Using IPv6 for information covert exfiltration

MSc. Bernhards 'Lockout' Blumbergs, GXPN

A pentester and exploit researcher view on IPv6

(we could be talking different language....)

Do you  ?

(Since 06/06/2012 IPv6 is the new normal)

What is wrong here?

```
# ip6tables -nvL

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Control and monitor

- Network ingress and egress

- IPv6 as "Backdoor protocol"?

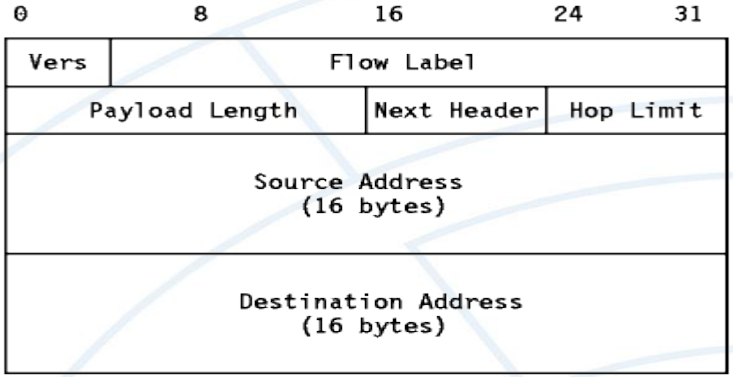
Evading detection [not really]

(for fun)

- Protocol ambiguities
- Device limitations (CPU, RAM, HDD, Sampling rate)
- Insertion, Evasion
- IPv6 product maturity and functionality

IPv6 Header(s)

- IPv6 Header



- IPv6 Extension headers

Known IPv6 security issues

- Extension headers
- Transition technologies
- ICMPv6
- Network reconnaissance

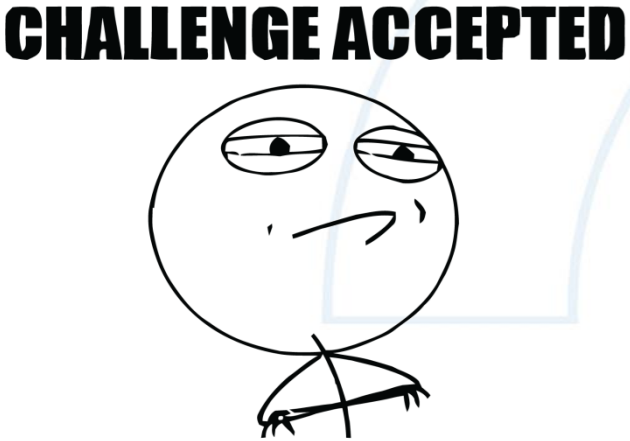
- Fuzz testing IPv6 implementations

Extension headers (RFC2460)

- Options header
- Hop-by-hop optins (Router alert attack)
- Routing headers (RH0 attack - deprecated)
- Fragmentation header (frag attacks)
- Destination options
- IPSec (ESP+AH), Mobility, Shim6
- Unknown options header

IPv6 Extension header chaining

- RFC2460: [...] it is recommended that those headers appear in the following order [...]



Long live IPv4!

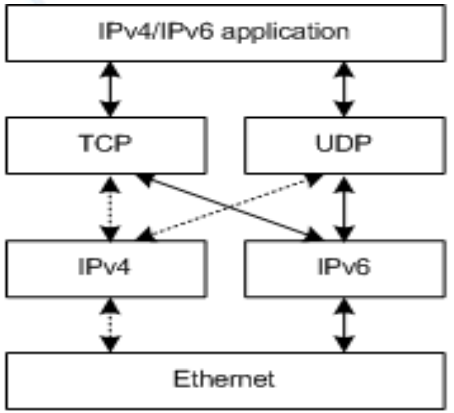
(when is it going to happily retire?)

