, 2500, WISM-2)	Nexus 3k/5k/6k/7k
RA Guard	15.0(1)SY	15.1(2)SG	15.0.(2)SE		15.2(4)S	15.0(1)EX	7.2	NX-OS 7.2
IPv6 Snooping	15.0(1)SY[1]	15.1(2)SG	15.0.(2)SE	XE 3.9.0S	15.2(4)S	15.0(1)EX	7.2	NX-OS 7.2
DHCPv6 Guard	15.2(1)SY	15.1(2)SG	15.0.(2)SE		15.2(4)S	15.0(1)EX	7.2	NX-OS 7.2
Source/Prefix Guard	15.2(1)SY	15.2(1)E	15.0.(2)SE[2]	XE 3.9.0S	15.3(1)S		7.2	NX-OS 7.2
Destination Guard	15.2(1)SY	15.1(2)SG	15.2(1)E	XE 3.9.0S	15.2(4)S			NX-OS 7.2
RA Throttler	15.2(1)SY	15.2(1)E	15.2(1)E			15.0(1)EX	7.2	
ND Multicast Suppress	15.2(1)SY	15.1(2)SG	15.2(1)E	XE 3.9.0S		15.0(1)EX	7.2	

FHS Availability / Cisco

Additional Information

¬ # A guy from Cisco wrote to us:

"FHS on NEXUS is still roadmaps for Nx7K in 7.3 due on CCO in January 2016. What FHS means in this context is RA Guard, DHCPv6 Guard and IPv6 Snooping. The other NEXUS platforms will follow later in 2016. The rest of the IPv6 FHS features will be extended to all platforms as well."
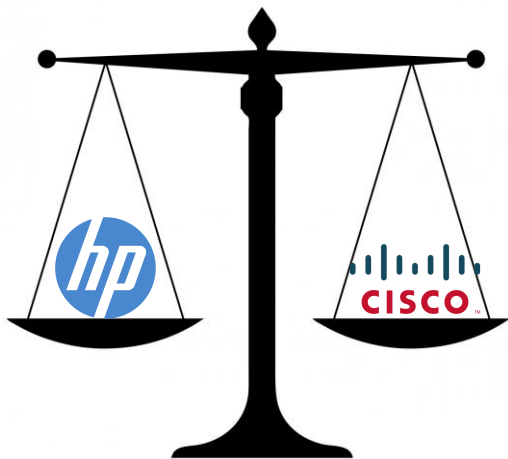
First Hop Security

HP

See also: Chris' talk later ;-)

¬ Most needed features available on relevant CMW platforms

– `ipv6 nd detection  [= raguard]`
– `ipv6 dhcp snooping`
– `ipv6 nd snooping`

¬ Different config paradigm though

– Enable globally
– Configure exemptions on port level

First Hop Security

On config paradigms

¬ Looking at our proposed way, the config approaches differ between the two vendors
  – Cisco: protection features enabled on port level
  – HP: enable globally & configure "trust".

¬ Disadvantages
  – Can confuse operations personnel
  – Different way of handling in templates

¬ → Discussion needed.
  – Mimicking HP way with Cisco might be cumbersome or impossible.

First Hop Security

MLD

As of March 2016 would have to be filtered by port-/VLAN-based ACL, e.g.

```
deny icmp any any mld-query
```

At some point "`mld guard`" might be available in Cisco space.

```
IP Multicast                                        E. Vyncke
Internet-Draft                                          Cisco
Intended status: Informational                         E. Rey
Expires: December 27, 2015                                ERNW
                                                    A. Atlasis
                                                    NCI Agency
                                                 June 25, 2015


                           MLD Security
                 draft-vyncke-pim-mld-security-00

Abstract

   The latest version of Multicast Listener Discovery protocol is
   defined in RFC 3810, dated back in 2004.  New security research has
   exhibited new vulnerabilities in MLD, both remote and local attack
   vectors.  This document describes those vulnerabilities and proposes
   specific mitigation techniques.
```

Host Level Perspective

Two main aspects:
- Residual risk
- Controls on system level

¬ (Reasonable) Assumptions:

- IPv6 mostly in dual-stack mode.
- FHS is implemented as of the above recommendations.
- Routing layer security only partially applied/deployed, if at all.
- IDP systems have lower detection/ prevention rates in IPv6 networks.

