Automated Attack Discovery in TCP Congestion Control Using a Model-guided Approach

Samuel Jero¹, Endadul Hoque², David Choffnes³, Alan Mislove³, and Cristina Nita-Rotaru³
¹Purdue University, ²Florida International University, and ³Northeastern University

Appeared in NDSS 2018

TCP Congestion Control Attacks

- **Congestion Control**
  - Prevents Congestion Collapse
  - Ensures fairness between flows

- **Long history of powerful attacks**
  - Decreased Throughput
  - Increased Throughput, starving other flows
  - Connection Stalls

**Model-based Attack Discovery**

1) **Model Congestion Control as a State Machine**

2) **Create Abstract Strategies from State Machine**

   - Any Attack MUST:
     - Change cwnd
     - Cause a Cycle

3) **Create Concrete Strategies from Abstract Strategies**

4) **Apply Concrete Strategies to Real Implementations**

**Evaluation**

- Evaluated 5 TCP implementations

**New Attacks**

<table>
<thead>
<tr>
<th>Attack Class</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-path Repeated Slow Start</td>
<td>Increased Throughput</td>
</tr>
<tr>
<td>Amplified Bursts</td>
<td>Increased Throughput</td>
</tr>
<tr>
<td>Ack Lost Data</td>
<td>Connection Stall</td>
</tr>
<tr>
<td>Slow Injected Acks</td>
<td>Decreased Throughput</td>
</tr>
<tr>
<td>Sawtooth Ack</td>
<td>Decreased Throughput</td>
</tr>
<tr>
<td>Dup Ack Injection</td>
<td>Decreased Throughput</td>
</tr>
<tr>
<td>Ack Amplification</td>
<td>Increased Throughput</td>
</tr>
<tr>
<td>Off-path Repeated Slow Start</td>
<td>Increased Throughput</td>
</tr>
</tbody>
</table>

**Why so many attacks?**

- Hundreds of implementations and variations
- Lack of unified specifications
- Complex, highly dynamic behavior

**Can we automatically test implementations for attacks?**

Key Challenge: Scalability, attacks are complex, multi-stage and the system is highly dynamic