Scamper update

Matthew Luckie
University of Waikato
mjl@wand.net.nz
Recent work on scamper

- Enhanced control socket
- Numerous enhancements to regular traceroute
- Load-balancer traceroute
- IP Alias resolution techniques
- Firewall support (limited)
- Sting

- http://www.wand.net.nz/scamper/
Traceroute probe method and forward IP path inference

Matthew Luckie
Young Hyun
Brad Huffaker
Traceroute methods surveyed

- **UDP**
  - probe id: dport (unused); ephemeral sport;
- **UDP-Paris**
  - probe id: UDP checksum field; ephemeral sport; unused dport;
- **ICMP**
  - probe id: icmp sequence field;
- **ICMP-Paris**
  - probe id: icmp sequence field;
- **TCP (port 80)**
  - probe id: IP ID; dport 80, ephemeral sport
- **UDP-Paris DNS**
  - probe id: UDP checksum field; 5-tuple constant; sport 53; unused dport; valid DNS payload
Goals

• Determine which traceroute technique is the most effective
  – most reachable destinations
  – most complete paths
  – most IP links discovered
  – most AS links discovered
  – fewest gap limits (5 consecutive unresponsive hops)
  – fewest loops
  – fewest obviously spoofed responses

• … depending on the destination type
  – 261,530 routable IP addresses selected at random
  – top 500 web servers as ranked by alexa (422 IPs)
  – 2000 routers selected at random

• will focus mostly on random routable IP addresses
Random routable IP addresses

- 257,504 prefixes observed at routeviews for week of 19-25 March 2005 (median snapshot per day)
- 255,981 prefixes observed in at least 3 snapshots
  - one random address per prefix if prefix is more specific than /16
  - one per /16 otherwise
  - never select more than 1 address per /24, addresses in team cymru bogon list, do-not-probe (1.14 /8s)
- 261,530 addresses selected
- use unique list per vantage point
Methodology

• conduct six traceroutes for each destination in random order
  – UDP
  – UDP-Paris
  – UDP-Paris DNS
  – ICMP
  – ICMP-Paris
  – TCP

• 5 second cool-down between methods finishing

• conduct traceroutes at 100pps from *.ark.caida.org
  – 11 vantage points
  – 2 attempts per hop
  – 5 hop gaplimit
  – halt on first loop
# 261,530 routable IP addresses: cbg-uk

<table>
<thead>
<tr>
<th>Protocol</th>
<th>reached</th>
<th>icmp unreachable</th>
<th>loop</th>
<th>gaplimit</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp</td>
<td>5.9%</td>
<td>10.8%</td>
<td>10.0%</td>
<td>73.3%</td>
</tr>
<tr>
<td>udp-paris</td>
<td>6.1%</td>
<td>11.0%</td>
<td>7.9%</td>
<td>75.1%</td>
</tr>
<tr>
<td>udp-paris dns</td>
<td>6.0%</td>
<td>11.1%</td>
<td>7.9%</td>
<td>75.0%</td>
</tr>
<tr>
<td>icmp</td>
<td>9.8%</td>
<td>12.2%</td>
<td>9.2%</td>
<td>68.8%</td>
</tr>
<tr>
<td>icmp-paris</td>
<td>9.9%</td>
<td>12.4%</td>
<td>8.0%</td>
<td>69.7%</td>
</tr>
<tr>
<td>tcp (p 80)</td>
<td>9.1%</td>
<td>11.4%</td>
<td>7.8%</td>
<td>71.8%</td>
</tr>
</tbody>
</table>
Comments

- ICMP-Paris reaches most destinations
  - also obtains most ICMP unreachables, which is better than having your probe silently discarded
- UDP reaches the least
  - But it and the ICMP technique are known to produce invalid IP paths more frequently than their Paris counterpart
- UDP-Paris DNS performs slightly worse than UDP-Paris
Comments

• Reachability results very similar across other ten vantage points
  – despite different IP lists

• Some variation in ICMP-Unreach, Loops, Gaplimit
  – vantage point a factor
UDP-paris: 15927

TCP 23770

ICMP-paris 25965

915 6407 7795 12073

cbg-uk: Total reachable: 34353 (13.1%)
Reachable destinations

• Total reachable: 34353 (13.1%)
• ICMP-paris by itself yields the most:
  – 25965 (9.9%)
• ICMP-paris and TCP to get:
  – 33438 (12.8%)
• Not using UDP misses 2.7% of destinations reachable with three methods
Additional hops past blocking system to reachable destination
Complete Paths