Transition mehanisms

- RFC6180
- Dual stack
- Tunneling
- Protocol translation

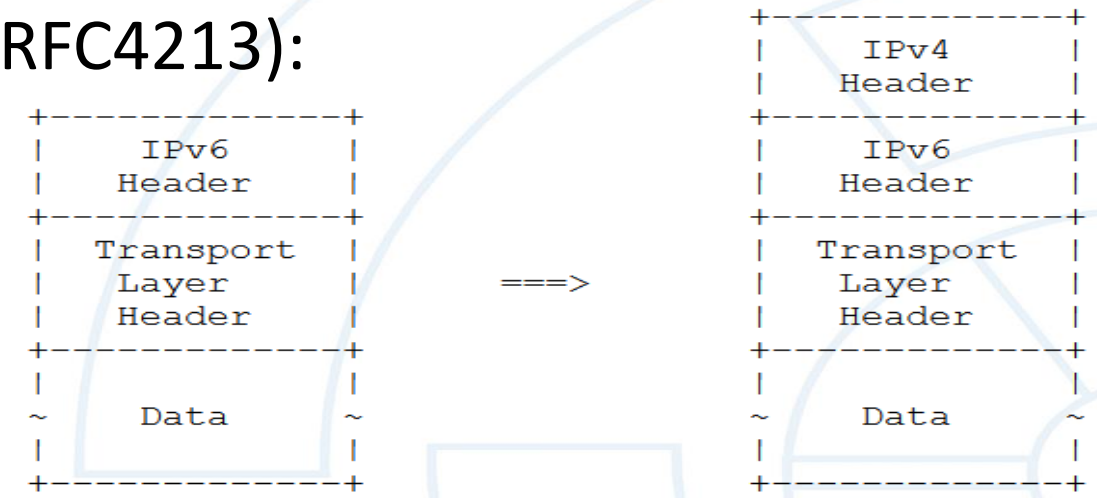
Dual stack

- IPv6 preferred over IPv4
- Attacks on both IP protocols
- Upper layer attacks still work



Tunneling

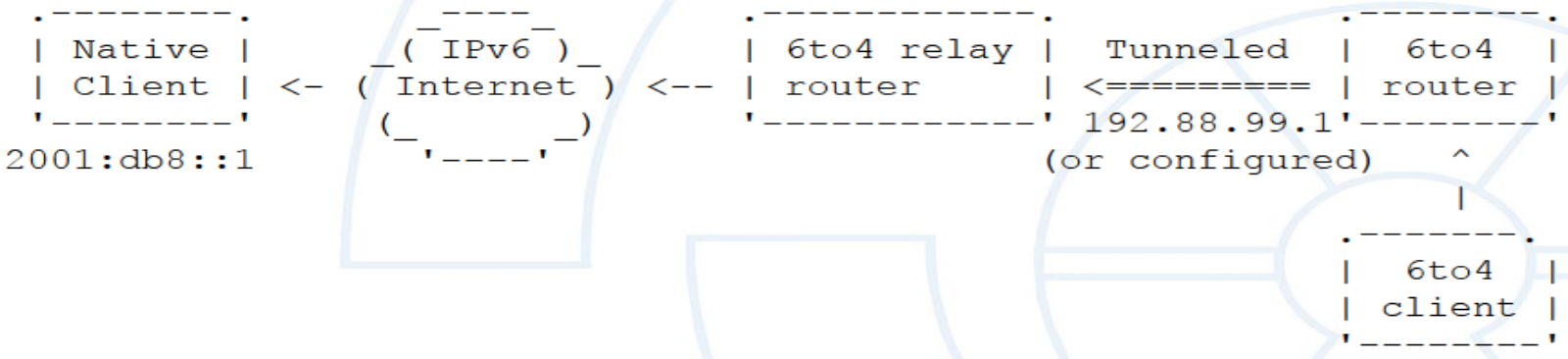
- Static and dynamic
- Such as: Teredo, ISATAP, 6in4, 6to4, 6over4, 6rd...