Host Level Perspective

Main Residual Risks (case study org)

[Note: without specific context no reasonable numbers as for "risk delta" can be determined]
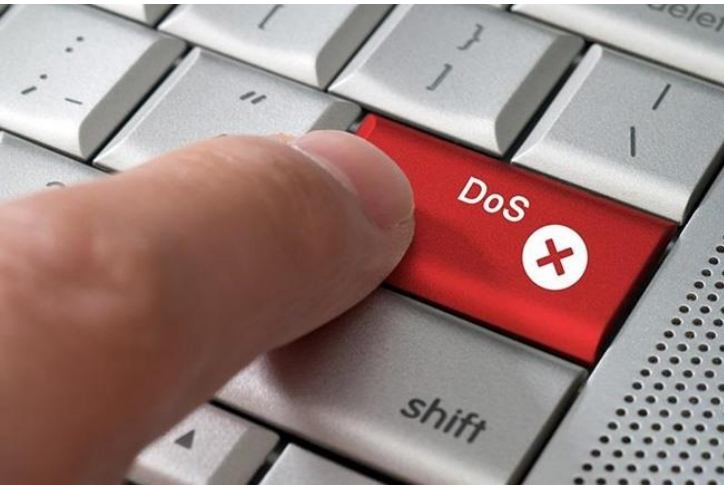
¬ Denial-of-Service originating from the *local-link*.

– Increased exposure wrt malformed pkts.

– Flooding of helper protocols.

¬ Unauthorized access

– Less isolation/separation of address space.

– Less protection from security controls on the network infrastructure level.

Host Level Perspective

Controls

¬ To be covered in tomorrow's talk on "Protecting Hosts"

So...

... now that've covered the new stuff related to IPv6 specifics,
can we otherwise keep our existing controls and operate them the
same way we did before?

Alas, not really.
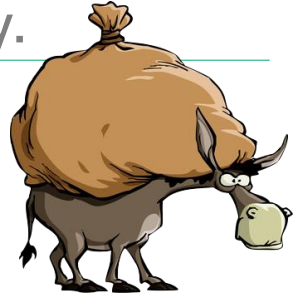
¬ There's some elements that will have a hard time working properly.

¬ There's some elements of current sec architectures that won't work at all, anymore.

¬ Some paradigm shift might be needed.

Elements Having a Hard Time

¬ Reputation based stuff

¬ Stateful stuff
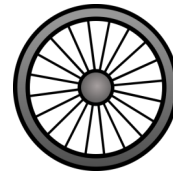
Reputation

Messaging, Malware and Mobile Anti-Abuse Working Group
M³AAWG Policy Issues for Receiving Email
in a World with IPv6 Hosts

September 2014

Internet mail anti-abuse efforts have often relied on the reputation associated with a sending host's IPv4 address. This reputation data provides an identifier for active agents in email handling. Although less stable and less reliable than would be preferred, IPv4 addresses have proved useful for rate limiting and reputation assessment, and most anti-abuse systems will be unable to function if the effectiveness of these mechanisms are degraded. Over the years, there has been a continuing effort to develop reputation assessment based on the more stable alternative of domain names, with or without associating an IP address. The advent of IPv6 addresses makes this essential, along with improved address-based mechanisms.

M³AAWG encourages the industry's development of technologies, policies and procedures to address this concern for relaying email across administrative domains by pursuing the targeted efforts described here. These efforts will provide a solid foundation for building and operating integrated Internet mail and anti-spam systems that include IPv6 in the operational mix. The goals are: to aggregate the massive address space into more easily trackable assignments, to require operators to identify hosts intended to act as outbound mail

¬ Right now most reputation based systems don't work well with IPv6.

¬ Not sure if this will change in the future
  − Internet of things & services

¬ See also:
¬ https://moderncrypto.org/mail-archive/messaging/2014/000780.html
¬ http://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Inbound_IPv6_Policy_Issues-2014-09.pdf

¬ Simple rule: the higher the complexity of a communication act, the higher the cost of keeping state of it.

¬ IPv6 has a high degree of complexity...

