Scamper remote control

Matthew Luckie
mjl@wand.net.nz

Overview of scamper

- Powerful open-source packet-prober
  - Precise: stores details (warts, warts2json)
  - Parallelized: event-driven simultaneous measurement
  - Portable: UNIX-like systems, MacOS, Windows
  - Flexible: standalone vs. coordination+control
  - Volunteer friendly: standalone, low resource requirements
  - Modular: extensible, but supports most popular active measurements (traceroute, ping, alias resolution, tbit)
  - Documented: 48 pages of man pages (16 for scamper itself)
- Users: CAIDA, Dyn, many other researchers.
- Contact: Matthew Luckie mjl@wand.net.nz
- http://www.caida.org/tools/measurement/scamper/

Interactive Control in Scamper

- Scamper has a “control socket” since 2004:
  - TCP socket listening on loopback interface
    - scamper –P <port>
  - Unix domain socket listening in file system
    - scamper –U <unix-socket-filename>
- Control socket:
  - Control macroscopic behavior of scamper, or
  - Schedule and receive measurement responses

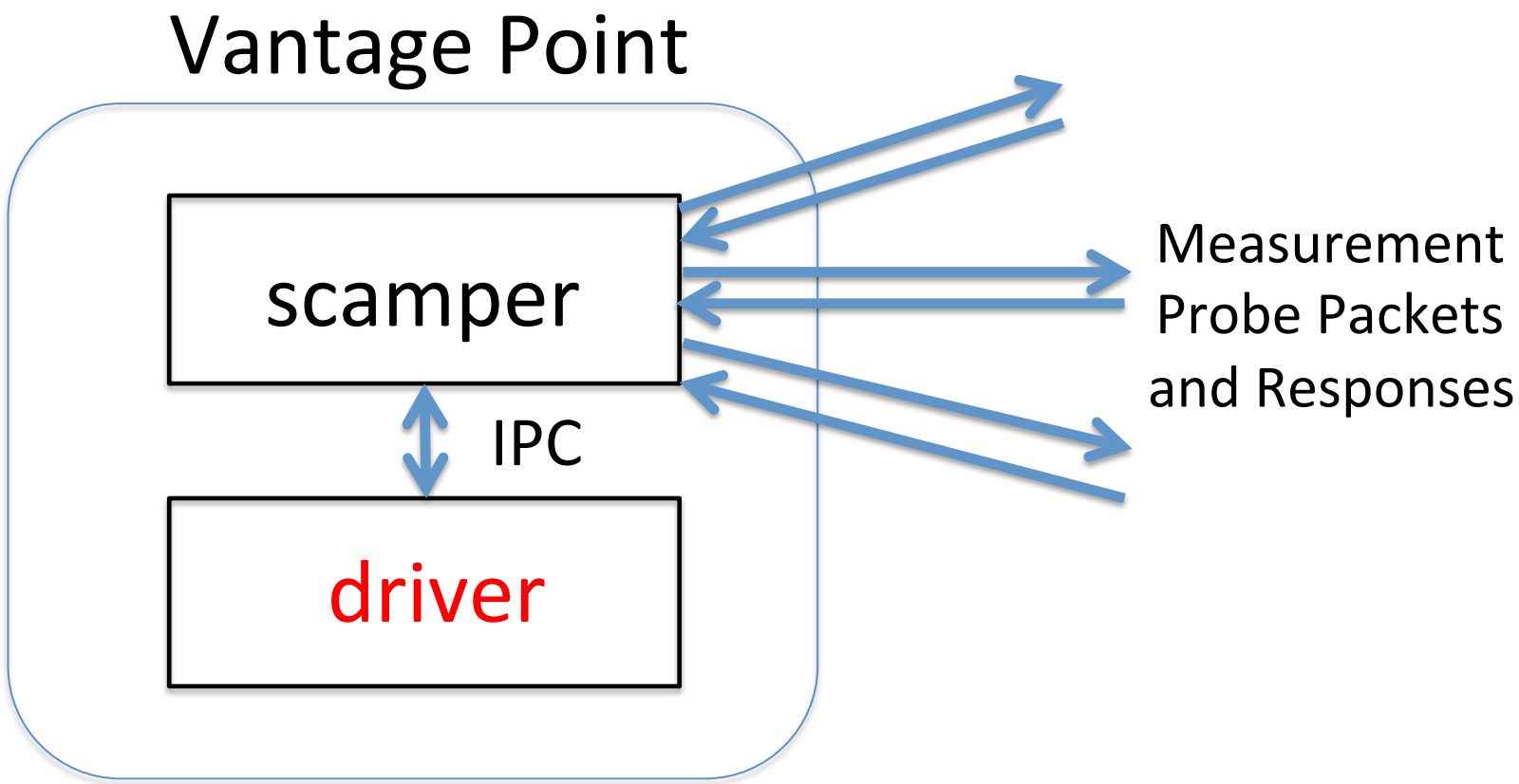
Interactive measurements in scamper

```
$ telnet 127.0.0.1 31337
attach
OK
MORE
DATA 48
A$@4``O```!D````!`````#$R-RXP+C`N,3HU-S8Y,P``
`
DATA 60
J$@4``@```"(````!`````O````%6NLE'`@`/36%T=&AE=W,MO6ER+3(`
`
ping 8.8.8.8
OK id-1
MORE
DATA 292
M$@4`!P```,GS_&4`*@````$````!5KK)3``)4OH!```$`%O!O`````2,/PO!
MP*@!Q`O!"`@("``$_I,#`"$'.`!4`````+>Z``"SOO2R`````$`````5KK)
M3``)4Y;^DP,`(O<X`%O`````F>L``;5Z__X`````O````!6NLE-``EGLOZ3
M`P`A!S@`5`````"VO@`"N%@$3`````!`````%:ZR4X`"6TM_I,#`"$'.`!4
=`````*2?``.X>W=I`````$`````5KK)3P`)@2$`
`
```

