The Problem: Clouds, Businesses and Users

- Modern businesses face an increasing need to store sensitive information on the cloud.
- Clouds are multi-tenant infrastructures that share resources for achieving economies of scale.
- Cloud enterprises employ shared management and statistical multiplexing on physical resources for efficient utilization.
- The necessity of shared infrastructure leads to the danger of information leakage across tenants.
- Covert and side channels are a concern as they can easily bypass network monitors and cause sensitive data exfiltration.

The Contributions of Our Work

- Construction of a high speed timing based covert channel.
- Derivation of a mathematical model along with analysis of an upper bound on the channel bitrate.
- Empirical evaluations of the achieved bitrate in an in-house environment as well as on EC2 and Azure clouds.
- Discussion of possible mitigation techniques for our channel.

Channel Construction and Analysis

- Our channel is of a unidirectional nature and operates across virtually isolated networks

Covert Channel Message Encoding

- Our channel is modeled as a FIFO queue shared by two packet processes on different networks
- To maintain queue stability, the maximum achievable information rate proposed by our channel is 67% of the bitrate.

Adaptive Decoding Scheme

- The Adaptive decoding algorithms leverage on the following methodologies to minimize channel error rates:
  - Threshold Evaluation: Calculating accurate cutoffs for 0’s & 1’s
  - Bit Marking: Synchronizing clocks at the sender and receiver

Channel Evaluation

- We use a UDP based scheme to evaluate the covert channel in various environments.
- For a realistic evaluation, cross traffic is generated as temporally spaced UDP and TCP flows of varying duration and size

Achieved Error Rates

<table>
<thead>
<tr>
<th>Bit Rate</th>
<th>Error Without Cross Traffic</th>
<th>Error With Cross Traffic (No Message Splitting)</th>
<th>Error With Cross Traffic (Message Splitting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>67 bps</td>
<td>0%</td>
<td>3.30%</td>
<td>0%</td>
</tr>
<tr>
<td>134 bps</td>
<td>0%</td>
<td>42.80%</td>
<td>0%</td>
</tr>
<tr>
<td>335 bps</td>
<td>0%</td>
<td>Error&gt;80%</td>
<td>8.68%</td>
</tr>
</tbody>
</table>

Empirical Evaluation Parameters

- The Hurst measure of self similarity for our covert channel remains well below the threshold of anomalous behavior.
- To optimize our channel we also consider the following empirical factors:
  - Effect of Total Traffic Load/Network Conditions
  - Effect of Packet Size
  - Effect of Queuing Policy and Hypervisor

Mitigation Techniques

- Leveraging on the over-provisioned paths between nodes and high quality load balancers in data-centers, we suggest “path-hopping” to rate limit the capacity of the covert channel.
- Flow Selection: Can be done based on flow similarity, flow timing or just random.
- Flow Placement: Performed randomly, or by selecting either the earliest available or least crowded link.