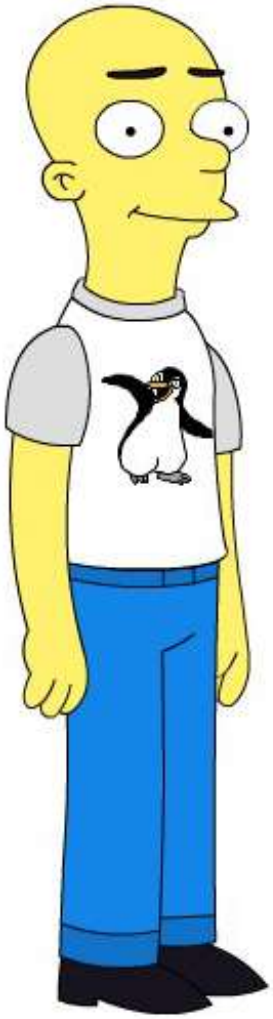
IPv6 – Risiken & Nebenwirkungen unbeabsichtigt?

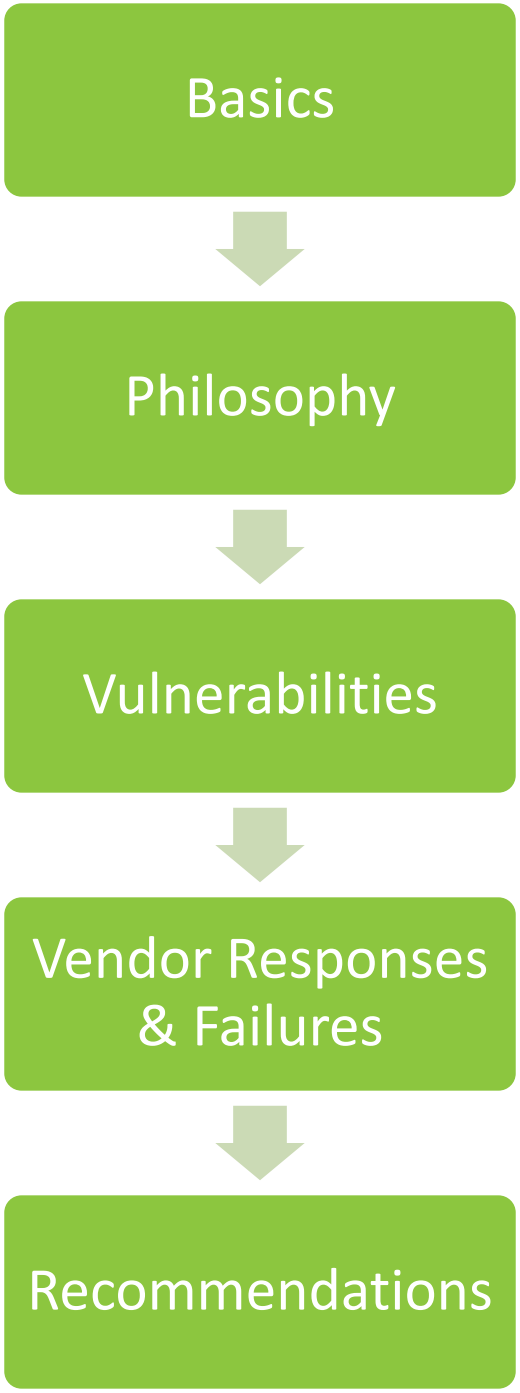
Marc “van Hauser” Heuse

main.IT 2012

© 2012 Marc Heuse <mh@mh-sec.de>

Hallo …




Basics
Philosophy
Vulnerabilities
Vendor Responses & Failures
Recommendations


Devil
inside

Basics

© 2012 Marc Heuse <mh@mh-sec.de>

Episode 2

"In a distant future ...
IPv6 will come.
Maybe.
Hopefully never!"


The future is here already
STAR WARS
adidas

IPv4

4 octets

4.294.967.296 addresses

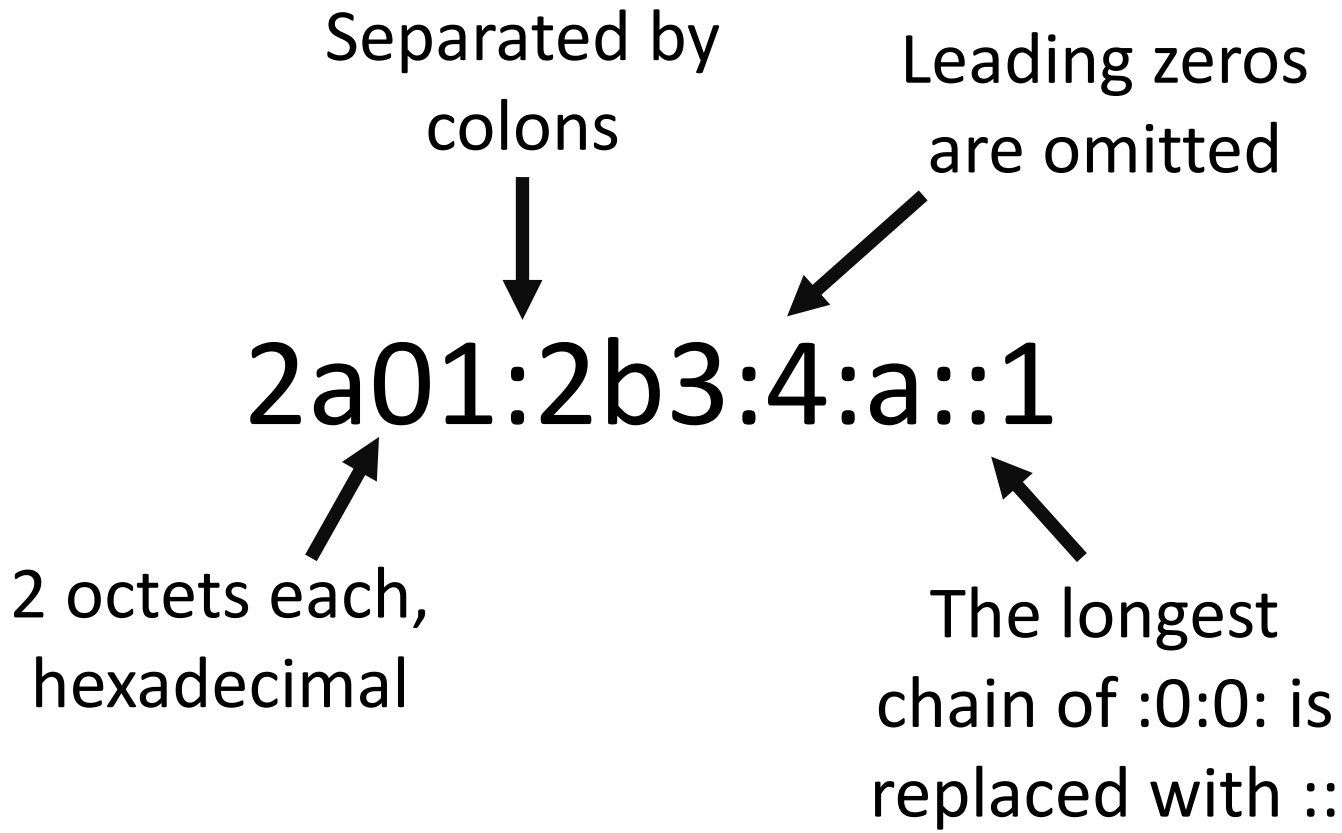
192.168.1.1

IPv6

16 octets

340.282.366.920.938.463.463.374.607.4
31.768.211.456 addresses

2a01:2b3:4:a::1


Separated by colons
Leading zeros are omitted
2a01:2b3:4:a::1
2 octets each, hexadecimal
The longest chain of :0:0: is replaced with ::

Subnets are /64

4.294.967.296 x the size of the Internet!