Interactive measurements in scamper

```
$ echo "ping -c 1 8.8.8.8" |
  sc_attach -i - -o - -p 31337 |
  sc_warts2json
{"version":"0.4", "type":"ping", "method":"icmp-echo",
"src":"192.168.1.196", "dst":"8.8.8.8", "start":
{"sec":1455082543,"usec":735979}, "ping_sent":1,
"probe_size":84, "userid":0, "ttl":64, "wait":1,
"timeout":1, "responses":[{"from":"8.8.8.8", "seq":0,
"reply_size":84, "reply_ttl":56, "reply_proto":"icmp",
"tx":{"sec":1455082543, "usec":736028}, "rx":{"sec":
1455082543, "usec":777779}, "rtt":41.751,
"probe_ipid":26599, "reply_ipid":40658, "icmp_type":0,
"icmp_code":0}],"statistics":{"replies":1, "loss":0,
"min":41.751, "max":41.751, "avg":41.751, "stddev":
0.000}}
```

scamper measurement drivers



Interactive measurements in scamper

- We used the control socket for intelligent measurement control in research, e.g.:
- sc_filterpolicy (NDSS2016):
  - for a list of dual-stack systems, check each IP address for congruent filtering policy
- sc_tbitblind (IMC2015):
  - for a list of webservers and routers, test resilience to blind TCP attacks
- sc_trlinks (PAM2014):
  - traceroute a set of destinations, and infer if observed IP-links are point-to-point

