ICMPv6 support for libpcap

Matthias Hannig, Moritz Wilhelmy, Daniel Lublin

November 6, 2017

RIPE NCC IPv6 Hackathon Copenhagen

Teaching somebody else's old dog new tricks

The Problem

```
tcpdump -i en0 "icmp6[icmptype] = icmp6-echo"
tcpdump:  IPv6 upper-layer protocol is not supported
by proto[x]
```

With the current version of libpcap it's not possible to match directly on ICMPv6 packet header attributes.

Enter BPF

- Berkeley Packet Filter is a bytecode register machine that runs inside the kernel.
- Used for performing computational operations on network packets (and nowadays other data on Linux).
- Linux and FreeBSD JIT-compile the bytecode to native assembly on a variety of platforms for additional speed.
- libpcap uses it internally as a compile target for its filter expression syntax.

Example bytecode: IPv6 packet?

```
(000) ldh      [12]
(001) jeq      #0x86dd          jt 2  jf 3
(002) ret      #TRUE
(003) ret      #0
```

- Load half-word (16 bit) at offset 12 (EtherType) into the accumulator
- Compare equality with magic value for IPv6 packet `0x86dd`
- If true, jump to line 2, else jump to line 3
- Return true if it matches, or false if it doesn't

What is libpcap?

- Packet capture: OS independent engine to tap into the network stack
- Fallback BPF bytecode interpreter in case the kernel rejects the BPF code
- BPF filter code generator

Adding ICMPv6

```
# tcpdump 'icmp6[icmptype] = icmp6-neighboradvert'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
19:21:23.046939 IP6 2001:470:ddf6:0:209a:219e:ffd4:5e74 > 2001:470:ddf6::1: ICMP6, neighbor
 ↪    advertisement, tgt is 2001:470:ddf6:0:209a:219e:ffd4:5e74 length 24
^C

# tcpdump 'icmp6[icmptype] = icmp6-echoreply || icmp6[icmptype] = icmp6-echo'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
13:50:43.424237 IP6 2001:470:ddf6:0:209a:219e:ffd4:5e74 > 2a00:1450:4013:c00::65: ICMP6,
 ↪    echo request, seq 1, length 64
13:50:43.457299 IP6 2a00:1450:4013:c00::65 > 2001:470:ddf6:0:209a:219e:ffd4:5e74: ICMP6,
 ↪    echo reply, seq 1, length 64
```

Future developments

There are several shortcomings in IPv6 processing inside libpcap, for instance there is no generic IPv6 header processing code.

This is partly because IPv6 allows chaining of extension headers, making processing in plain BPF complicated due to restrictions imposed by the kernel (no loops allowed to ensure that the BPF program terminates).

Thank you!

Questions?