Features!

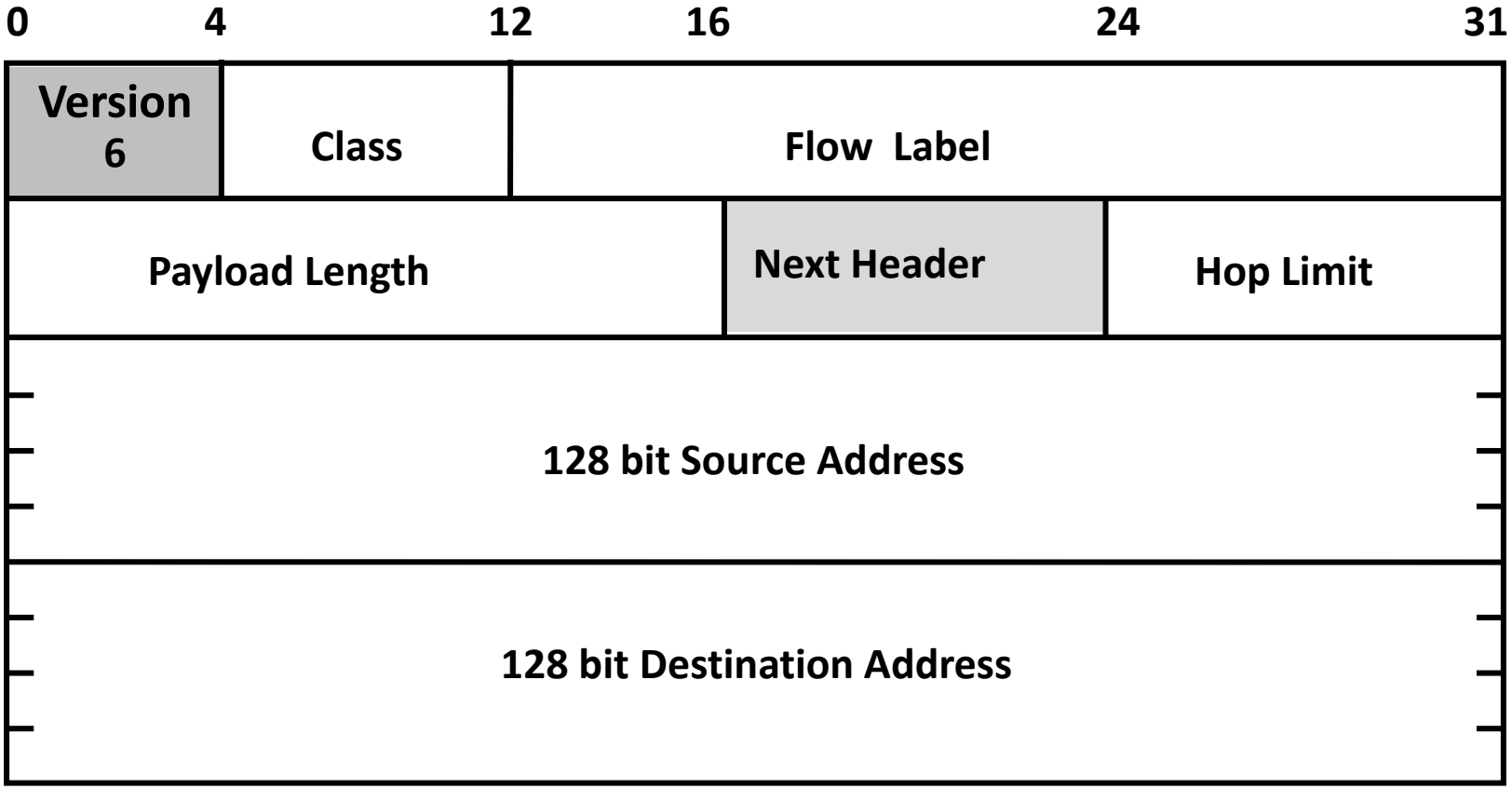
Autoconfiguration

IPSEC

Mobility

Enough addresses!

IPv6 header layout



Philosophy

© 2012 Marc Heuse <mh@mh-sec.de>

Eliminate IPv4

True end-to-end communication

No NAT

No fragmentation
by routers

No defragmentation
by firewalls

Many ICMPv6 msgs
must pass the firewall

“IPv6 is secure”

IPv6 has mandatory IPSEC

Security Model is from 1995

Local = Trusted

Security = Encryption

Security = Filter Rules

Networking + Features > Security

From networkers for networkers

Features

Features!

FEATURES !!!