• Defined as reaching destination and every hop returning an ICMP message
  – UDP-Paris: 10842
  – ICMP-Paris: 17703
  – TCP: 15244
  – Intersection: 7829
cbg-uk:
Total unique complete IP paths: 17738 / 7829
Total unique adjacent IP hops: 246484
Unique adjacent IP hops

- Total 246484
  - UDP-Paris 89.2%
  - ICMP-Paris 88.3%
  - TCP 87.4%
- ICMP-paris and UDP-paris to get 96.7%
Total AS links inferred: 18049

UDP-paris 15754
TCP 16652
ICMP-paris 16662

118 756
944
14788
335 595
Summary so far

- **ICMP-paris** reaches most destinations, infers most AS links
  - TCP not far behind
- **UDP-paris** infers most IP links
  - TCP least
- **TCP and ICMP IP paths** appear to be the most similar
  - vantage point has an effect, but trend is there
- **Firewalls** are most commonly two TTLs from the target.
Inferring Spoofed Destinations #1

• ICMP destination unreachable: port unreachable
  – RFC 792: Indicated port is not running an active process
  – Source address may vary, but supposed to be from destination
  – Used in alias resolution
Inferring Spoofed Destinations #1

Of 13335 port unreachablees for UDP-Paris, 44 were spoofed
Of 23770 destinations reached with TCP, 212 were spoofed.

162 SYN/ACK
43 RST/ACK
Packet counts

- ICMP-Paris: 6,183,075
- TCP: 6,266,375
- UDP-Paris: 6,362,914 (3% more than ICMP)
Router list

• 2000 IP addresses selected at random
• Previously observed in traceroute path:
  – to send time exceeded message
  – at least one additional ICMP time exceeded past the address, from a different IP
## 2000 random routers

<table>
<thead>
<tr>
<th></th>
<th>reached</th>
<th>icmp unreachable</th>
<th>loop</th>
<th>gaplimit</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp</td>
<td>69.2%</td>
<td>5.8%</td>
<td>1.7%</td>
<td>23.3%</td>
</tr>
<tr>
<td>udp-paris</td>
<td>70.0%</td>
<td>5.8%</td>
<td>0.8%</td>
<td>23.4%</td>
</tr>
<tr>
<td>udp-paris DNS</td>
<td>68.2%</td>
<td>6.0%</td>
<td>0.8%</td>
<td>25.1%</td>
</tr>
<tr>
<td>icmp</td>
<td>84.5%</td>
<td>5.9%</td>
<td>1.4%</td>
<td>8.2%</td>
</tr>
<tr>
<td>icmp-paris</td>
<td>85.1%</td>
<td>5.8%</td>
<td>0.8%</td>
<td>8.3%</td>
</tr>
<tr>
<td>tcp (p 80)</td>
<td>67.1%</td>
<td>6.7%</td>
<td>0.7%</td>
<td>25.6%</td>
</tr>
</tbody>
</table>
Webserver list

- Screen scrape of alexa.com top 500
- Resolved from san-us.ark.caida.org
- 422 IP addresses selected
  - 58 Google ccTLD instances => 4
  - Ebay ccTLD instances
  - Akamai
# 422 webservers

<table>
<thead>
<tr>
<th></th>
<th>reached</th>
<th>icmp unreachable</th>
<th>loop</th>
<th>gaplimit</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp</td>
<td>43.0%</td>
<td>4.3%</td>
<td>3.3%</td>
<td>49.4%</td>
</tr>
<tr>
<td>udp-paris</td>
<td>43.0%</td>
<td>3.5%</td>
<td>2.4%</td>
<td>51.1%</td>
</tr>
<tr>
<td>udp-paris DNS</td>
<td>46.3%</td>
<td>2.6%</td>
<td>2.4%</td>
<td>48.7%</td>
</tr>
<tr>
<td>icmp</td>
<td>76.4%</td>
<td>2.4%</td>
<td>2.6%</td>
<td>18.7%</td>
</tr>
<tr>
<td>icmp-paris</td>
<td>76.6%</td>
<td>1.9%</td>
<td>2.1%</td>
<td>19.4%</td>
</tr>
<tr>
<td>tcp (p 80)</td>
<td>95.5%</td>
<td>nil</td>
<td>2.1%</td>
<td>2.4%</td>
</tr>
</tbody>
</table>
Conclusion

- ICMP-Paris is superior in destinations reached, AS links
- UDP-Paris finds more intra-AS IP links
- Using multiple probe methods improves coverage
  - Also allows integrity of IP paths to be tested
- UDP-Paris DNS bit of a flop