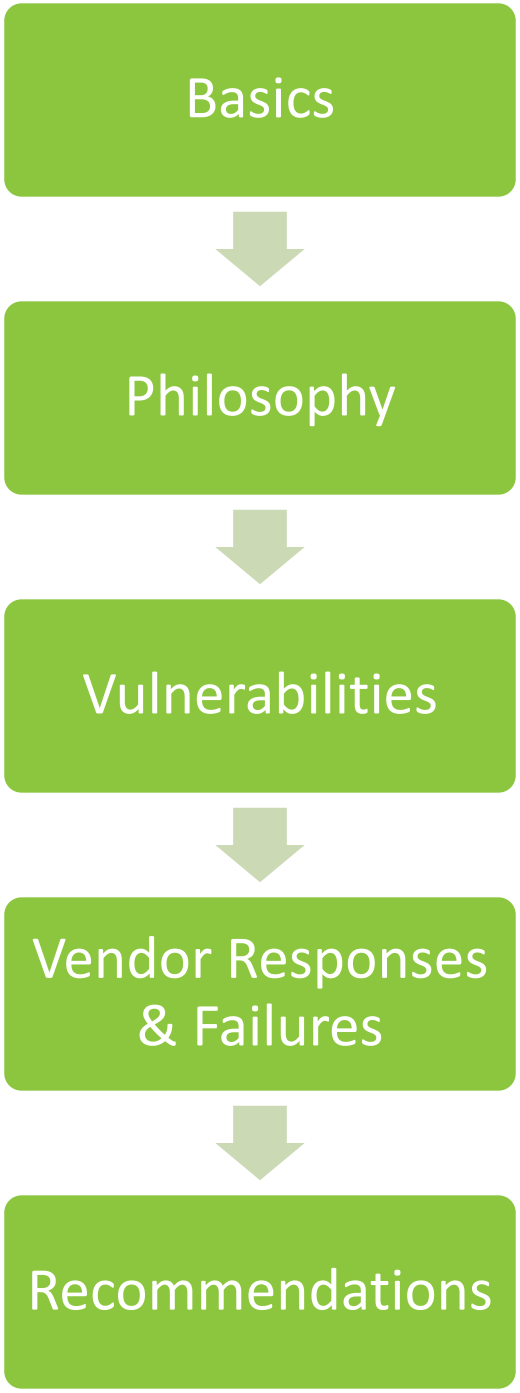
IPv6
Vulnerabilities, Failures - and a Future?

Marc “van Hauser” Heuse

November 2011

Hello, my name is …


Basics
Philosophy
Vulnerabilities
Vendor Responses & Failures
Recommendations


Devil
inside

“There is more money to be made with IPv6 than with Y2K”

me

Basics

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

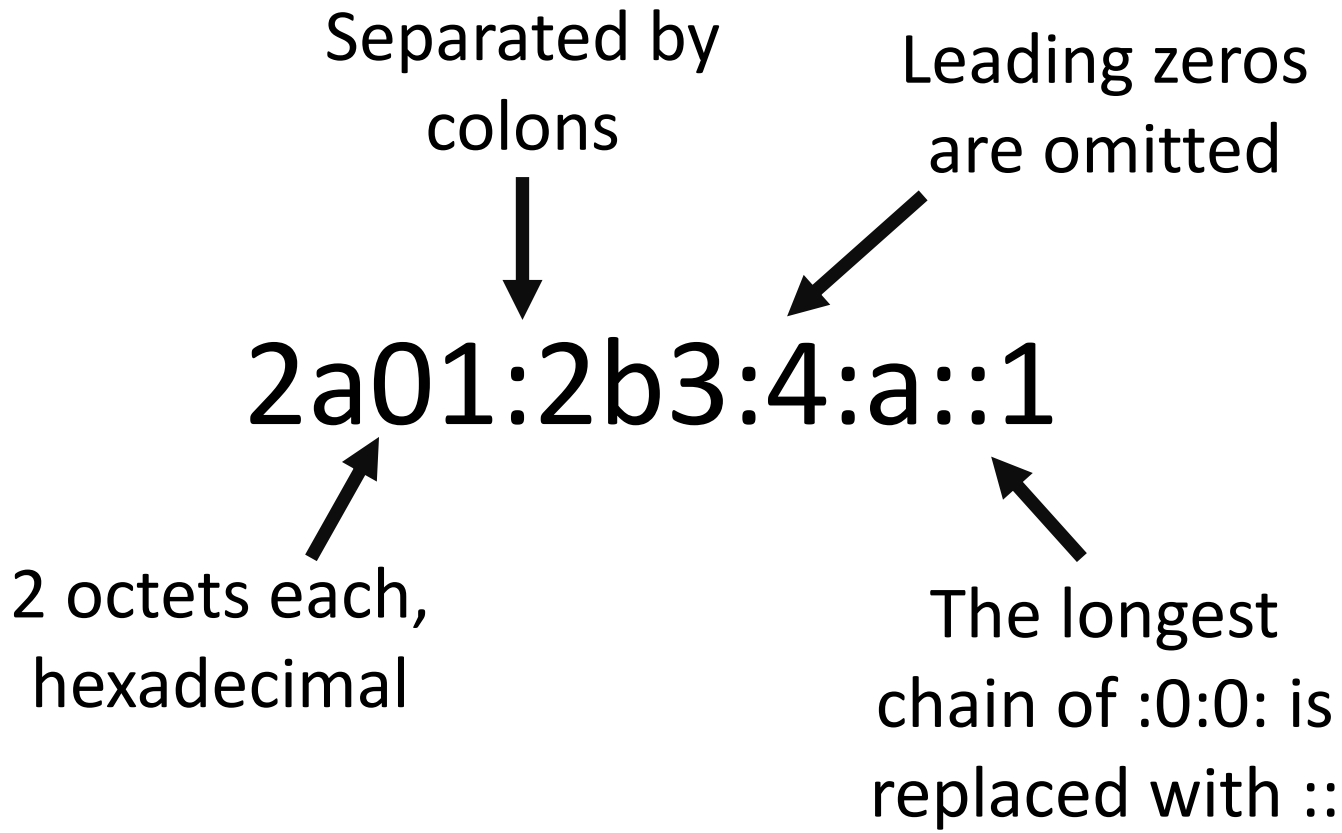
192.168.1.1

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!

No broadcasts

Multicasts, but they are local only

Features!

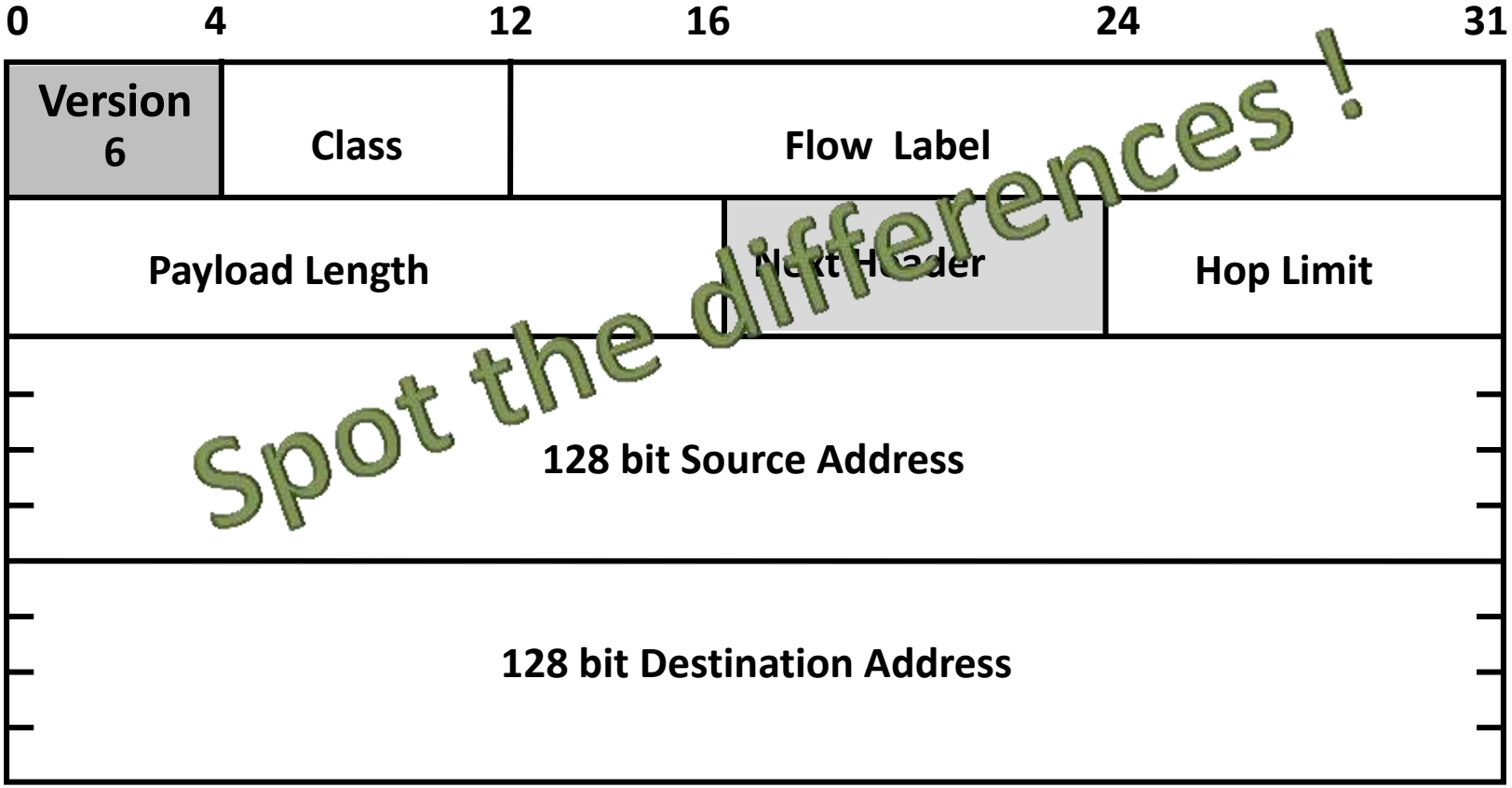
Autoconfiguration

IPSEC

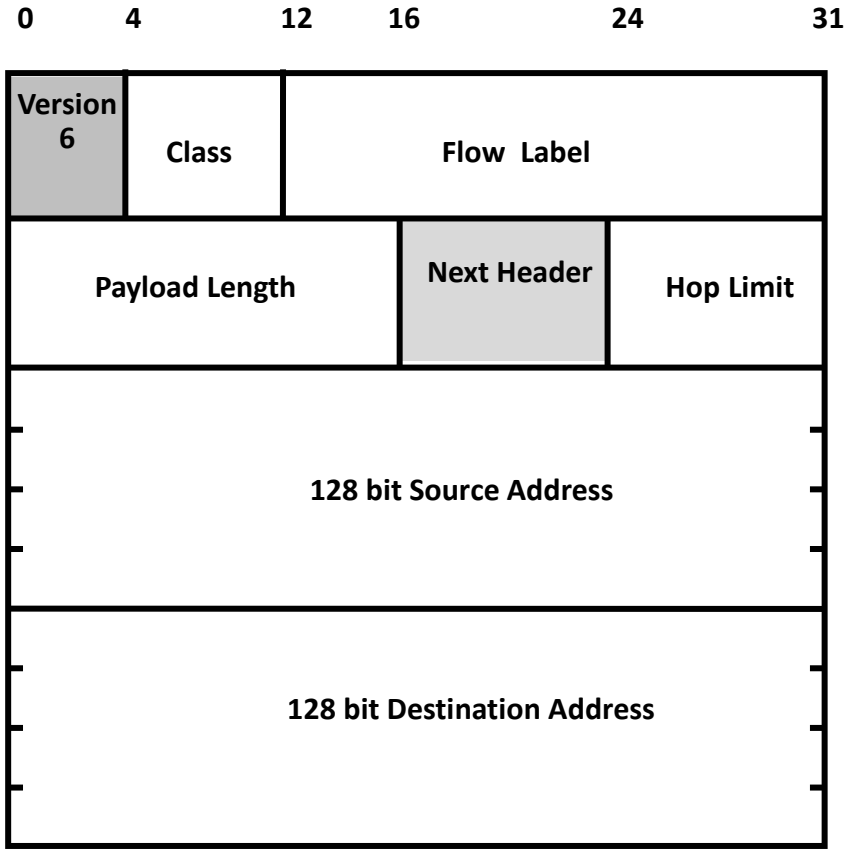
Mobility

Enough addresses!