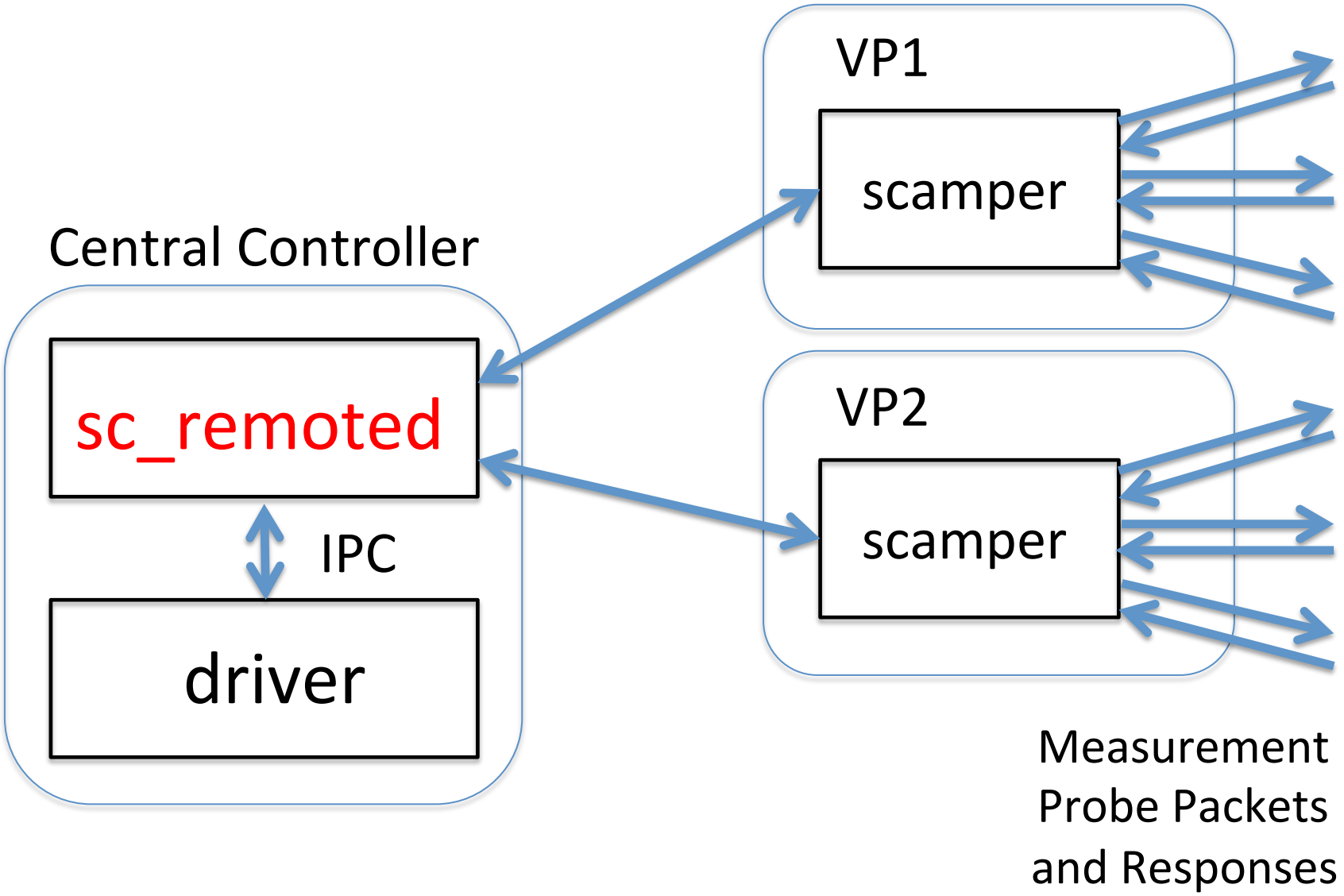
Why add remote control?

- Original scamper motivation was to build a stand-alone packet prober
  - i.e., avoid centralized controller issues
  - at the time, other infrastructures seemed to couple prober with control
  - never going to please everyone
- Prompted by Ethan and David's reboot of reverse traceroute, I built remote control functionality into scamper

Why add remote control?

- Researchers and operators may use low-resource nodes for complex measurements
  - scamper drivers might need more memory to keep state than VP has available

Using scamper remote control



Using scamper remote control

- sc_remoted exposes remote scamper instances as Unix domain sockets
  - One socket per remote VP
- Supports TLS
  - CA certificate built into scamper for validation
- VP naming
  - Scamper instance can supply monitor name to allow identification of remote nodes

Remote measurements in scamper

```
$ echo "ping -c 1 8.8.8.8" |
  sc_attach -i - -o - -R
      OWXXXXXXXXXXX-98.204.X.X\:39742 |
  sc_warts2json
{"version":"0.4", "type":"ping", "method":"icmp-echo",
"src":"98.204.X.X", "dst":"8.8.8.8", "start":{"sec":
1455140484,"usec":827228}, "ping_sent":1,
"probe_size":84, "userid":0, "ttl":64, "wait":1,
"timeout":1, "responses":[{"from":"8.8.8.8", "seq":0,
"reply_size":84, "reply_ttl":44, "reply_proto":"icmp",
"tx":{"sec":1455140484, "usec":827433}, "rx":{"sec":
1455140484, "usec":846943}, "rtt":19.510,
"probe_ipid":21510, "reply_ipid":0, "icmp_type":0,
"icmp_code":0}],"statistics":{"replies":1, "loss":0,
"min":19.510, "max":19.510, "avg":19.510, "stddev":
0.000}}
```

Experience so far

- Reverse traceroute reboot:
  - Will leave comments on their experience with scamper's remote control to Ethan and Dave
- Border mapping of networks:
  - Incorporated Project BISmark nodes into set of VPs to infer interdomain router involving the network hosting the VP
  - 3.5MB memory, 1-3% CPU on BISmark (64-128MB memory, 400Mhz MIPS CPU)
  - 150MB memory, 0% CPU on controller per driver