Goal #1
Network Efficiency

Goal #2
Network Features

Goal #436
some security

Blatant mistakes

~~No DNS server in autoconfiguration~~

IPSEC does not work with multicast

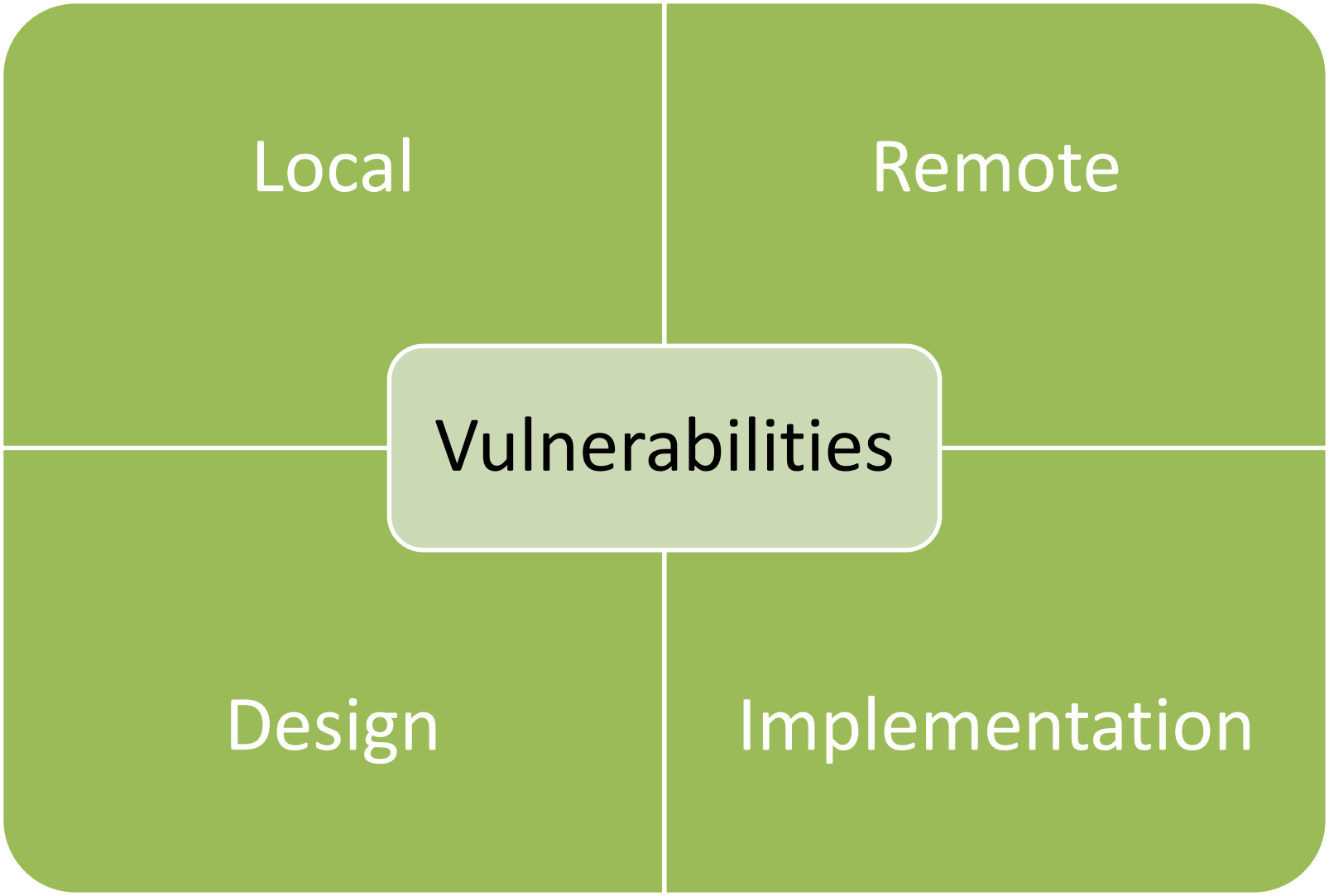
~~No private addresses~~

Many protocol security design problems

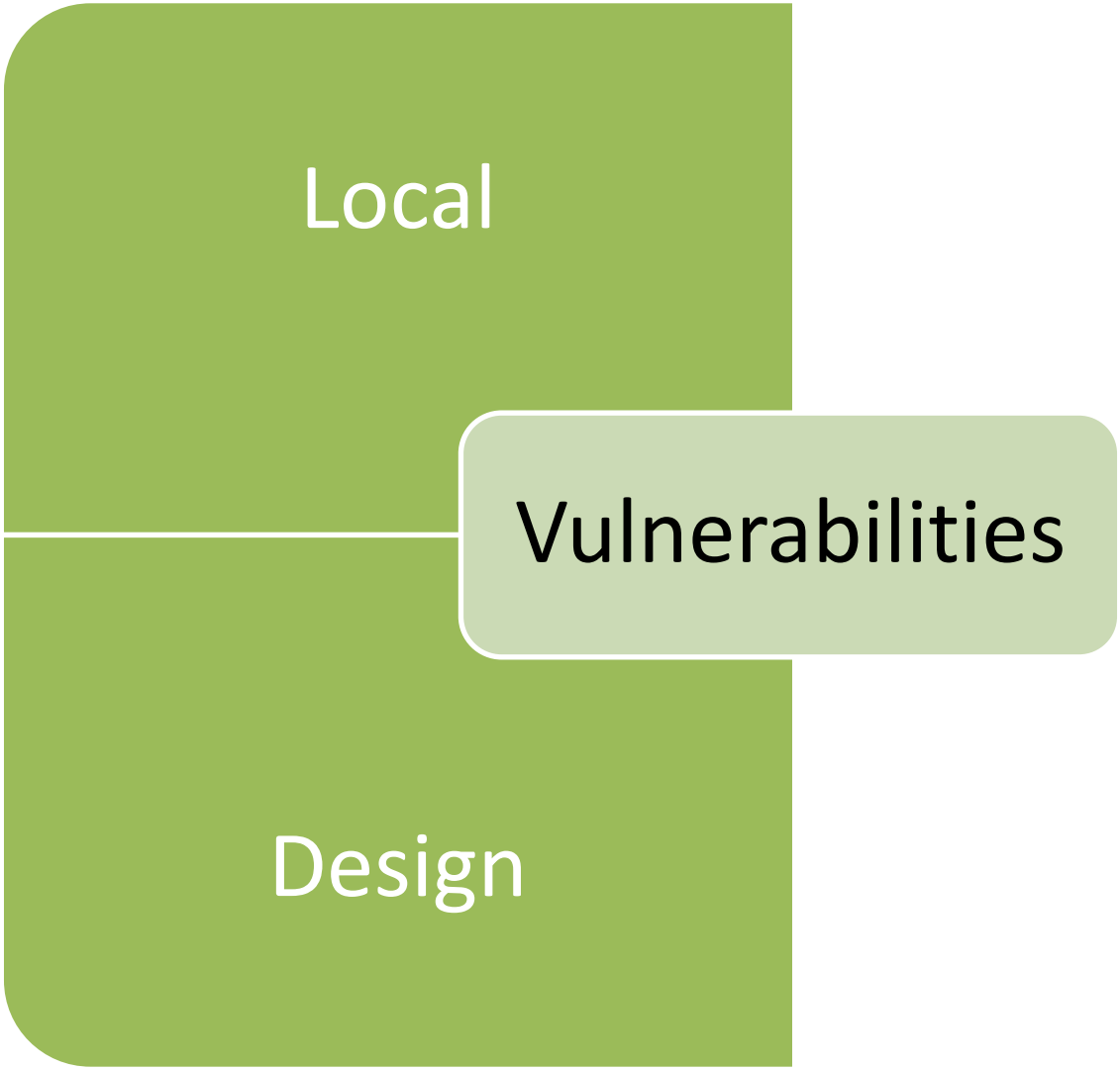
However, good progress since end of 2011

Vulnerabilities

© 2012 Marc Heuse <mh@mh-sec.de>


Local
Remote
Vulnerabilities
Design
Implementation

small, small, small excerpt!


