Flow Reconnaissance via Timing Attacks on SDN Switches

Sheng Liu

Advisor: Mike Reiter
Software-Defined Networking

• Control plane and data plane
### Reactive

![Diagram showing network components: Host, Switch, Controller, Policy library, and Server]

<table>
<thead>
<tr>
<th>Match Fields</th>
<th>Action</th>
<th>Timeout</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.250.246.187 to 120.54.232.15</td>
<td>Forward to port 2</td>
<td>10 s</td>
<td>3</td>
</tr>
<tr>
<td>16.252.255.196 to 144.20.252.16</td>
<td>Forward to port 3</td>
<td>100 s</td>
<td>2</td>
</tr>
</tbody>
</table>
Timing Side-Channel Attack

• Matching rule in switch:
  Host → Switch → Server → Host

• No matching rule in switch:
  Host → Switch → Controller
  Switch → Server → Host

Delay is significantly increased!
What Information?

- Whether a network runs OpenFlow
- Size of switch forwarding table
- Fingerprint packet-forwarding logic
- Traffic analysis
  - Which website you visited
  - Who you were talking to
  - Whether IDS logged an event

- Delay of the probe packet
- Presence of the matching rule in switch
- Occurrence of the target flow
Motivation

• Reactive operation gives rise to a timing side-channel attack
• Adding delays increases overhead
• Practical challenges:
  - Rule expiration
  - Rule overlapping
  - Rule eviction
Project Goals

• Develop a formal method to measure the information leakage exploited by this attack

• Build an effective method to mitigate this attack by transforming rule structure
Quantifying Information Leakage

- Step 1: Use Markov model to estimate the switch-rule distribution

- Step 2: Computing information gain related to the target flow

\[ IG(\hat{X}|Q_f) = H(\hat{X}) - H(\hat{X}|Q_f) \]
Defense

• Transform rule structure
• Increase the uncertainty by merging or splitting rules
• Steer the system toward more coarse-grained rules
• The optimal balance between coarse-grained and fine-grained control
Evaluation

• Set up network environment using simulation tool and real-world data

• Evaluate the effectiveness of the attack with and without defense (network size, distribution of flow occurrence)
Next Steps

• Develop algorithm to transform rule structure
• Deal with scalability issue
• Implement the protocol on real-world testbed