IPv6 header layout



IPv6 header layout



- No header length
- No identification
- No checksum
- No fragmentation
- No options

Every option is an extension header

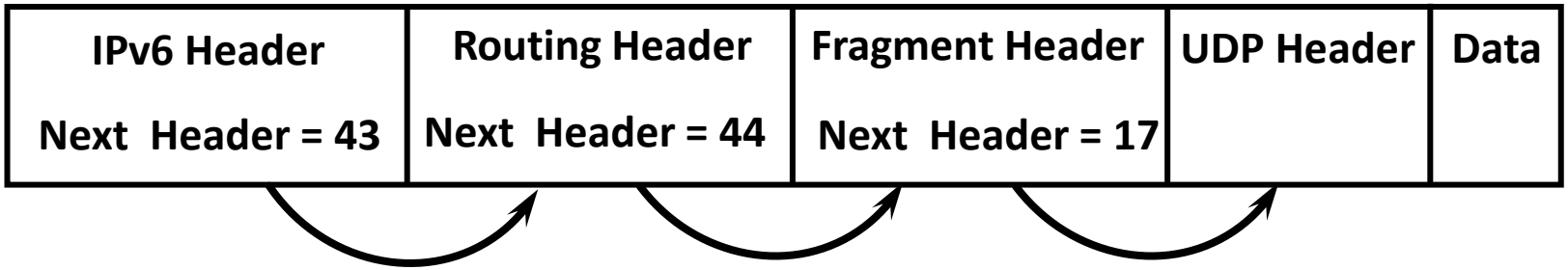
Fragmentation

Source routing

IPSEC

Destination Options

Hop-byHop


IPv6 Header
Next Header = 43
Routing Header
Next Header = 44
Fragment Header
Next Header = 17
UDP Header
Data

Most in IPv6 is OPTIONAL

Mandatory

- Multiple IPv6 addresses per interface
- ARP => ICMPv6
- Router Advertisements
- No router & routes via DHCPv6!
- Multicast (local)

IPv6 is much simpler than IPv4

… in theory.

Philosophy

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

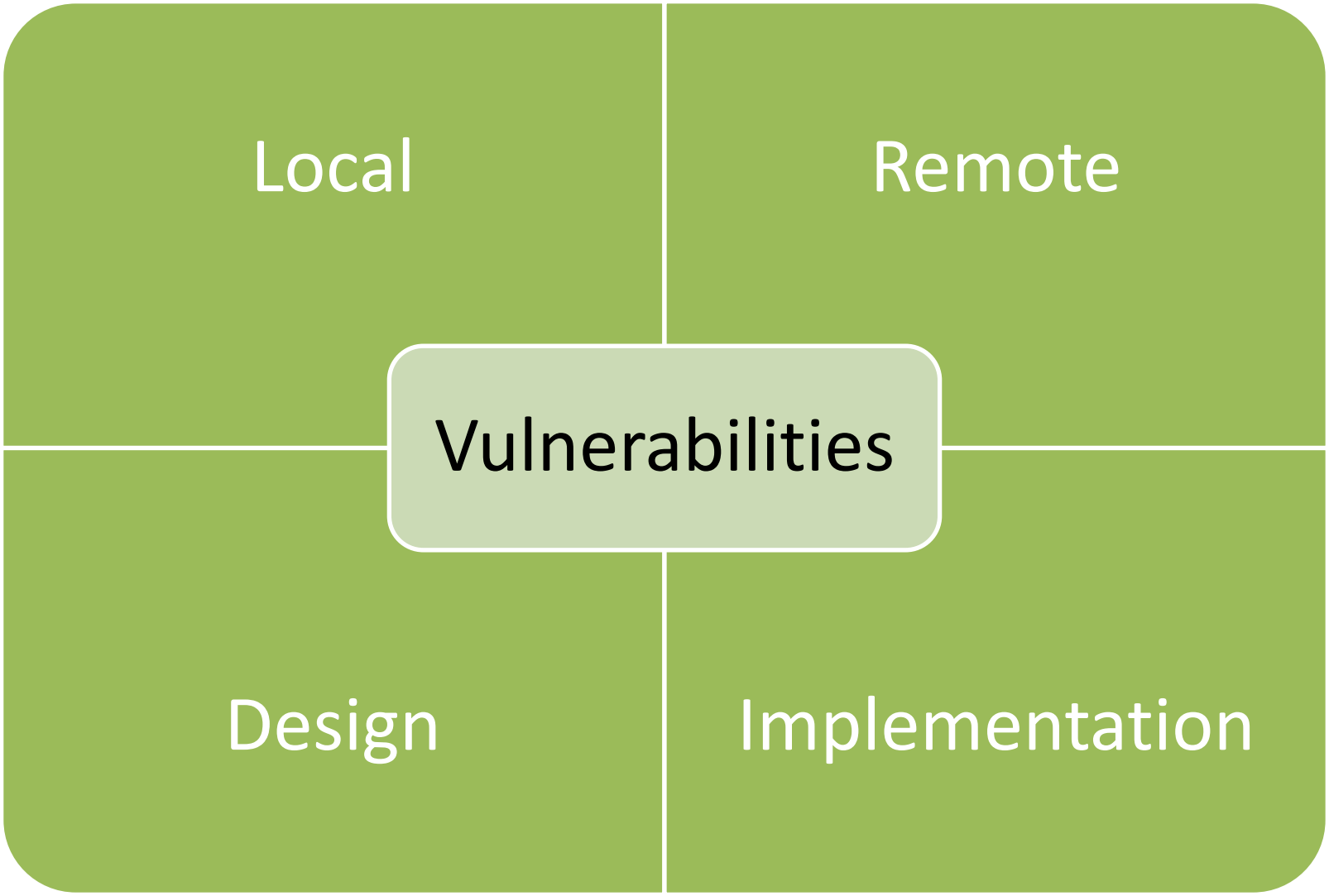
Vulnerabilities

thc-ipv6 – why?

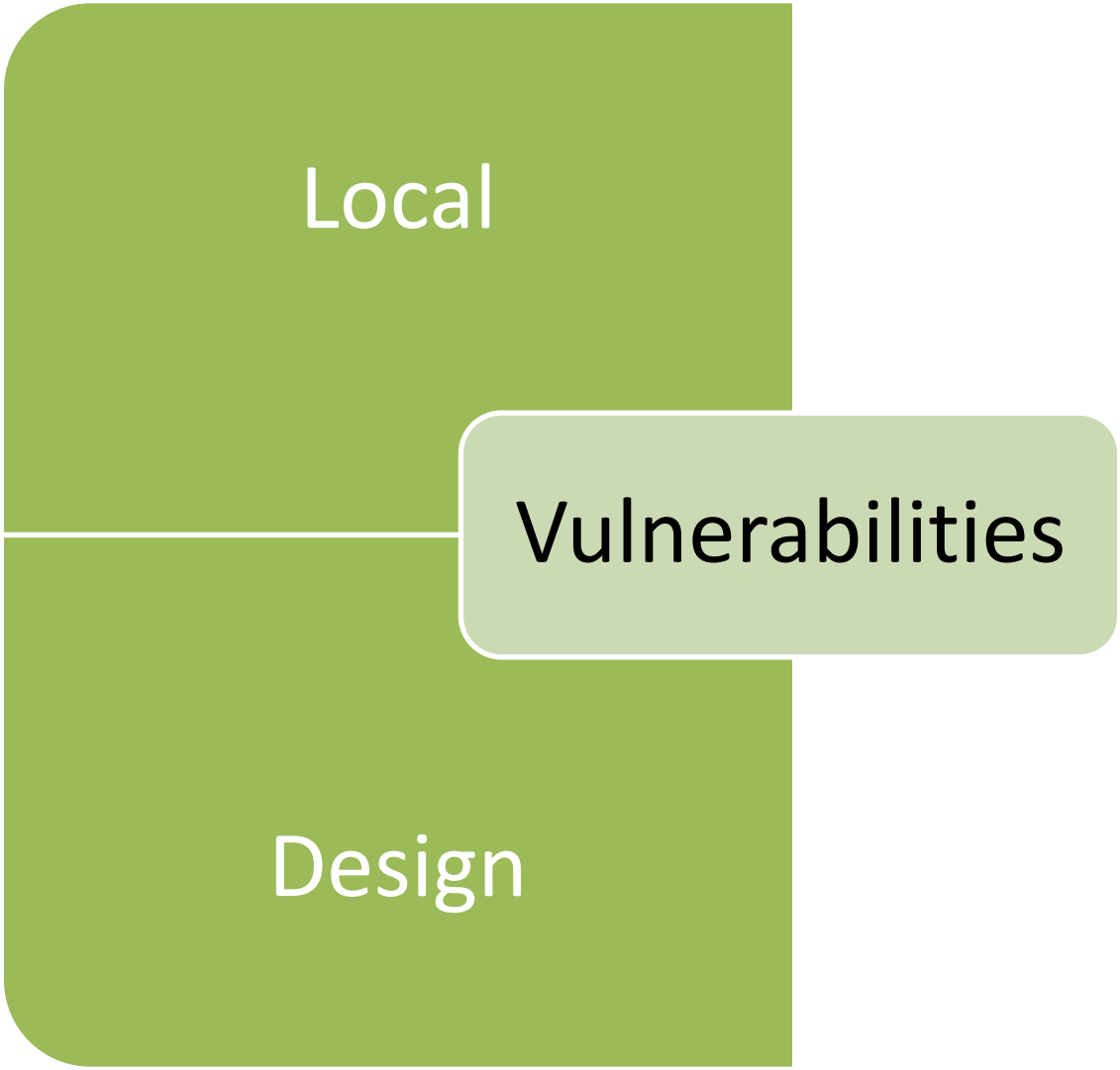
thc-ipv6

- Linux
- Ethernet
- GPLv3

http://www.thc.org/thc-ipv6


Local
Remote
Vulnerabilities
Design
Implementation

Excerpt!


Local
Vulnerabilities
Design

Neighbor Discovery Spoofing

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

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

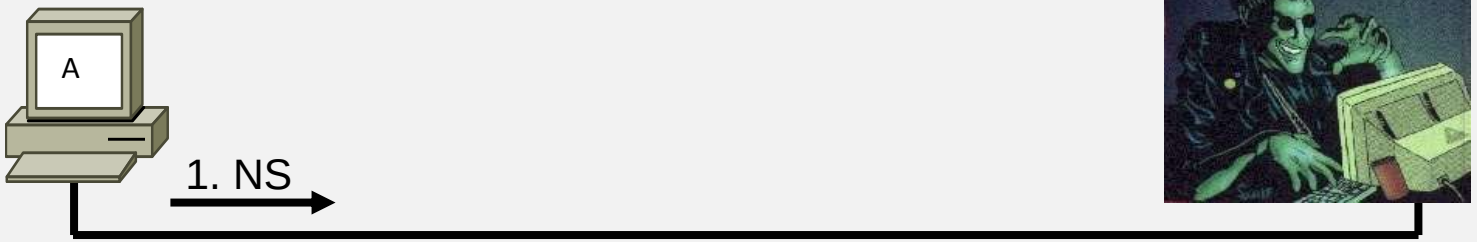
2. NA:
   ICMP Type = 136
   Src = B
   Dst = A
   Data= MAC