Local
Vulnerabilities
Design

Neighbor Discovery Spoofing

1. NS:
   ICMP Type = 135
   Src = A
   Dst = All-Nodes Multicast
   Query= Who-has IP B?

parasite6:
Answers to every NS, claims to be every system on the LAN

2. NA:
   ICMP Type = 136
   Src = B
   Dst = A
   Data= MAC

"ARP spoofing" in IPv4
more dangerous due "OVERRIDE" flag

Source: common knowledge

Tool: parasite6

Router Advertisement Spoofing

fake_router6:
Sets any IP as default router, defines network prefixes and DNS servers

ICMP Type = 134
Src = Router Link-local Address
Dst = FF02::1
Data= options, prefix, lifetime, autoconfig flag

many, many attacks

Source: common knowledge

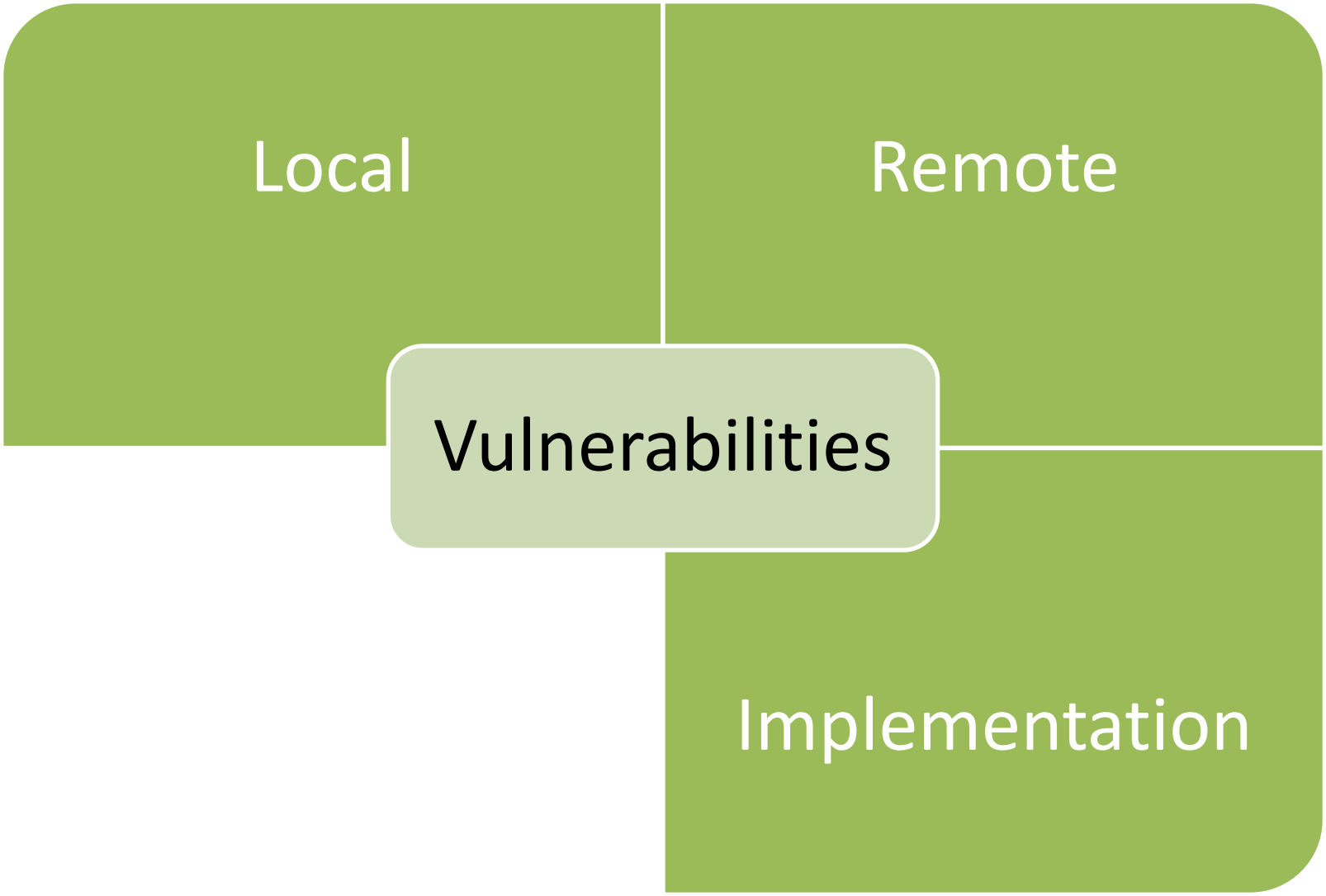
Tool: fake_router6

Router Advertisement Spoofing

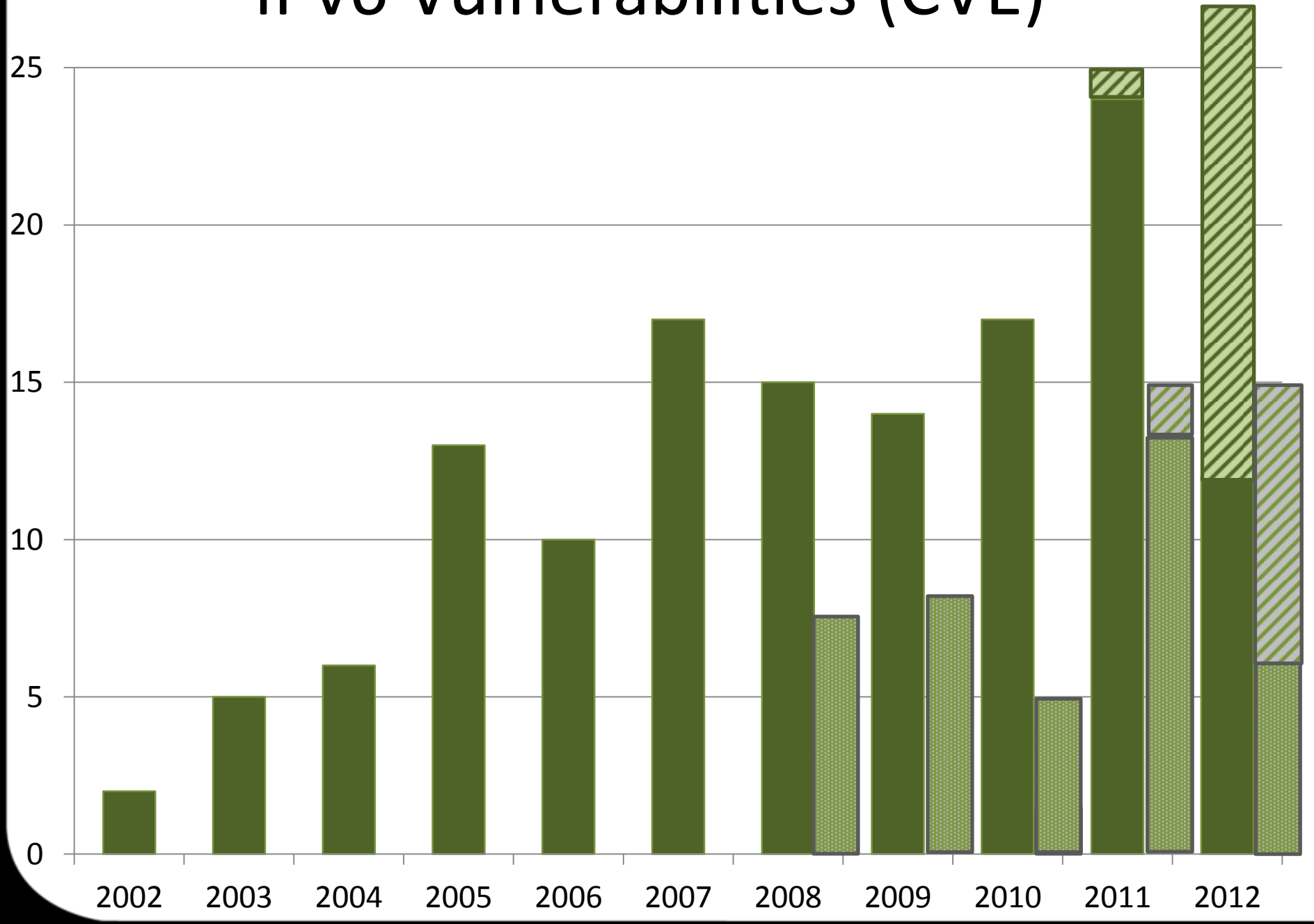
- Become the default router
  - MITM
- Assign multiple address spaces
  - Paypal, Ebay, Amazon, Google == local
  - MITM
- Remove real routing entry (spoofing lifetime 0)
  - DOS

