On Bringing Private Traffic into Public SDN Testbeds

Vasileios Kotronis · Dominik Schatzmann · Bernhard Ager

Bringing user traffic to the testbed

- SDN testbeds deployed everywhere
- Stand-alone islands for safety and privacy
- Experiments go wrong
- User traffic is highly sensitive
- But sometimes, user traffic is necessary!

⇒ Covering the gap between model and reality

What is an SDN testbed?

- Experimenter’s Controller
- Experimenter’s Controller
- FlowVisor
- Virtual hosts
- Virtual topology

Risks when bringing traffic into a testbed

- Simply injecting traffic is not a good idea:

Privacy threats
- Learn about traffic patterns
- Direct packets to controller
- Direct packets to hosts under attacker’s control

Availability threats
- Drop packets
- Create forwarding loops
- Disable switch ports
- Inject packets in established communication

Attacker model

- OpenFlow 1.0
- Access to testbed hosts
- Possible control of multiple slices
- Access to external resources, e.g., hosts
- Assume: no software flaws, and OpenFlow switches are bug free

How does it work?

- Utilize Header Space Analysis [1]
- Tracking how flows propagate
- Uses a header space algebra: Set-algebra on network flows
- Quite expensive!


Privacy and Availability Layer: PAL

- Proxy intercepts OpenFlow messages, can reject messages
- Gatekeepers perform selective traffic injection
- Policy violation ⇒ short-circuit testbed

Building a marketplace

Three roles

- User specifies policies
- Experimenter defines requirements for test traffic, provides incentives
- Operator matches user traffic to experiments, enforces guarantees

Example policies

<table>
<thead>
<tr>
<th>Part of traffic</th>
<th>Guarantees</th>
<th>Experiment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>no-sniff, copy-traffic any</td>
<td>-</td>
</tr>
<tr>
<td>BitTorrent</td>
<td>none</td>
<td>transparent BT cache</td>
</tr>
<tr>
<td>E-Banking</td>
<td>direct-delivery</td>
<td>-</td>
</tr>
</tbody>
</table>

How to attract users

- Network services
  - IP address anonymization
  - Network usage statistics
  - On-demand network tunnels
  - Games and competitions
  - Money

Insights

- Worst case: HSA exponentially expensive
- OpenFlow quirks make things harder than necessary
  - Flow timeouts triggered by switch
  - Ambiguities introduced by OF specification further help attacker

⇒ Need to limit analysis effort and to pro-actively handle timeouts

Summary

- Marketplace enables users to voluntarily donate traffic
- Experimenters may have to provide incentives, though
- Demonstrator running, final product to be deployed in OFELIA
- Approach is general: Outsourcing routing, “SDN app-store”

HotSDN 2013