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

Source: common knowledge

Tool: parasite6

Duplicate Address Detection DOS



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

dos-new-ipv6:
Answer to every NS, claim to be every system on the LAN

optional in IPv4, mandatory in IPv6 for all addresses

Source: common knowledge

Tool: dos-new-ipv6

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

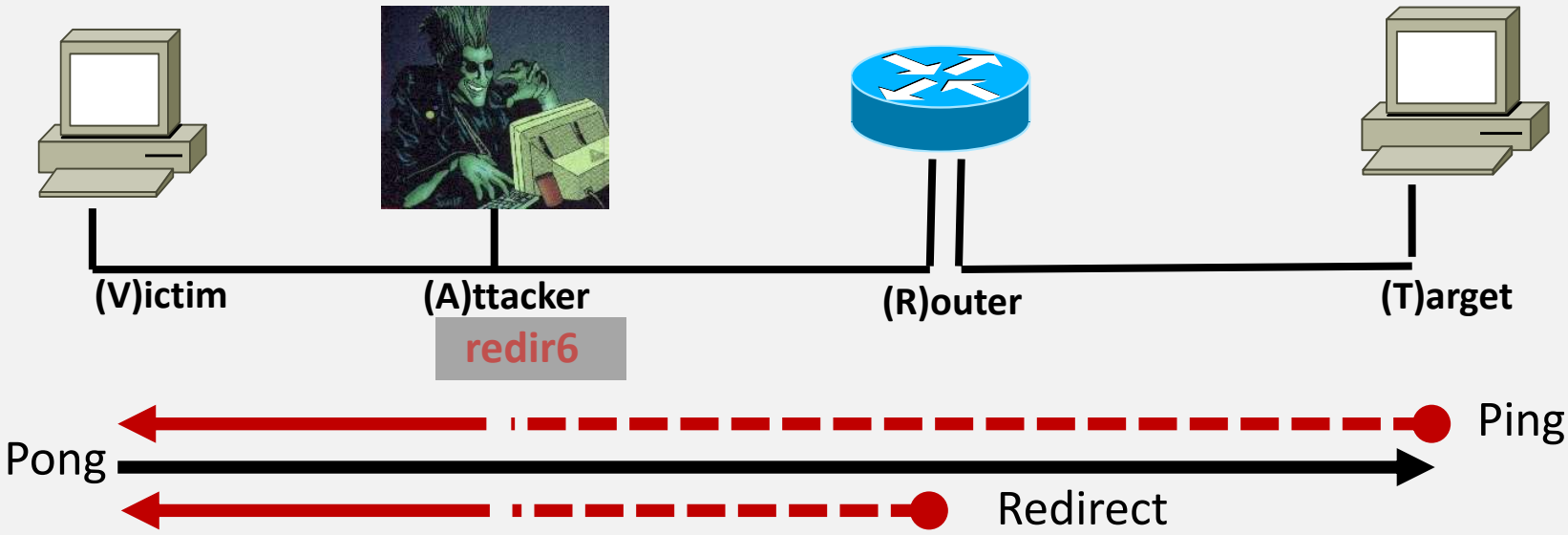
Router Advertisement Spoofing

- 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

ICMP Redirect Spoofing

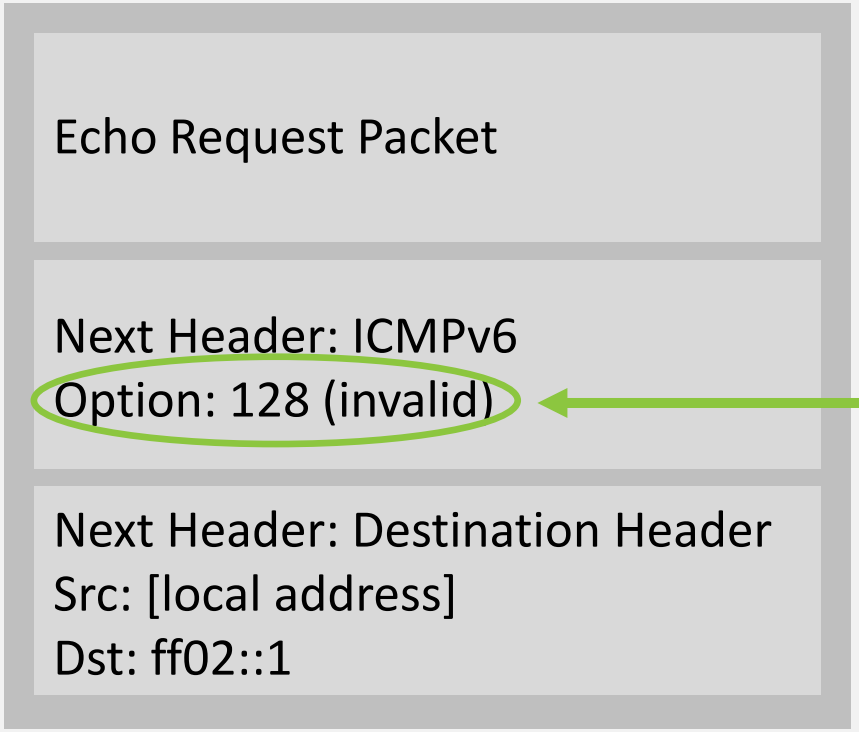


Bypasses “secure redirect” check, default on all OS. IPv4: remote, IPv6: local only

Source: Sebastian Krahmer, Marc Heuse

Tool: redir6

Alive Detection via Multicast



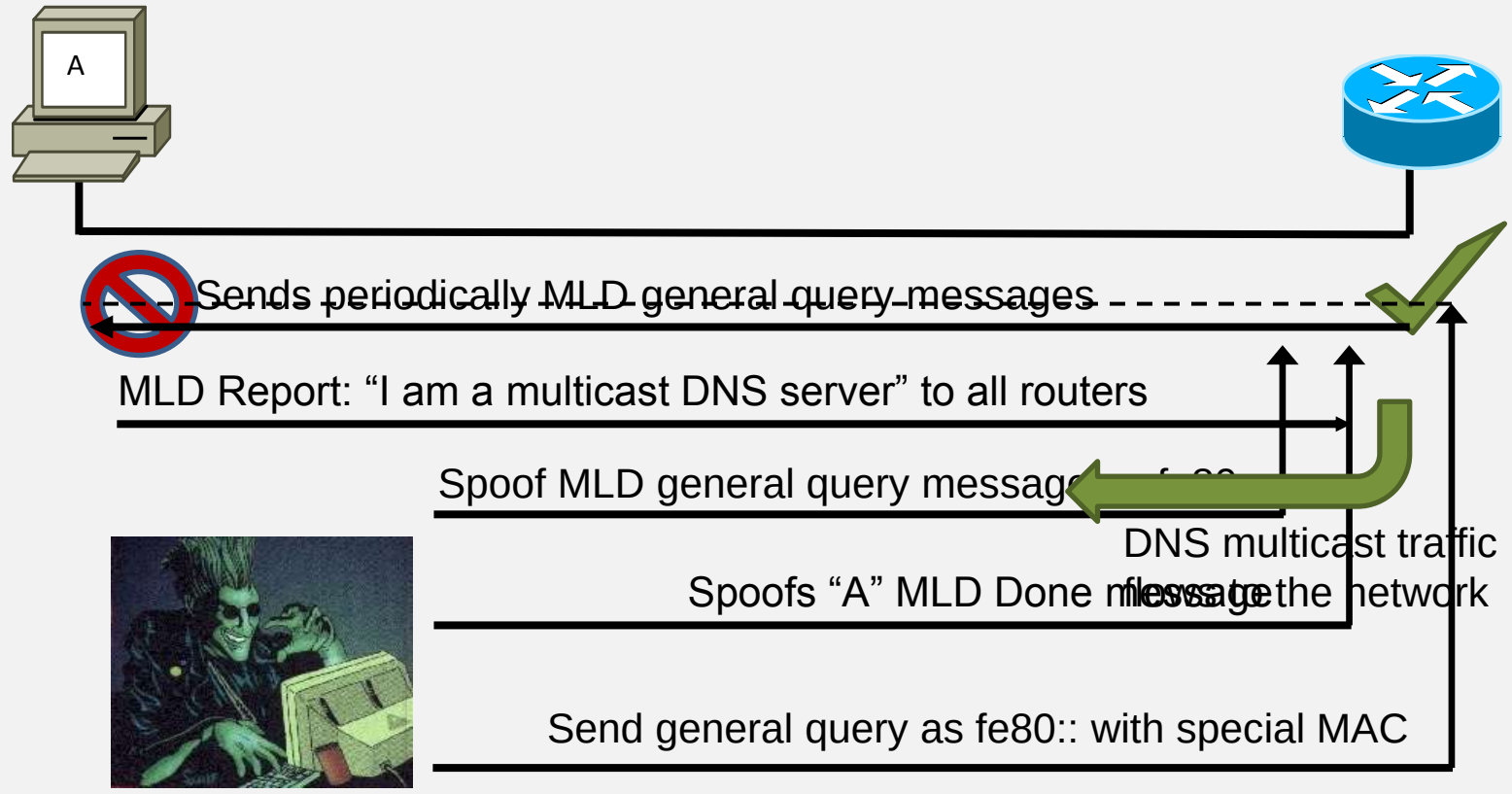
- Detect all local systems with one multicast packet
- Invalid option triggers ICMPv6 error reply from all systems