Router Advertisement Spoofing

- Turns IPv4 networks into Dual Stack environments
  - MITM to remote dual stack targets
  - Attack on IPv6 address potentially bypasses personal firewall


Local
Remote
Vulnerabilities
Implementation

IPv6 Vulnerabilities (CVE)



Router Advertisement Flooding

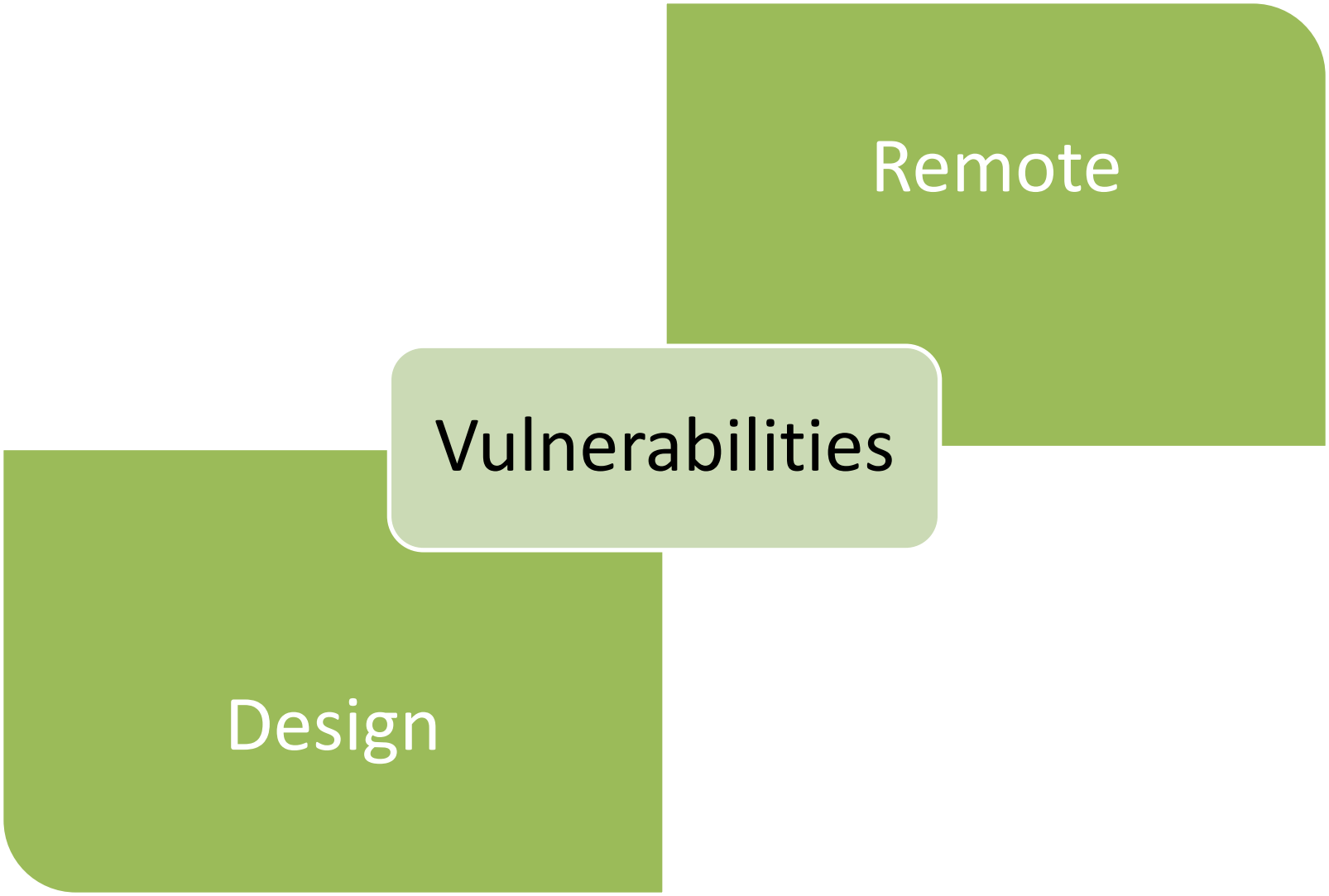
Flood LAN with random RAs.

DOS:

- Windows 7, 2008, 2003, XP
- Cisco IOS+ASA (fixed)
- Juniper Netscreen
- FreeBSD (should be fixed)

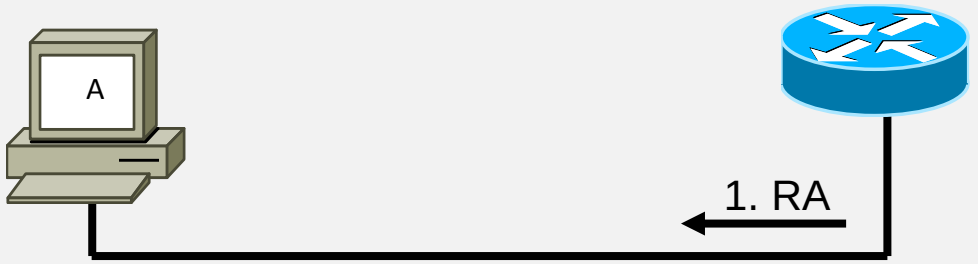
Source: Marc Heuse

Tool: flood_router6


Remote
Vulnerabilities
Design

Privacy Issues in Autoconfiguration

Autoconfiguration: host address based on MAC address



ICMP Type = 134
Src = Router Link-local Address
Dst = FF02::1
Data= options, prefix, lifetime, autoconfig flag

