On Bringing Private Traffic into Public SDN Testbeds

Vasileios Kotronis
Dominik Schatzmann
Bernhard Ager

ETH Zürich
December 8, 2014
Motivation

- 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!
Motivation

- 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!

We want to bring user traffic to the testbed
What is an SDN testbed?

Network slice:
- Virtual hosts
- Virtual topology
- Flow/Header-space
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: The “bad” experimenter

- OpenFlow 1.0
- Access to testbed hosts
- Possible control of multiple slices
- Access to external resources, e.g., hosts
- Assume: no software flaws, no switch problems
Proxy intercepts and re-writes OpenFlow messages
- Gatekeepers perform selective traffic injection
- Policy violation $\Rightarrow$ short-circuit testbed
How does the PAL work?

- Header-space analysis (HSA)
  - Tracking how flows propagate through testbed
- Checking every single message
  - Flow-mods are policed
  - Payload stripping from packet-ins, restoring on packet-outs
- Flow removals need to be handled *before* they happen
- Bail-out: short-circuit the testbed

Originally published in Kazemian's presentation on “Real Time Network Policy Checking Using Header Space Analysis”, NSDI 2013
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</td>
<td>any</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>
Insights

- Incentives for users
  - Network services
    - IP address anonymization
    - Network usage statistics
    - On-demand network tunnels
  - Games and competitions
  - Money
- OpenFlow quirks make things harder than necessary
  - Flow timeout handling
  - Worst-case exponentially expensive analysis
  - Ambiguities introduced by specification further help attacker

⇒ Workarounds required
Summary

Kotronis et al. On Bringing Private Traffic into Public SDN Testbeds