For ff02::1 you can also do an MLD general query

Source: Marc Heuse

Tool: alive6

Multicast Listener Discovery DOS



Denies site/org multicast traffic to LAN

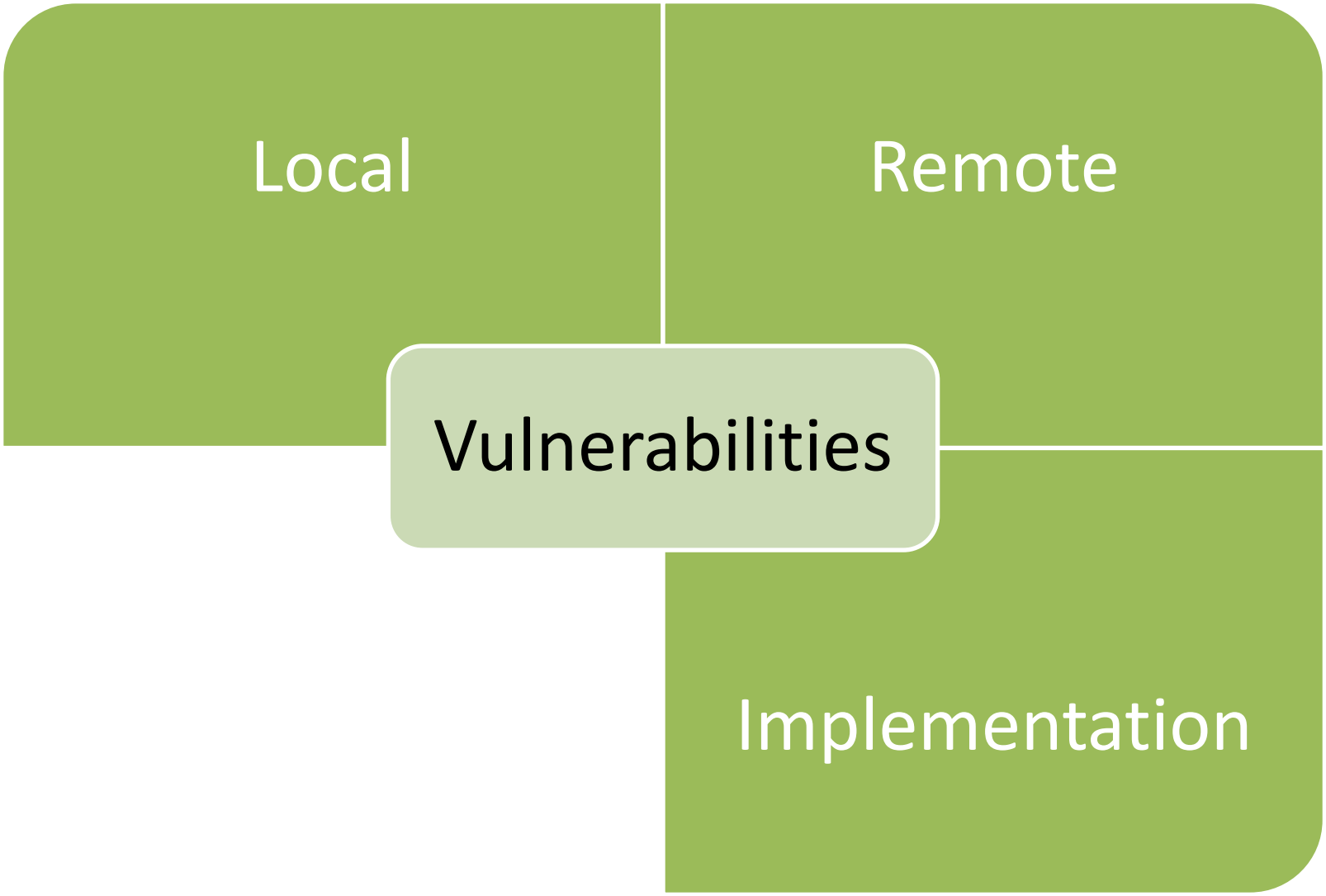
Source: Marc Heuse

Tool: fake_mld6

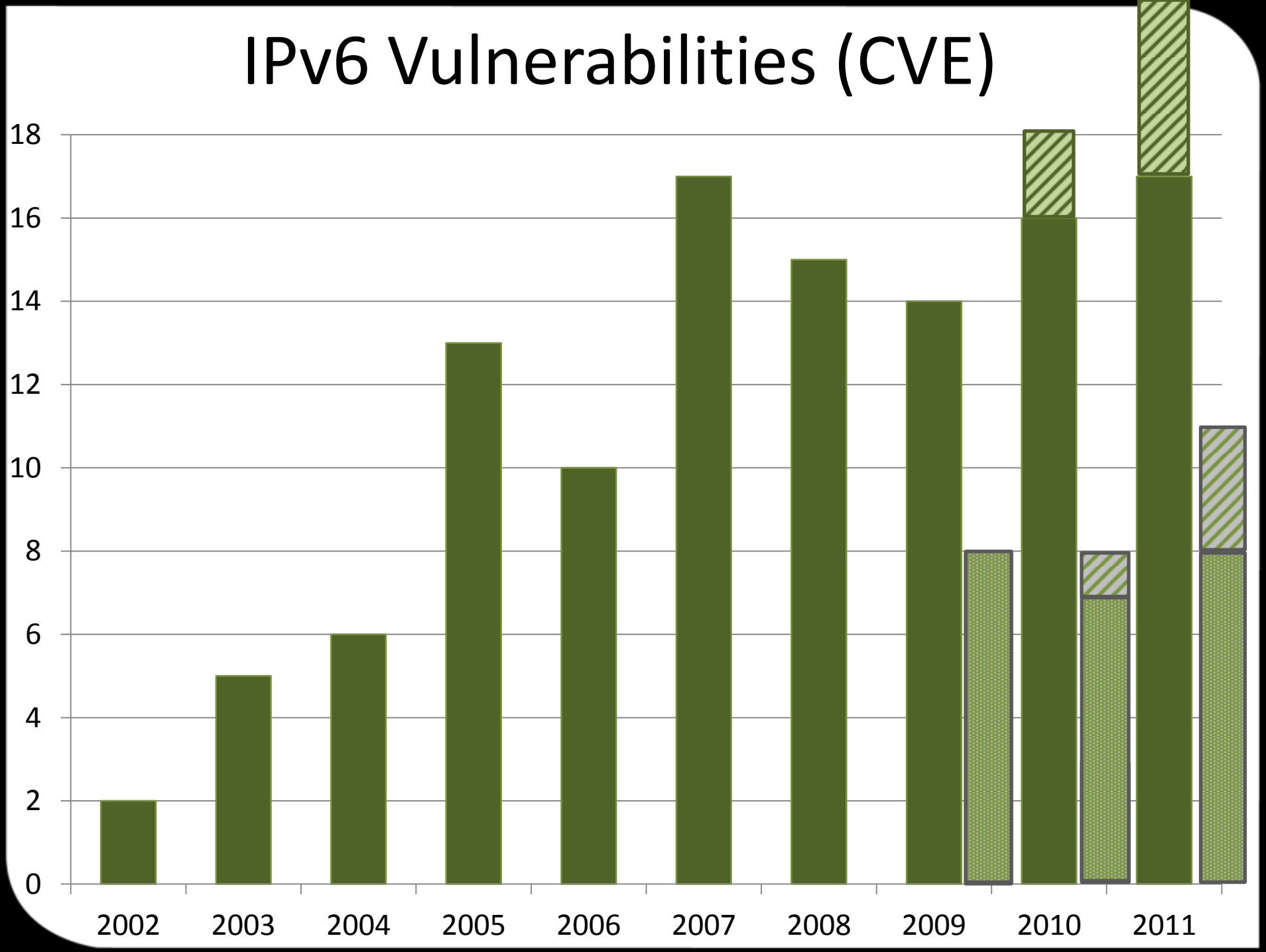
<DHCPv6 & mDNS attacks omitted>

More attack scenarios

- Use multicast to send an exploit to all servers in the organization
- Join multicast addresses and spoof server replies


Local
Remote
Vulnerabilities
Implementation

IPv6 Vulnerabilities (CVE)



Router Advertisement Flooding

Flood LAN with random RAs.

DOS:

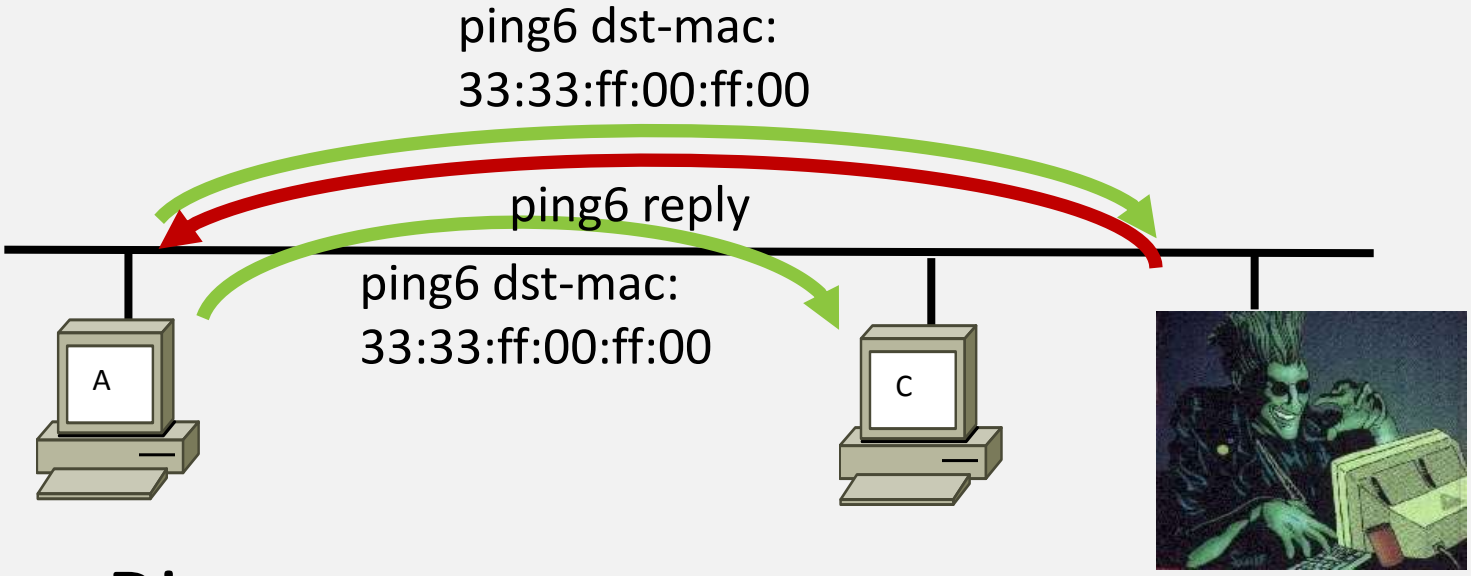
- Windows 7, 2008, 2003, XP
- Cisco IOS+ASA (fixed)
- Juniper Netscreen
- FreeBSD (should be fixed)

Source: Marc Heuse

Tool: flood_router6

Sniffer Detection

Sniffer Detection



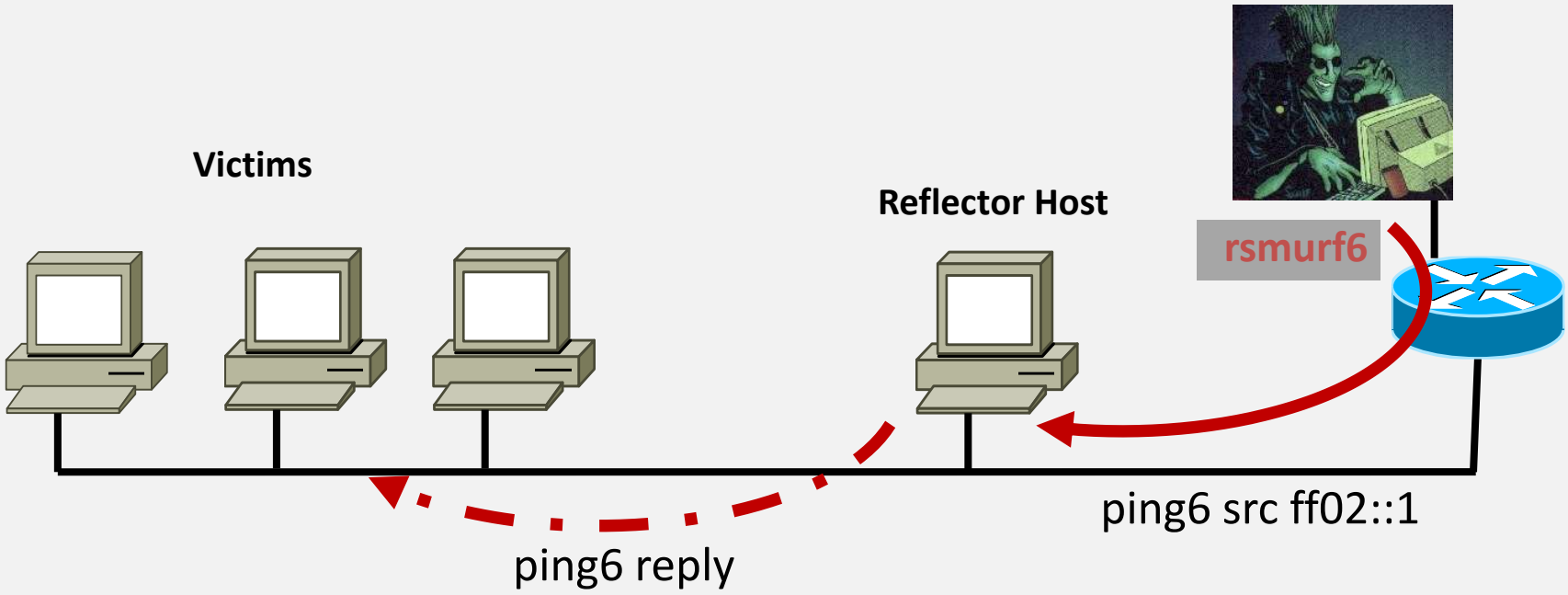
Discover:

- Windows 7, 2008, 2003, XP
- Linux
- FreeBSD

Source: Marc Heuse

Tool: thcping6

Reverse Smurfing



Reflective victims:

- Linux

Source: Marc Heuse

Tool: rsmurf6

Weird stuff

- Speed-up packet transmission by factor x100 on IPv6
  (details to be released in May 2012 ☺)

“Remote alive scans (ping scans) as we know them are unfeasible on IPv6”