MAC address: **00:0c:29:69:a6:66**

IPv6 host address: ::**02**0c:29**ff:fe**69:a666

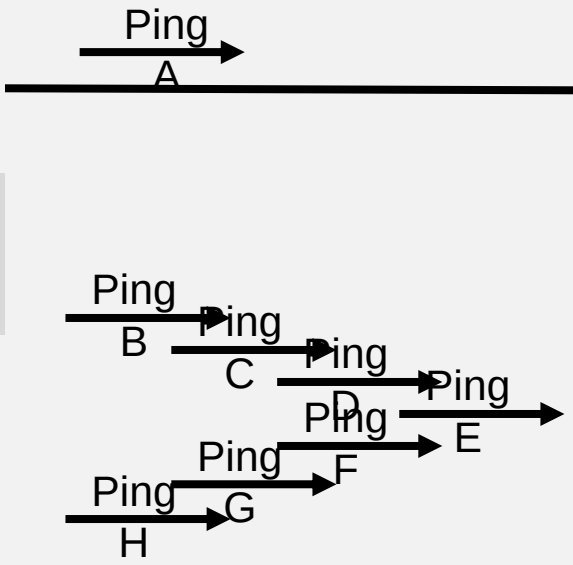
Identify a host wherever it travels

Source: common knowledge

Tool: not needed

NDP Exhaust

ndpexhaust6:
Flood the target network with ping6



1. NS:
ICMP Type = 135
Src = Router
Dst = All-Nodes Mulitcast
Query= Who-has IP A?

Router will drop packets as queue fills

Source: common knowledge

Tool: ndpexhaust6

Do not try this here

www.thc.org/thc-ipv6


COCAINE.
SO MUCH COCAINE.

Vendor Responses & Failures

© 2012 Marc Heuse <mh@mh-sec.de>

The complexity problem™

So many:

- extension headers
- options in extension headers
- possibilities of orders of headers and options

additions & changes happen regular

The vendor solution:

Different support of options

Different maturity

Changes with every update

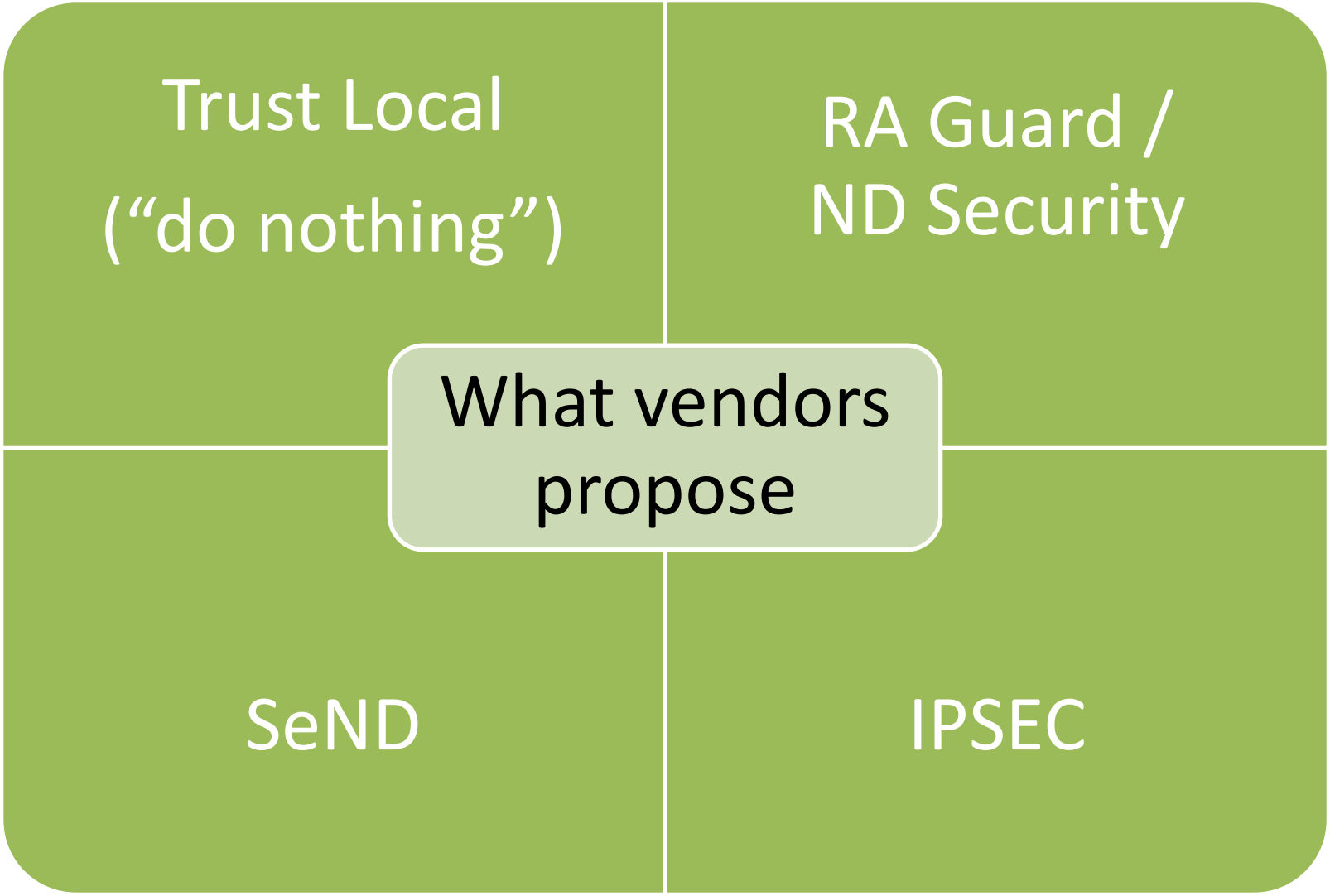
↓

“Product supports IPv6” means nothing

Firewalls

IPv4: Whitelist / Deny anything unknown

IPv6: Blacklist / Drop anything known evil


Trust Local
("do nothing")
RA Guard /
ND Security
What vendors
propose
SeND
IPSEC

Trust Local
("do nothing")

What vendors propose

a.k.a. as "The Microsoft Approach"™

“We consider this issue to be by design [and will not fix it].

The attack would require that an attacker has access to the targeted network - a situation that does not provide a security boundary.”

Microsoft statement

Microsoft, Juniper urged to patch dangerous IPv6 DoS hole

Despite growing pressure from security experts, Microsoft and Juniper have so far refused to patch a dangerous hole that can freeze a Windows network in minutes.

By Julie Bort, Network World
May 03, 2011 05:26 PM ET

1 Comment Print

Security experts are urging Microsoft and Juniper to patch a year-old IPv6 vulnerability so dangerous it can freeze any Windows machine on a LAN in a matter of minutes.

Microsoft has downplayed the risk because the hole requires a physical connection to the wired LAN. Juniper says it has delayed a patch because the hole only affects a small number of its products and it wants the IETF to fix the protocol instead.

SEE IT YOURSELF: How to use a known IPv6 hole to fast-freeze a Windows network

The vulnerability was initially discovered in July 2010 by Marc Heuse, an IT security consultant in Berlin. He found that products from several vendors were vulnerable, including all recent versions of Windows, Cisco routers, Linux and Juniper's Netscreen. Cisco issued a patch in October 2010, and the Linux kernel has since been fixed as well. Microsoft and Juniper have acknowledged the vulnerability, but neither have committed to patches.