- 6in4 (RFC4213):



Encapsulating IPv6 in IPv4

6to4 (RFC2529, RFC3964)

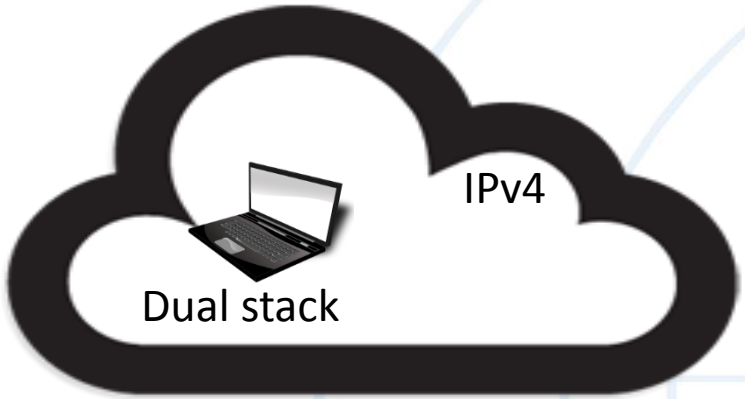
- Uses 6in4
- Protocol IP[9]=41
- 2002:V4ADDR:/48
- Anycast 192.88.99.1



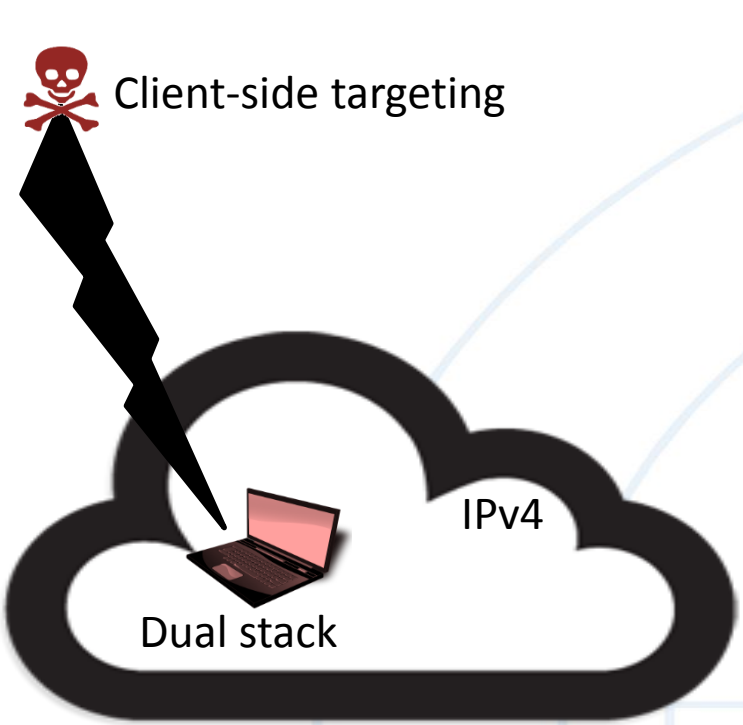
The scenario

(under development and testing)