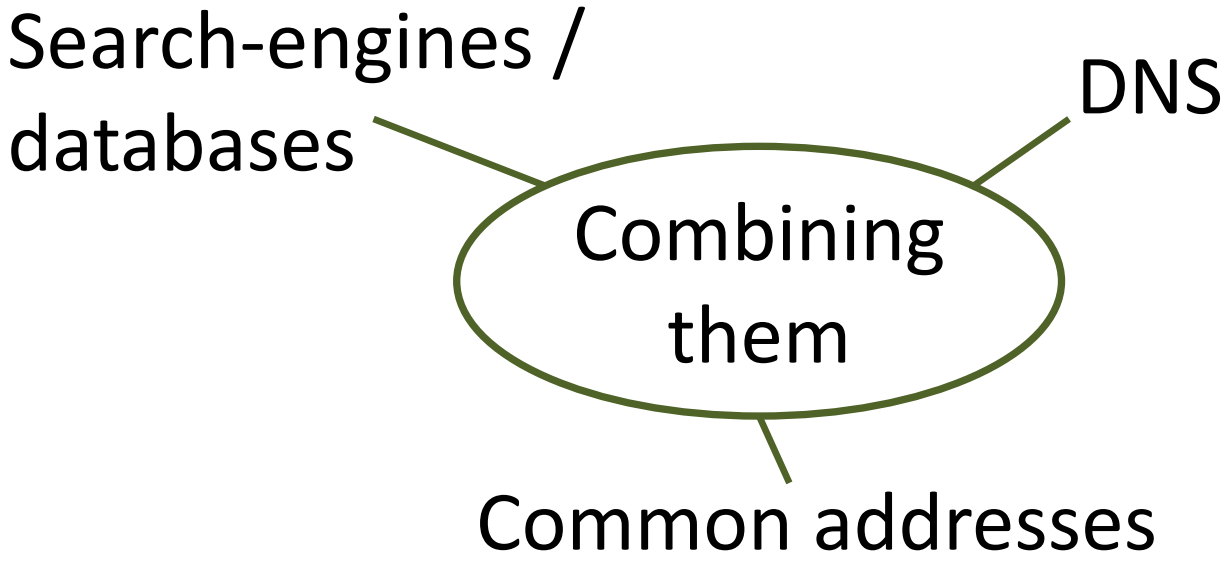
me in 2005

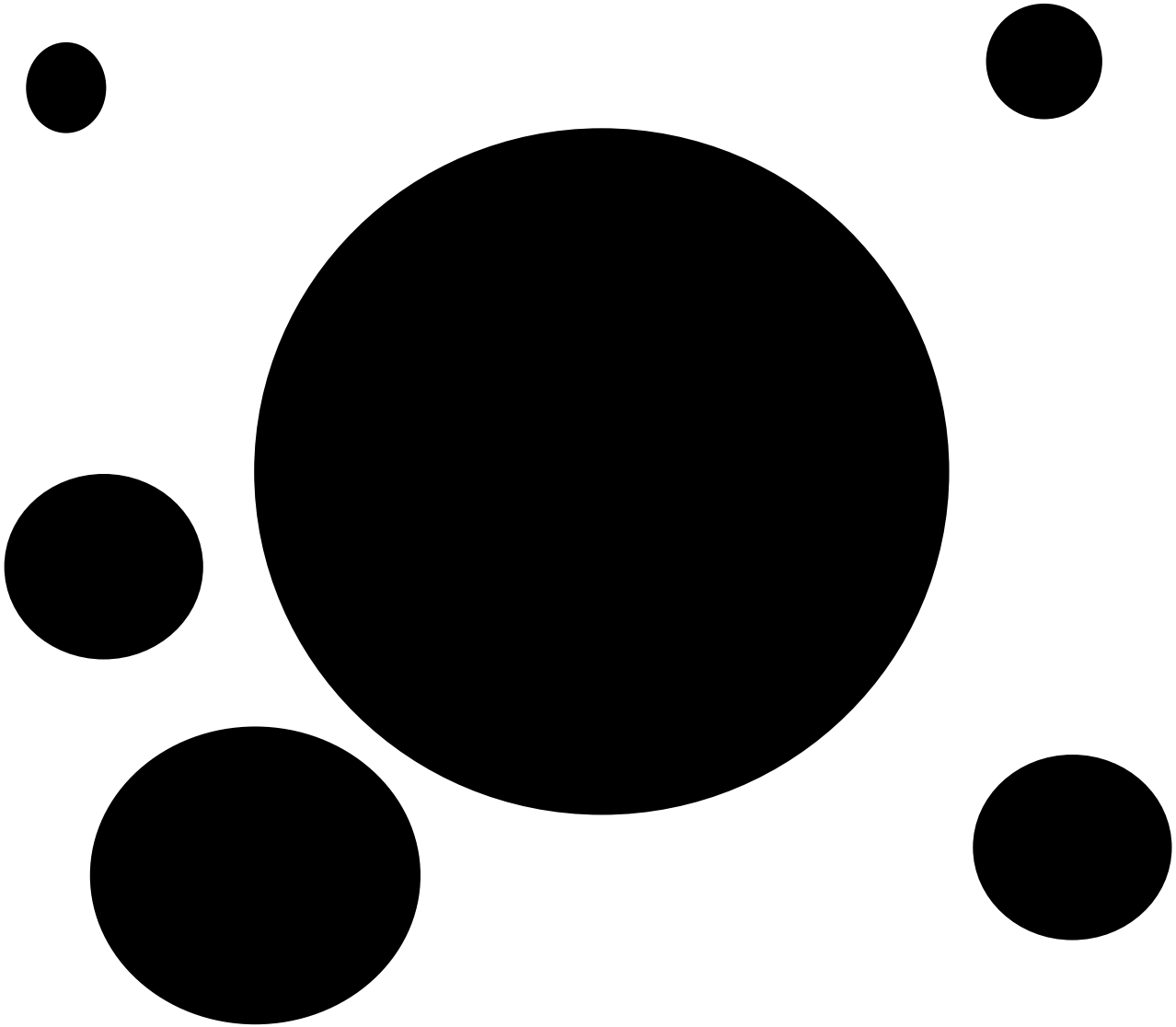
(and lots of other people
incl. RFC documents)

How to identify remote systems?

~~Broadcasts~~

~~Scan the whole range~~





Search Engines

Dumped various IPv6 directories

↓

17.000 possible domains & subdomains identified

DNS Results

17.000 domains
bruteforcing 3217 hostnames

↓

23.334 DNS entries found

↓

15.607 unique IPv6 addresses found

DNS Results

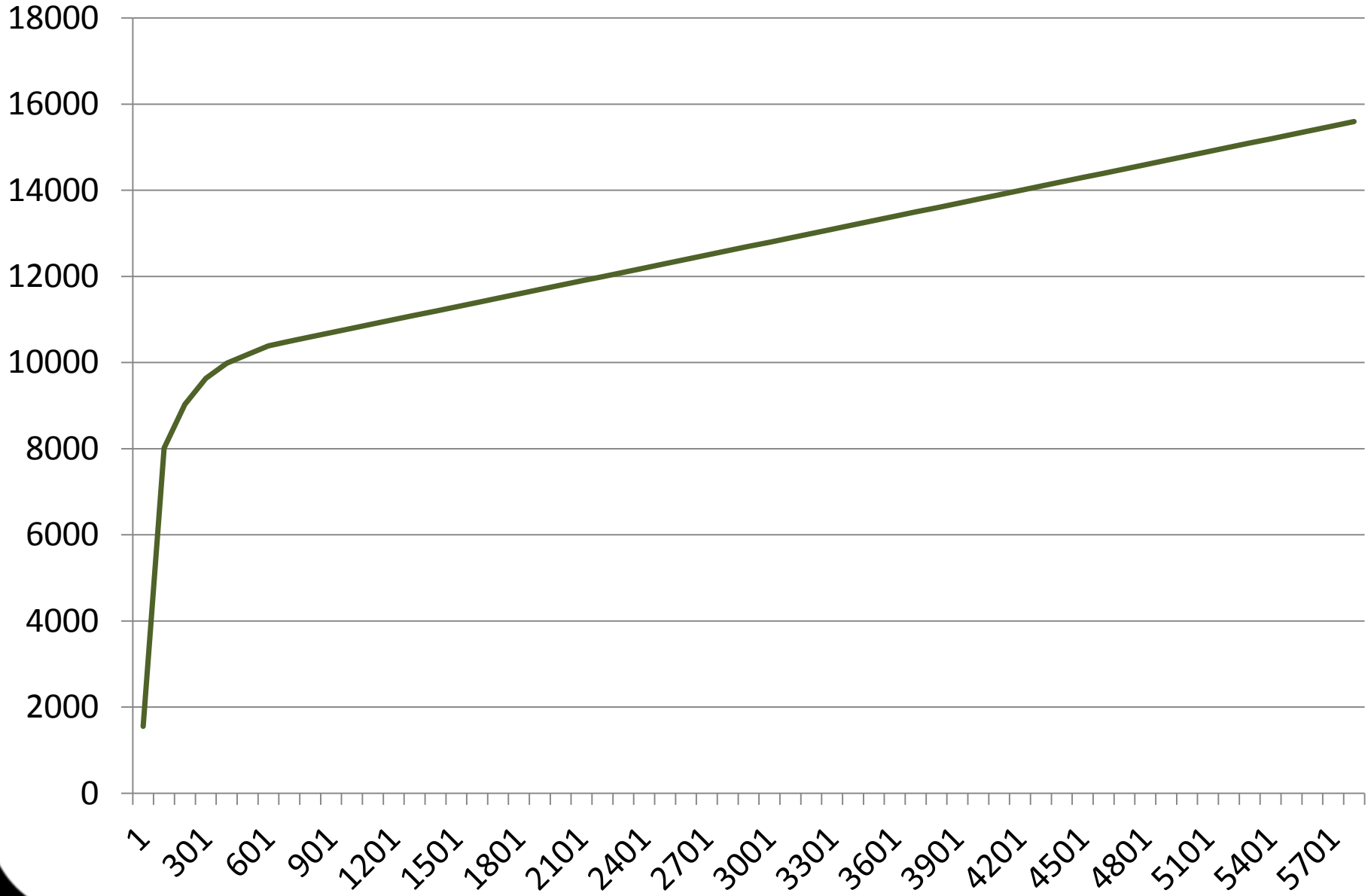
15.607 unique IPv6 addresses found

↓

7.305 networks

5.811 unique host addresses

IPv6 Host Addresses



Host address analysis

Autoconfiguration

- MAC address — ~24 bit key space per vendorID
- Privacy option — bad luck
- Fixed random — bad luck

DHCP

- Sequential
- Got one, got all
- Usually easy to find

by hand

- Pattern — got one, got all
- Random — bad luck

by hand

::1, ::2, ::3, …

::service_port

::1:service_port, ::2:service_port, …

::service_port:1, ::service_port:2, …

The IPv4 address

Funny stuff (::b00b:babe, etc.)

etc.