A Well-known *State* Related Security Problem

Neighbor Cache Exhaustion (NCE)
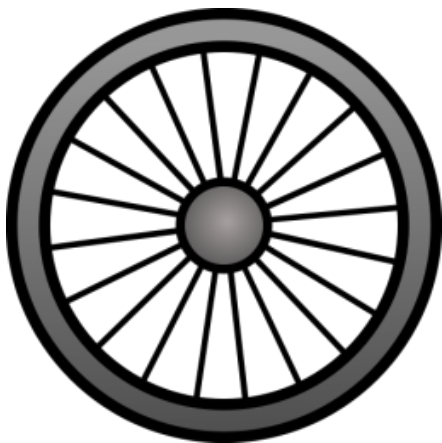
¬ In the end of the day, *neighbor cache exhaustion (NCE)* is a *state* problem

– ARP had an *incomplete* state as well.
– You just rarely saw segments > /24 exposed to the Internet.

¬ Let's assume NCE is a mostly solved problem.

¬ Still, there's much more opportunities for a state oriented sec model to fail in the IPv6 age

– I'm very interested to see how vendors of stateful firewalls will handle scenarios like "single infected machine sitting in a broadband /64 and establishing valid connections to web server from many many random source addresses". BCP 38 won't solve this.

Need (Another) Real Life Example?

"Our network switches have been observed using far more CPU than has historically been the case, we have had a variety of packet storms that appear to have been caused by forwarding loops despite the fact that we run a protocol designed to prevent such loops from taking place, and we have had a variety of unexplained switch crashes."

Massachusetts Institute of Technology

From: Network Meltdown due to MLD state

- http://blog.bimajority.org/2014/09/05/the-network-nightmare-that-ate-my-week/

Ceterum Censeo

[RFC 3439] – Go read it. Again!

Network Working Group   R. Bush
Request for Comments: 3439   D. Meyer
Updates: 1958   December 2002
Category: Informational

              Some Internet Architectural Guidelines and Philosophy

Status of this Memo

   This memo provides information for the Internet community. It does
   not specify an Internet standard of any kind. Distribution of this
   memo is unlimited.

Copyright Notice

   Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

   This document extends RFC 1958 by outlining some of the philosophical
   guidelines to which architects and designers of Internet backbone
   networks should adhere. We describe the Simplicity Principle, which
   states that complexity is the primary mechanism that impedes
   efficient scaling, and discuss its implications on the architecture,
   design and engineering issues found in large scale Internet
   backbones.

Table of Contents

¬ All/most content/signature based stuff once:

Stuff not Working at All
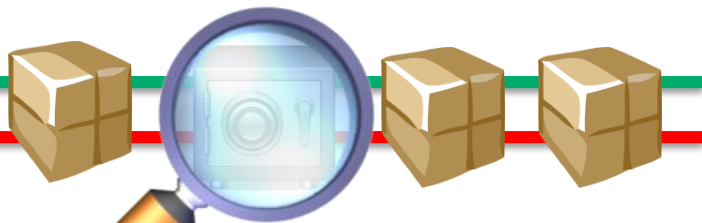
– Traffic is encrypted

– Traffic is not sanitized
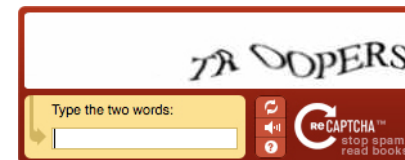
¬ Link to slides,
tool & whitepaper: **blackhat**
http://www.insinuator.net/2014/08/ernw-blackhat-us-2014/

What's the Cure, Man?

¬ Move security functions to end-points

¬ In case of choke-point sec model perform sanitizing before inspection

 – Some architecture change needed, maybe.

¬ Forget about state

 – Stateless ACLs might be your friend.