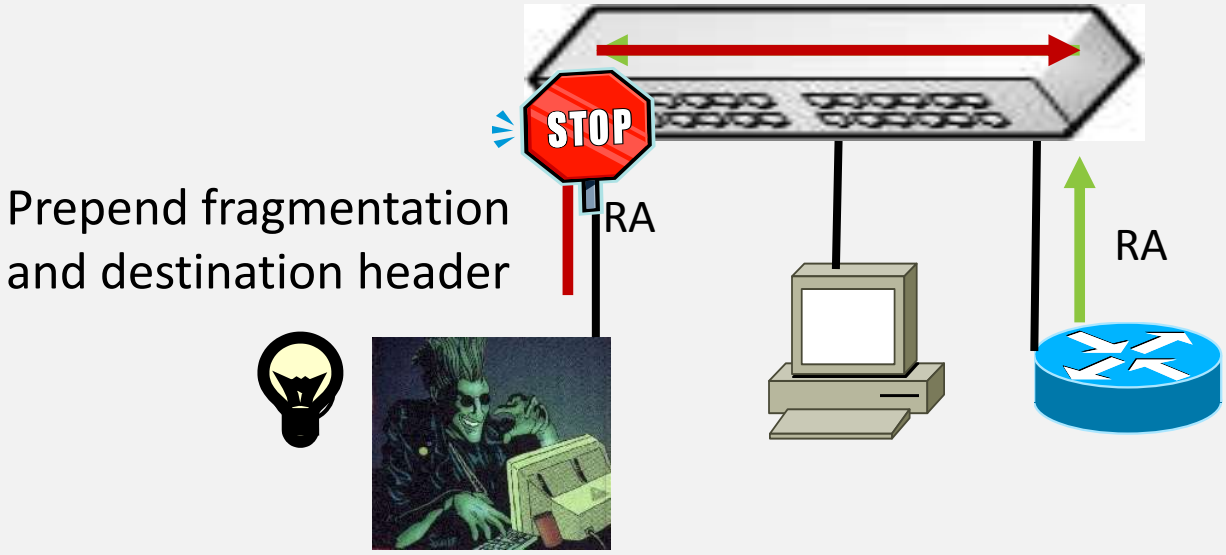
The hole is in a technology known as

Source: http://www.networkworld.com/news/2011/050311-microsoft-juniper-ipv6.html

RA Guard / ND Security

What vendors propose

RA Guard / ND Security Bypass



RA

Destination Options (large & empty)

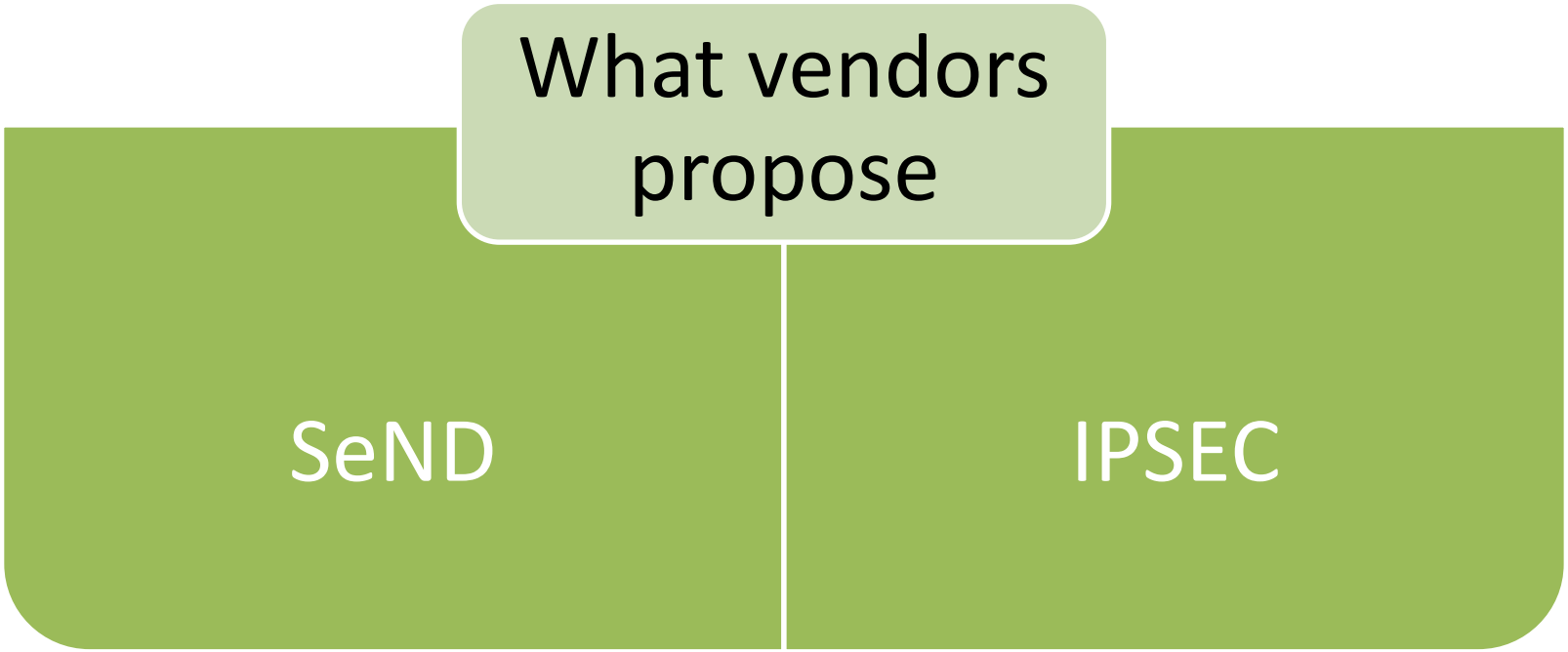
Fragmentation

IPv6

It is not a standard, has patents and is Cisco only.

Source: Marc Heuse

Tool: fake_router6


What vendors propose
SeND
IPSEC

Problems!

All devices must support it (printers!)