DHCP

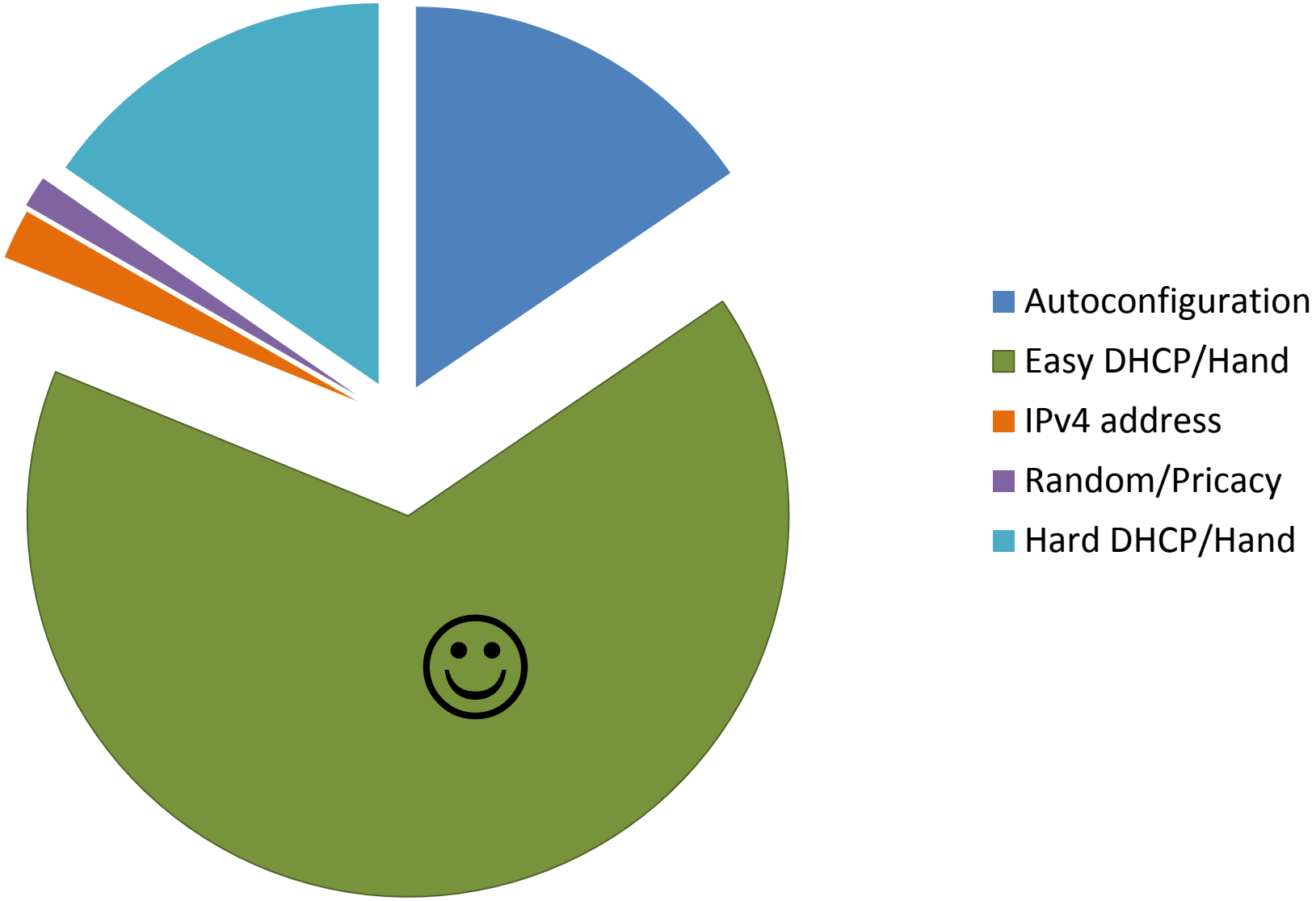
::1000-2000

::100-200

::1:0-1000

::1:1000-2000

IPv6 Host Address Distribution



Alive Scanning

7.305 networks
bruteforcing 3000 host addresses

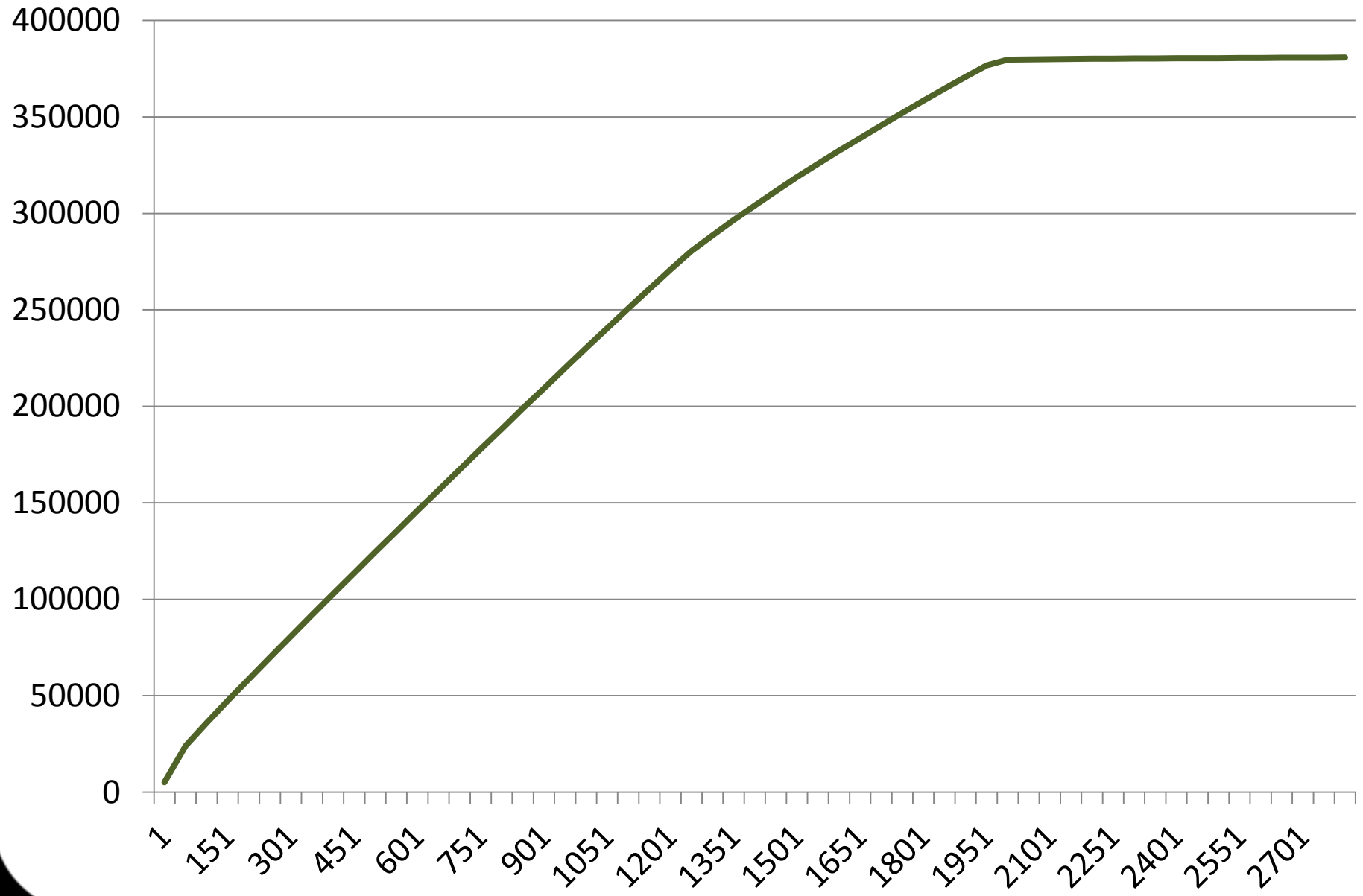
↓

380.766 alive systems

↓

8.160 networks
2.779 unique host addresses

Alive Host Addresses



DNS Analysis

<some slides omitted due boringness>

Conclusion

DNS bruteforcing: 90% of systems in DNS with 1900 words

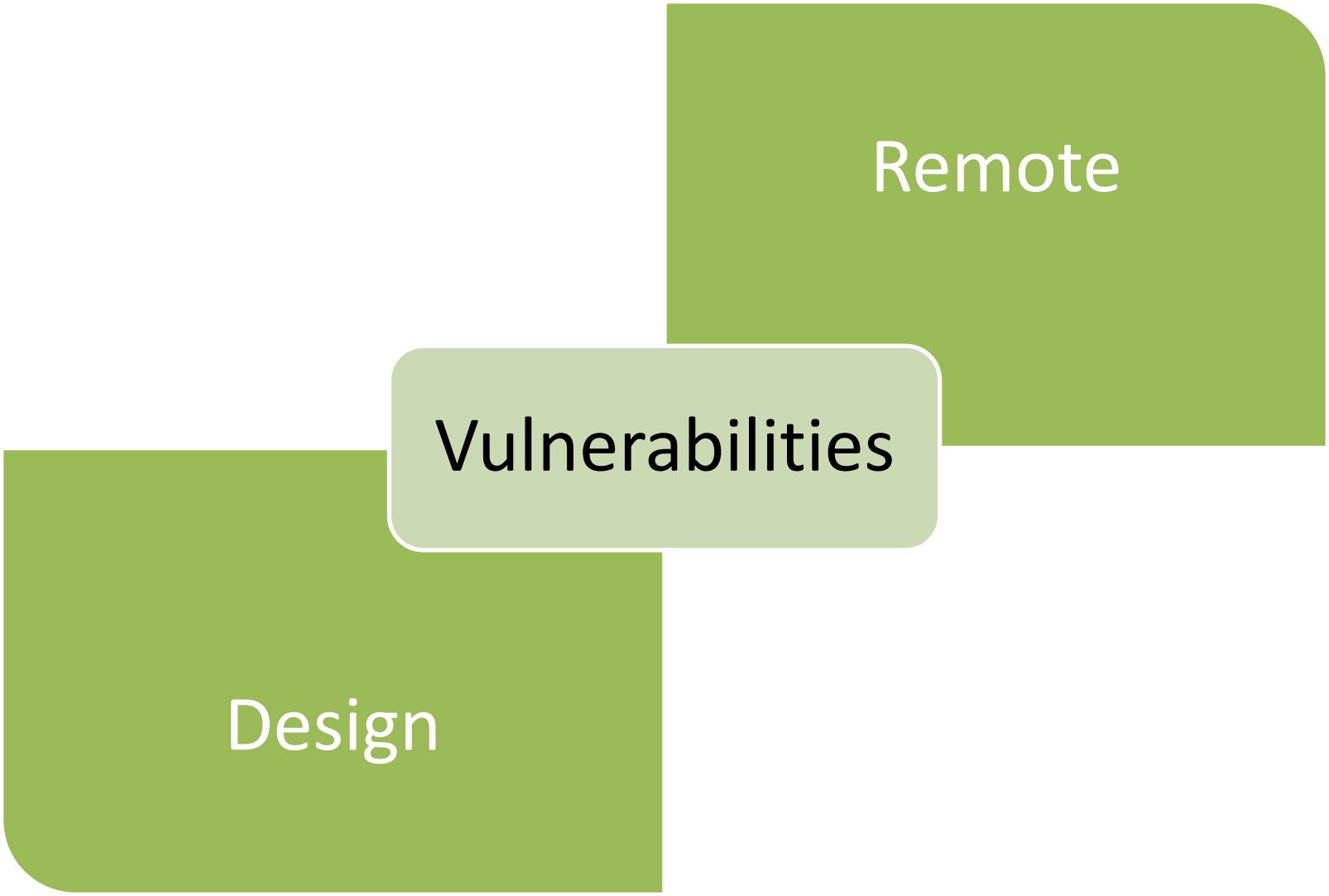
Conclusion

Alive bruteforcing: 66% of systems with 2000 addresses

scanned in 1-20 seconds

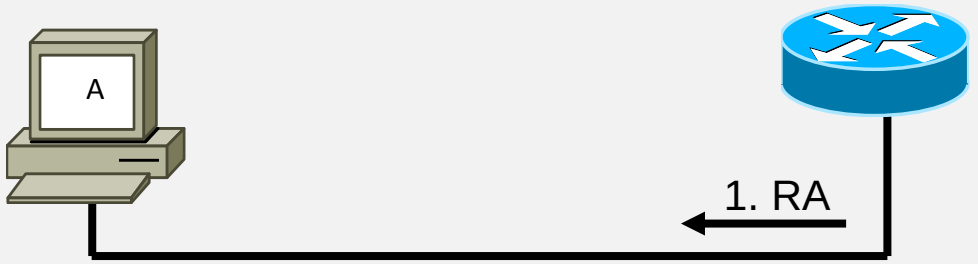
Final Conclusion

Combined (and use of brain)
~90-95% of **servers** are found


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**

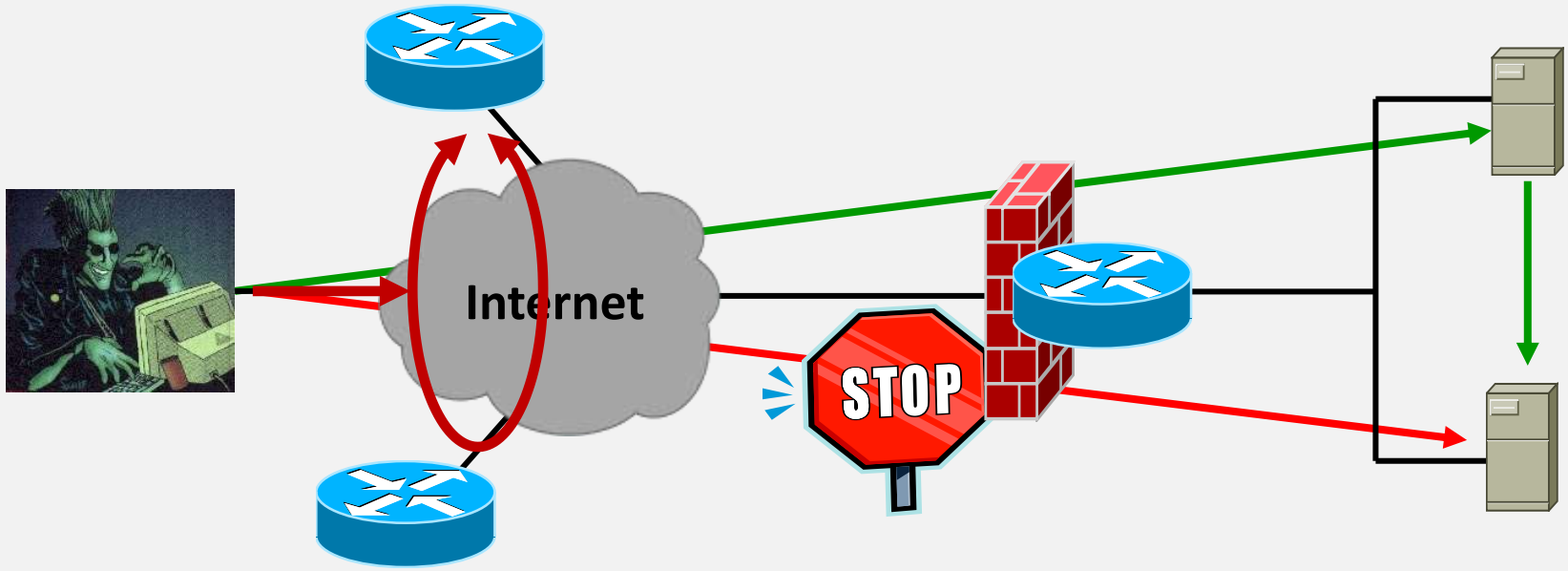
IPv6 host address: ::**02**0c:29**ff:fe**69:a666