Move Sec to End-points
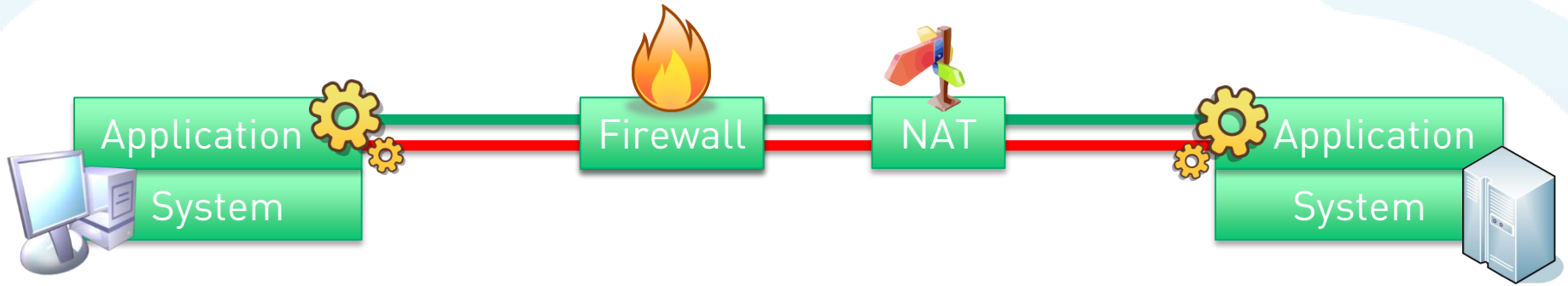
Move Sec to End-points

¬ **This is happening anyway**

– Think: hypervisor-firewalls

¬ **We understand you'll keep the centralized stuff for compliance reasons (and/or to save discussions with the PCI auditor)**

– As you do with anti-virus...

In Case You Use an IDPS

Decryption
& Scrubbing
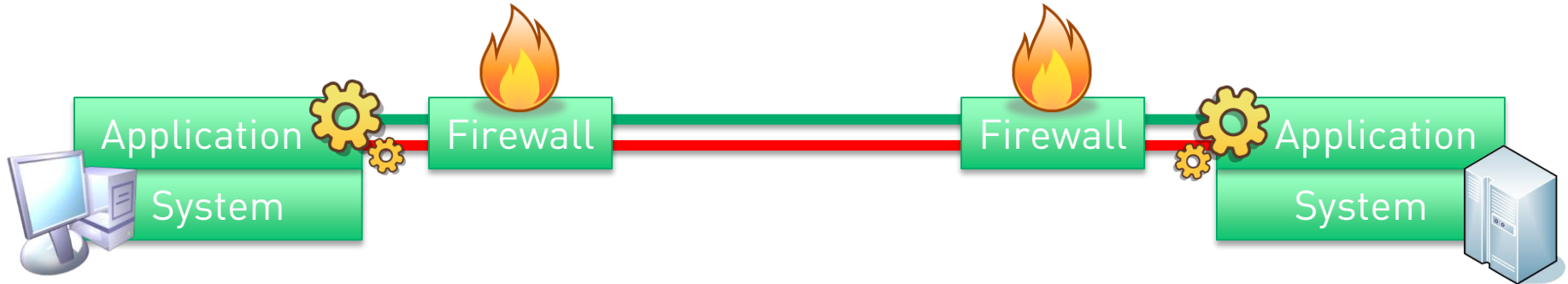
IDPS

¬ You MUST decrypt and (header-wise) scrub the traffic before entering the IDPS. Alternatively you might just drop all packets with EHs, see above.

Forget about State

```
permit tcp any host 2003:60:4010:10A0::11 eq smtp
permit tcp any host 2003:60:4010:1090::11 eq www
permit tcp any host 2003:60:4010:1090::11 eq 443
```

¬ Again, it's back to the roots:
  – On the network layer look at *packets*.
  – The concept of "connections & circuits" might be hard to maintain.

¬ Stateless ACLs will be good enough.
  – "Good enough" is just that.

¬ Again, you might keep the *stateful* stuff for compliance reasons...

Last but not Least

It's not about feature parity

¬ **IPv6 is very different from IPv4**

  – So is IPv6 security.

¬ **Don't rely on transforming v4 models 1:1 to v6. Do not!**

¬ **Think *feature suitability* instead.**

Summary

¬ Understanding the (security) differences between IPv4 & IPv6 helps to come up with reasonable controls.

¬ Most threats can (and should) be addressed on the network level.

¬ Quite some people mostly think about FHS but long-term probably routing approach most important.

¬ All these are common elements of an enterprise IPv6 security strategy.

There's never enough time…

THANK YOU…   **…for yours!**

🐦 @Enno_Insinuator

✉ erey@ernw.de

Slides & further information:
https://www.troopers.de
https://www.insinuator.net
(..soon)

Questions?

Image Credits

¬ Icons made by Freepik
are licensed by CC 3.0 BY.