No privacy extensions possible

Key distribution => big overhead

Only protects RA & ND (SeND)

SeND DOS

1. NS:
   ICMP Type = 135
   Src = A
   Dst = All-Nodes Mulitcast
   Query= Who-has IP B?
   CGA = signing information

Flood NS:
   ICMP Type = 135
   Src = Attacker
   Dst = All-Nodes Mulitcast
   Data= MAC
   CGA = fake signing information

CGA verification => CPU expensive

Flood => DOS

Source: Will Damn

Tool: seenpees6

The Problem:
IPv4 thinking applied to IPv6

IPv6 requires a new thinking for

- Designing
- Implementing
- Configuring
- Hacking

Recommendations

© 2012 Marc Heuse <mh@mh-sec.de>

The Good Thing™:

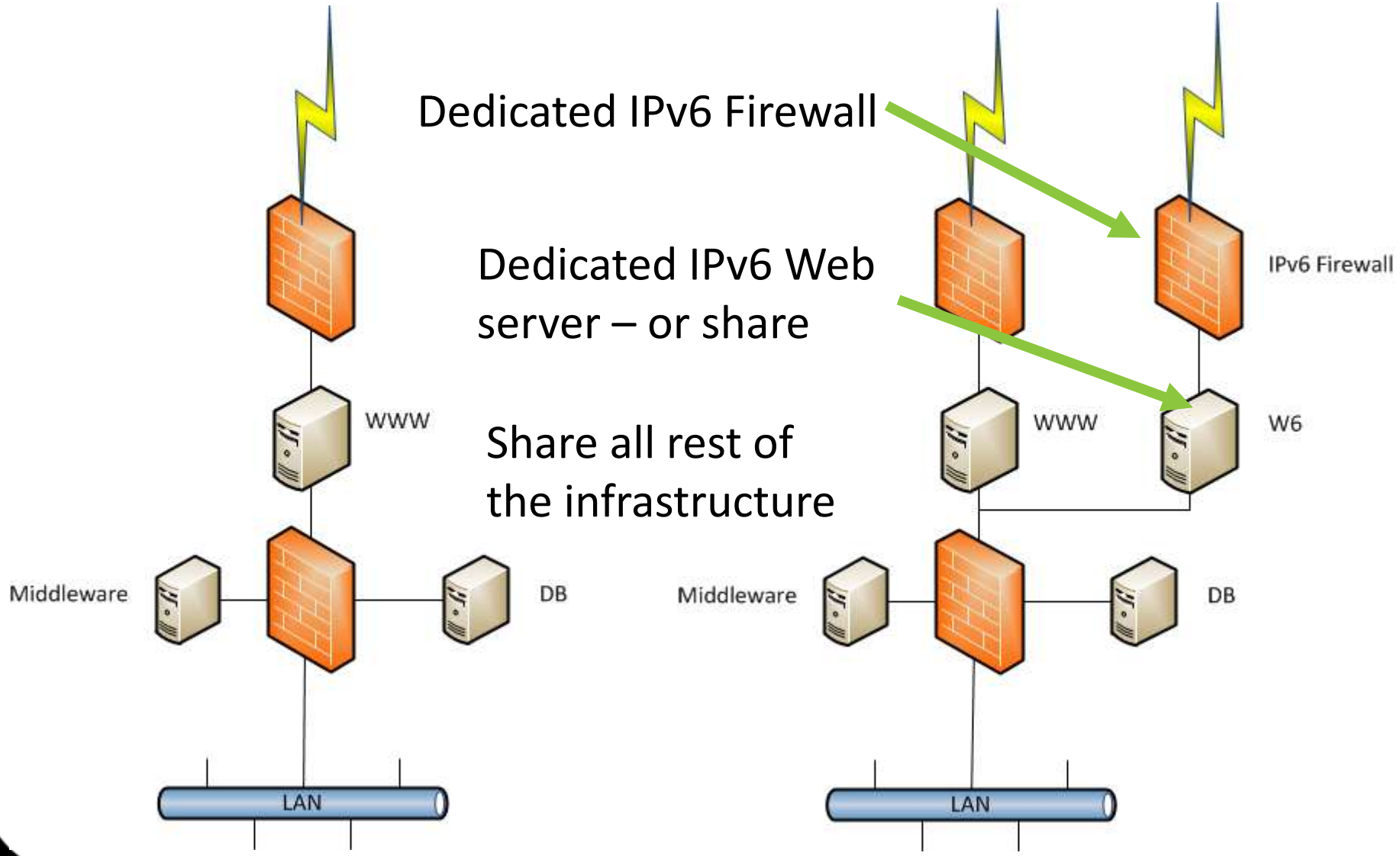
Critical issues are site-local only

Where to deploy IPv6 in the next 2 years?

Front-end DMZ only

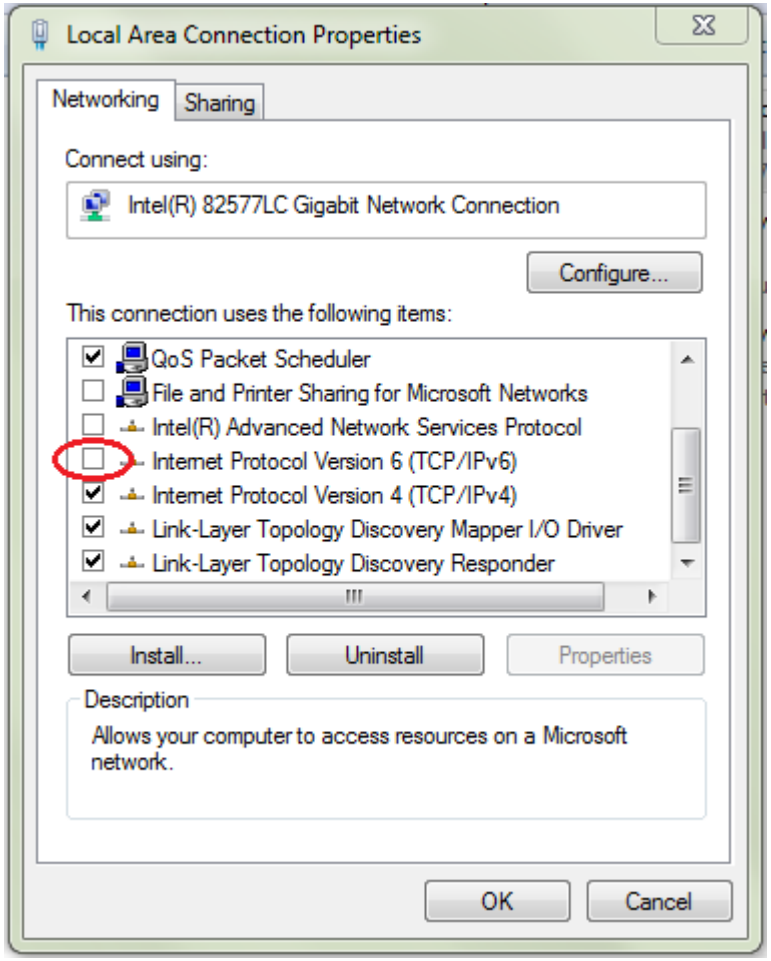
(if you are a “normal” company.
ISPs, Telcos, Universities, etc.: good luck)

How to deploy in the DMZ?



Everywhere else …

- Disable IPv6 on all devices possible



IPv6 requires new thinking

If even vendors can’t do it – who can?

Contact

© 2012 Marc Heuse <mh@mh-sec.de>

Contact

Marc Heuse


+49 (0)177 961 15 60


+49 (0)30 37 30 97 26


mh@mh-sec.de


www.mh-sec.de


winsstrasse 68
d-10405 berlin

End

© 2012 Marc Heuse <mh@mh-sec.de>