Identify a host wherever it travels

Source: common knowledge

Tool: not needed

Source Routing



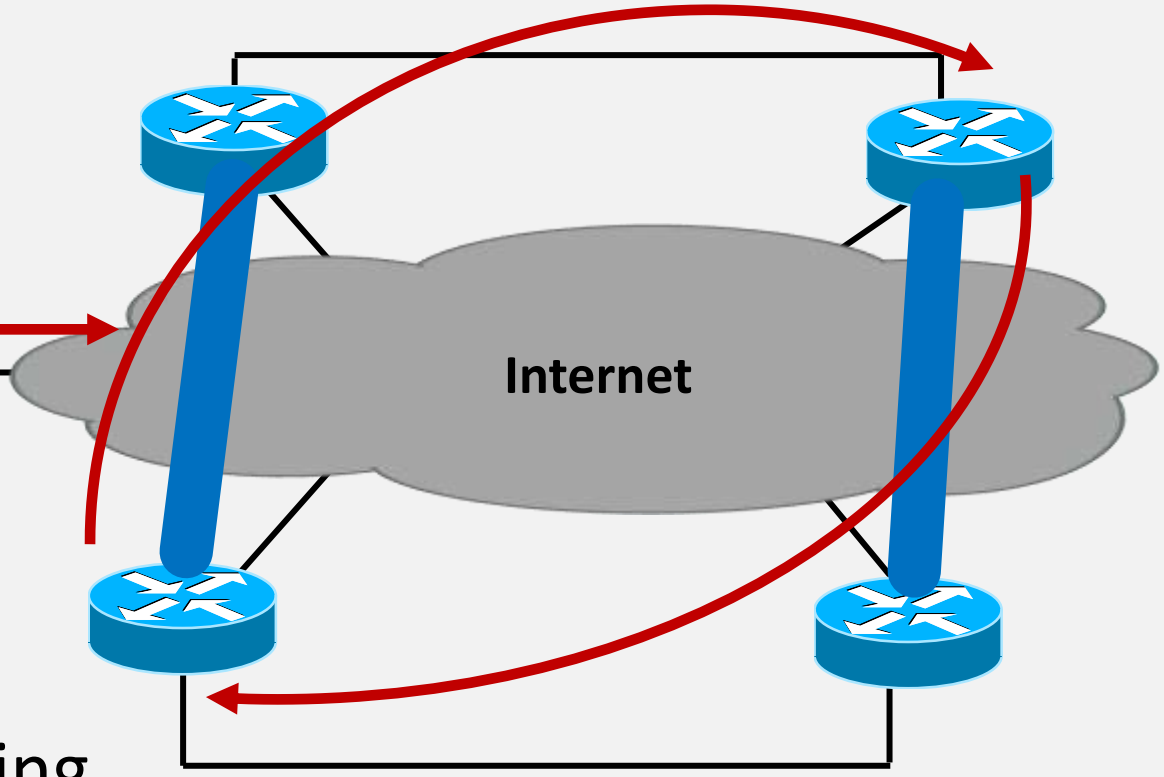
Spoofing, DOS

Now deprecated by RFC

Source: Philippe Bondi

Tool: alive6

Routing Loop Tunnel DOS



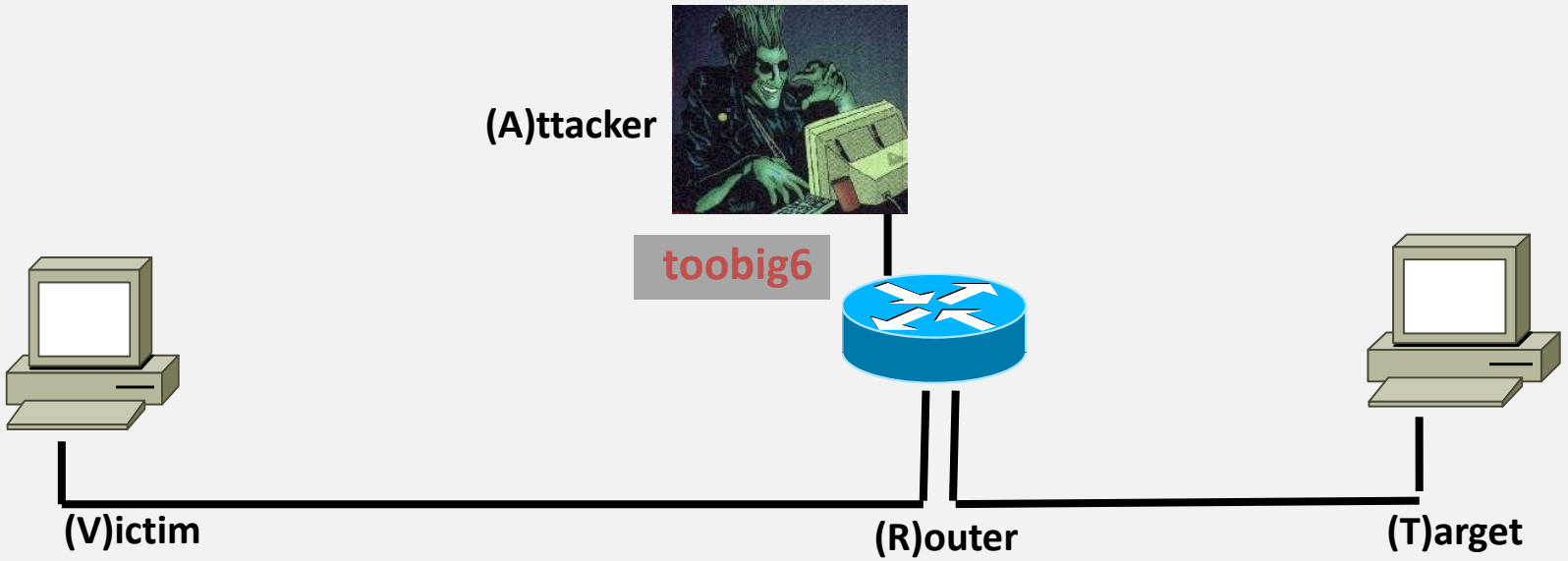
Multiple encapsulation headers specifying tunnel endpoints => DOS

Source: Gabi Nakibly

Tool: unknown

<more tunneling issues omitted>

Reduce MTU



Reduces MTU to 1280, limited impact

Same as redirect attack, but remote

Source: Marc Heuse

Tool: toobig6


COCAINE.
SO MUCH COCAINE.

Vendor Responses & Failures

The complexity problem™

So many

- extension headers
- options in extension headers
- possibilities of orders of headers and options
- new additions come often

The vendor solution:

Different support of options

Different maturity

Changes with every update

↓

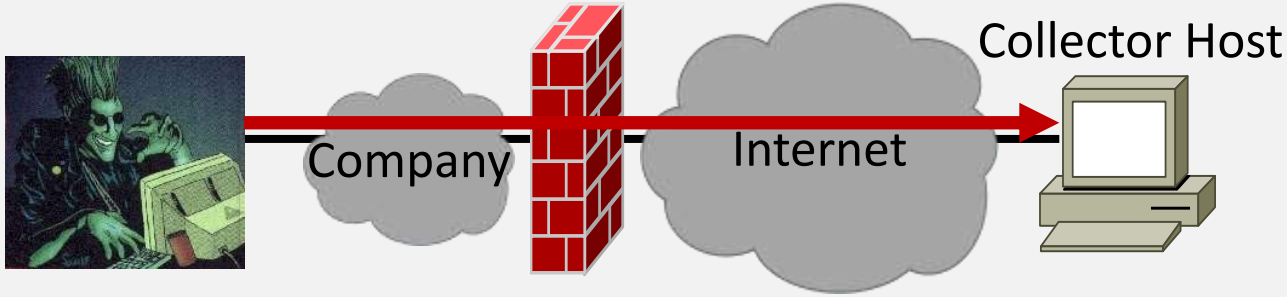
“Product supports IPv6” means nothing

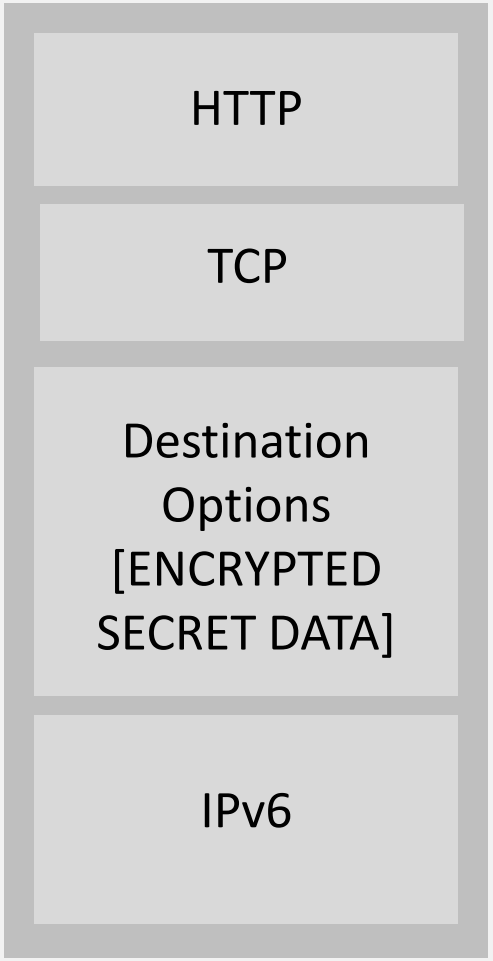
Firewalls

IPv4: Whitelist / Deny anything unknown

IPv6: Blacklist / Drop anything known evil

Covert Channels





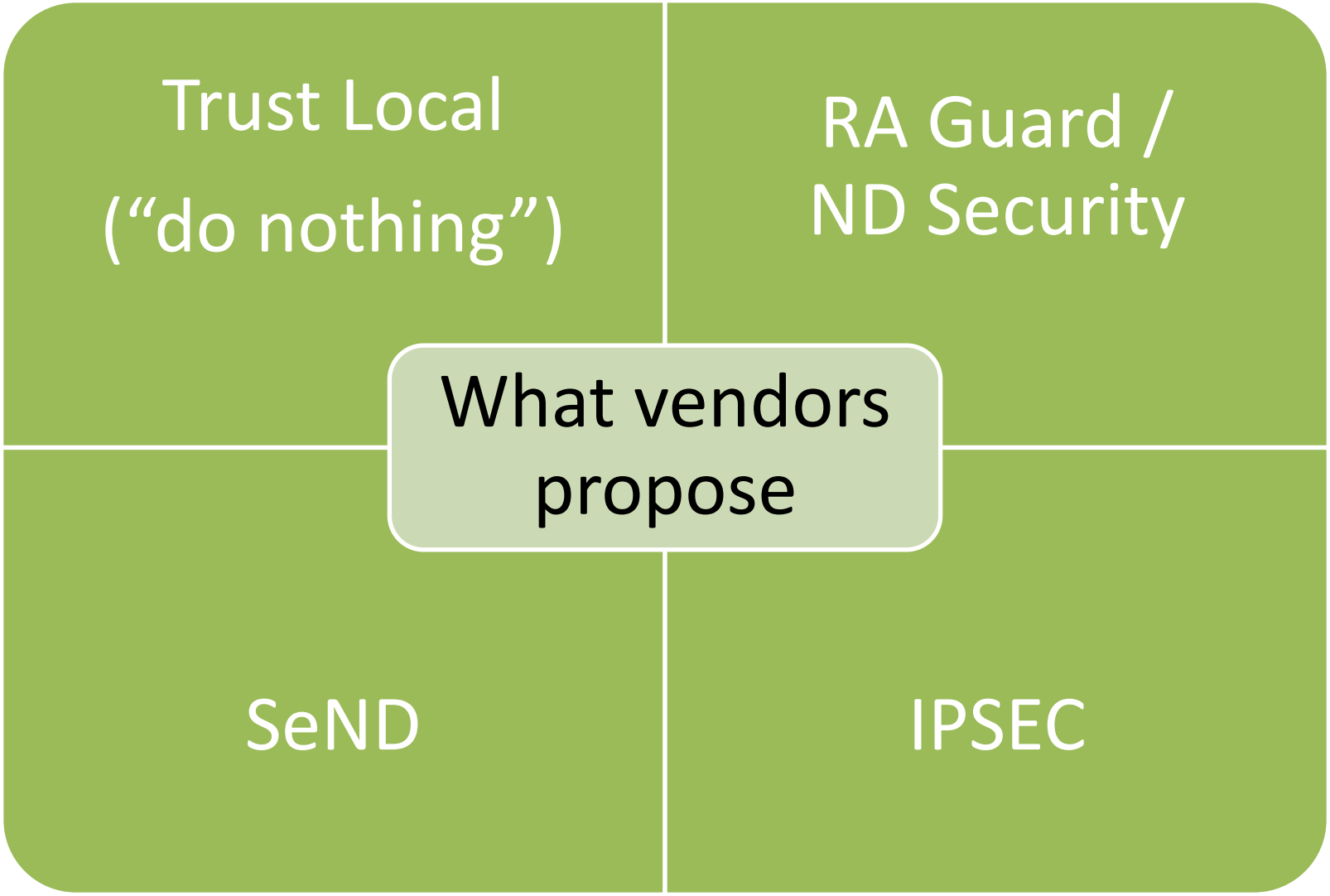
Every field can be used

(IPv6 header fields, Fragment ID, …)

1.4kb per packet (>90%)

Source: Marc Heuse

Tool: covert_send6


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

“while there are no explicit RFC violations in our implementation, we do agree that there is room for improvement

Juniper is currently working through the IETF to come up with a standard method of avoiding

[and won’t move a finger until then, see you again in two years]”

Juniper 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

Public WLANs?