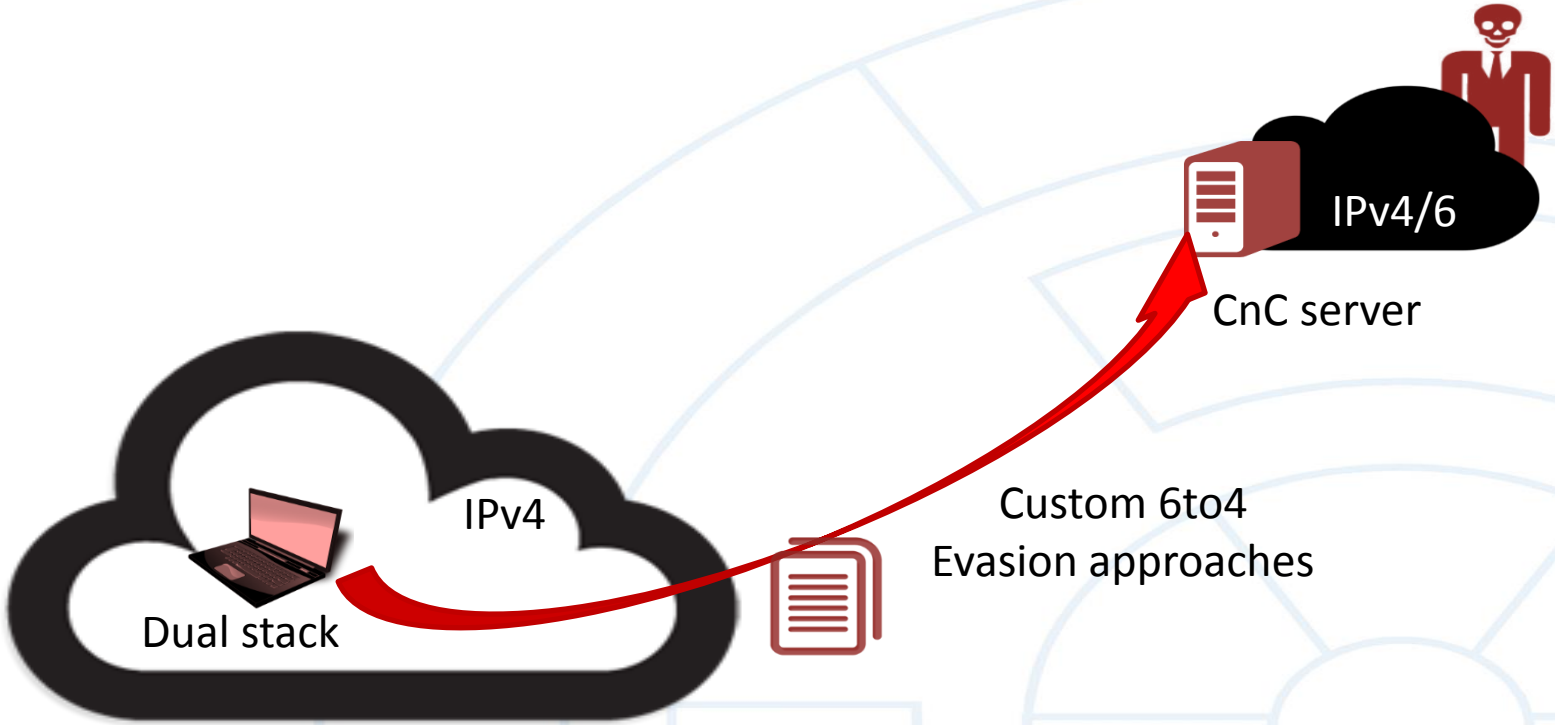
The layout



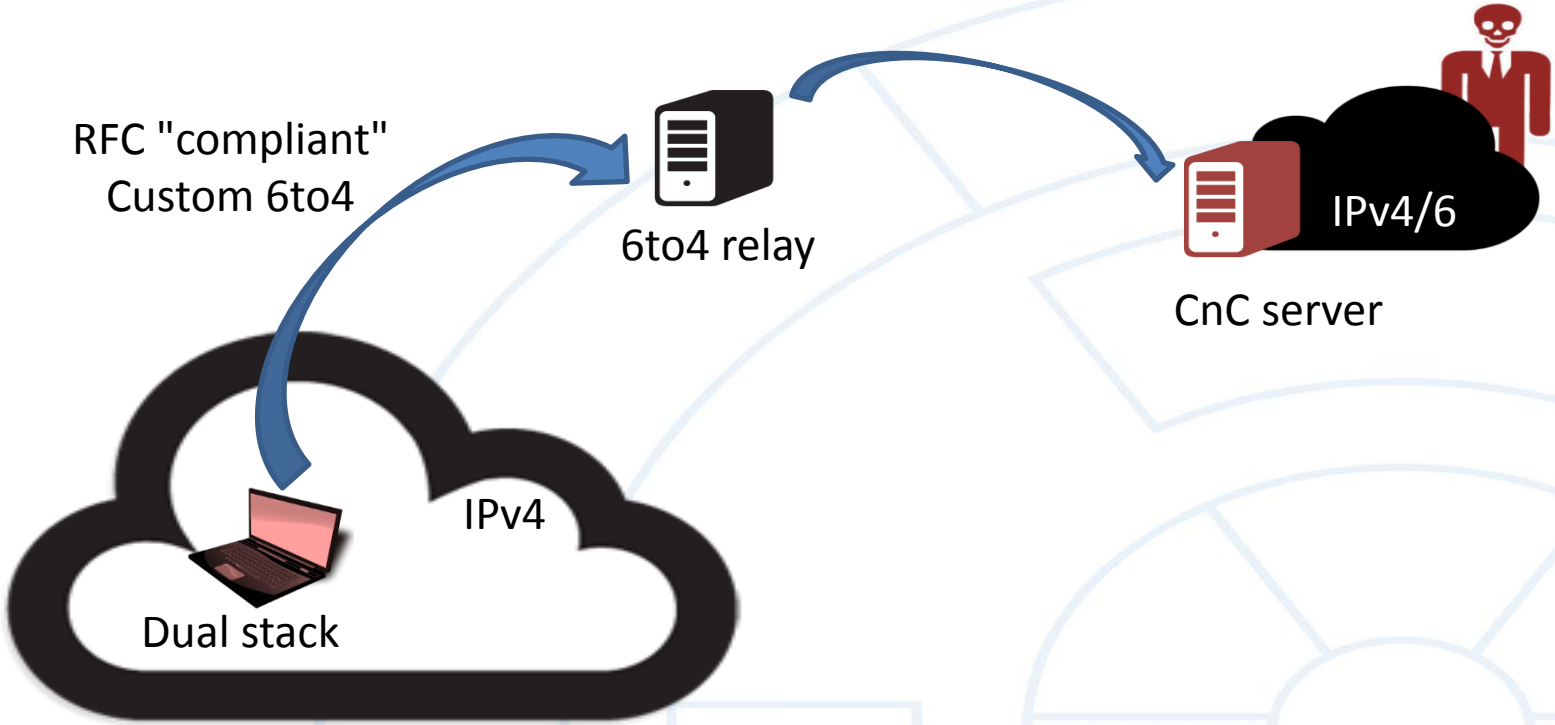
Initial foothold



Calling back home



Hitchhiking back home



All the things

- Know what you use
- Use wisely
- Control and monitor
- Be prepared to react
- …

To be continued...