Untrusted/uncontrolled environments?

Microsoft has fixed similar bugs before

on IPv4

Options: accept risk or disable IPv6

This builds public confidence in IPv6, good work!

RA Guard / ND Security

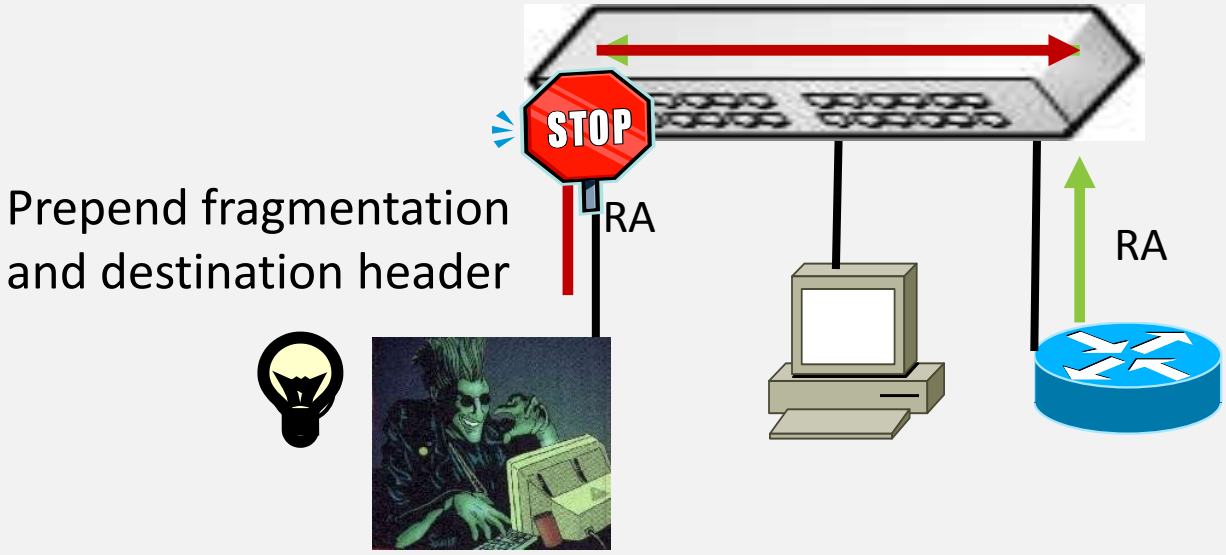
What vendors propose

My opinion of RA guard

(and NDP security)


RA Guard

RA Guard / ND Security Bypass



RA

Destination Options (large & empty)

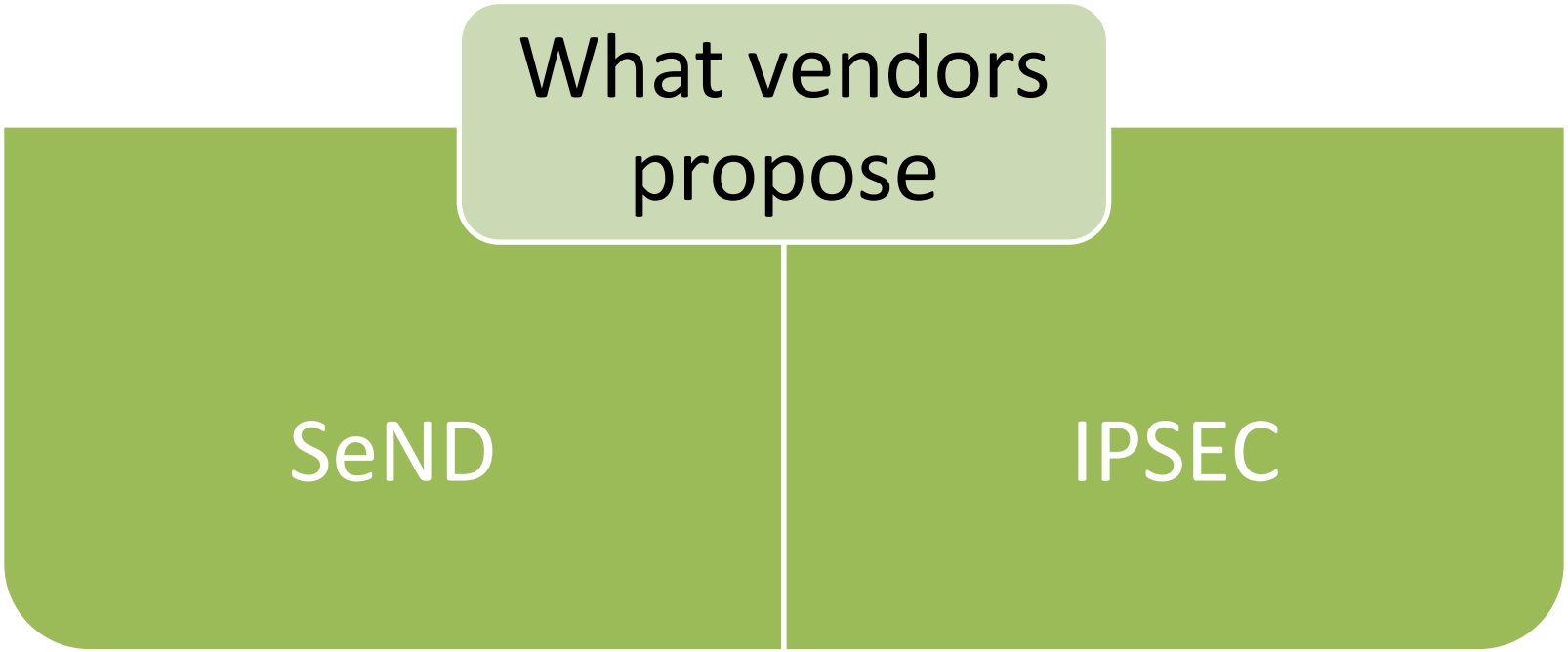
Fragmentation

IPv6

+ use overlapping fragments, and it's game over

Source: Marc Heuse

Tool: fake_router6


What vendors propose
SeND
IPSEC

Sorry, but:

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

SeND Attack

<I am not publishing this yet, sorry>

Source: Marc Heuse

Tool: ******6

IPSEC Attack

<I am not publishing this yet, sorry>

Source: Marc Heuse

Tool: ******6

The Problem:
IPv4 thinking applied to IPv6

IPv6 requires a new thinking for

- Designing
- Implementing
- Configuring
- Hacking

Besides security, lots of problems …

- Tunnel/MTU problems
- Client DNS server config
- …

Recommendations

BEWARE!

Nobody really knows

(including me)

The Good Thing™:

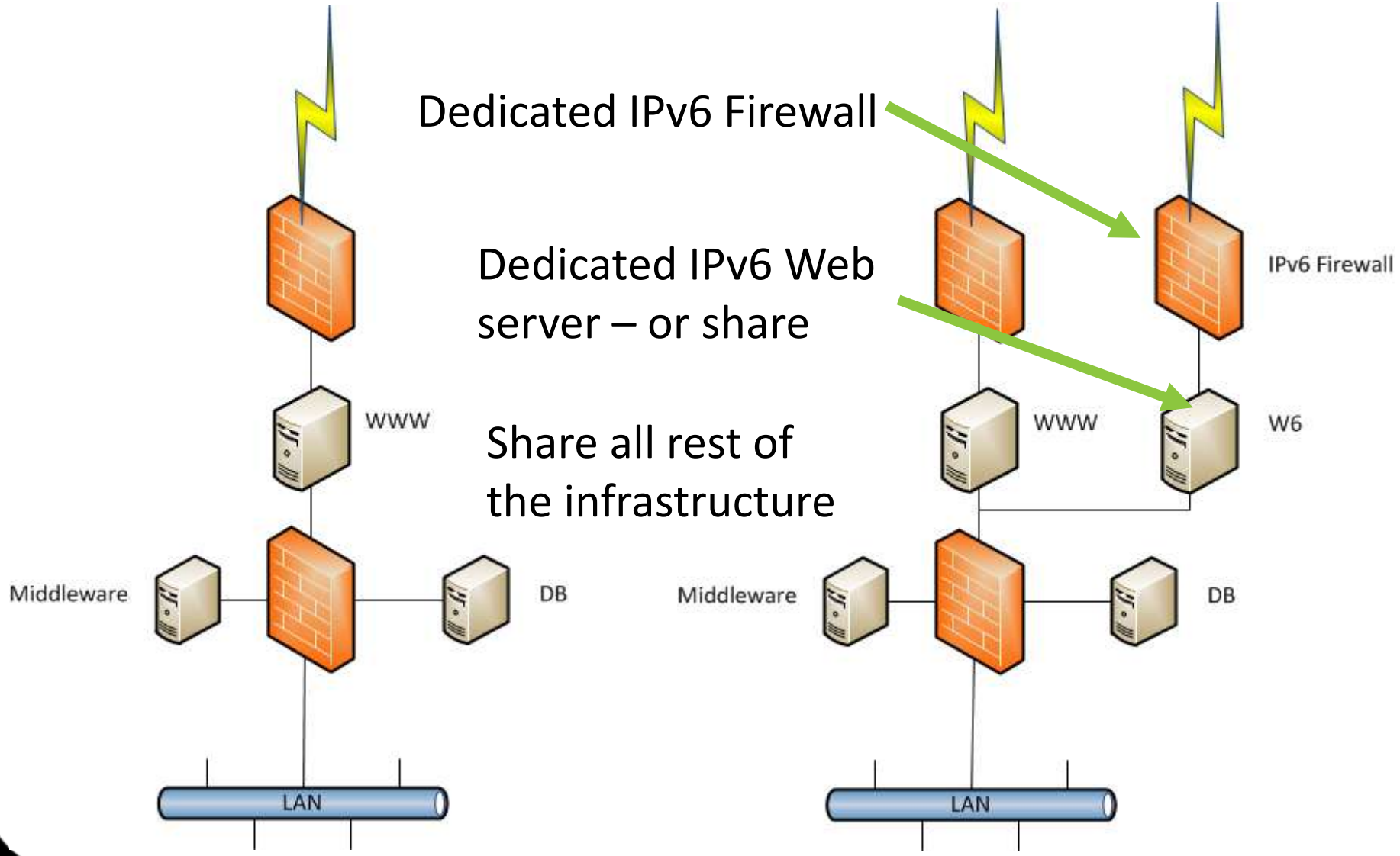
Critical issues are site-local only

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?



What to configure in the DMZ

- Strong incoming/outgoing ICMPv6 filtering on firewall
- Random host numbering
- Secure DNS, implement DNSSEC with NSEC3

Everywhere else …

- Disable IPv6 on all devices possible
  - Laptops, smartphones, embedded, …

If ever on the LAN …

- Private address space internally (random identifier)
- Don’t use privacy extension (discuss with data protection officer & Betriebsrat)
- Don’t use DHCPv6

If ever on the LAN …

- Forget RA guard and SeND
- Don’t use site/org multicast, disable MLD
- IPv6 hardening on client/server/router

IPv6 requires new thinking

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

IPv6 Pentesting Tools

IPv6 Pentesting Tools

- THC-IPv6 Attack Suite
- Portscanner: Nmap / Halfscan6 / strobe / amap
- Protocol Analyzer: Wireshark / COLD
- Packet Generators: Scapy6 / Multi-Generator (MGEN) / spak6 / isic6 / Hyenae / SendIP / Packit
- Forwarder: socat / Relay6 / 6tunnel / NT6tunnel
- Covert Channel: VoodooNet
- Exploitation Framework: Metasploit

Contact

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