Measuring and Analyzing DoS Flooding Attacks

Amir Farhat
Setup

- Flooding DoS experiments
- 144 experiments (5 trials each), 354GB of data
- ⇒ Difficult to collect data, unwieldy to manage
- ⇒ We developed a toolkit for this

Design Goals

⇒ Capture packets for low-overhead instrumentation
  ◆ 3% CPU and 0.5% memory utilization
⇒ Decode and transform packet captures
⇒ Group experiments for analysis
⇒ Automated as much as possible

Bonus: Comparative evaluation of storage engines
Toolkit Design

1. DeterLab

2. Processing Server

3. Server

   File System

   unzip exp1.zip

4. capture1.pcap
   capture2.pcap
   capture3.pcap
   ...

5. decode
   capture1.out
   capture2.out
   capture3.out
   ...

6. transform
   exp1.out
   exp2.out
   exp3.out

7. combine

8. Database

scp exp1.zip
Next

Capture Decoding Times

Experiment Group Storage Sizes

Read Query Times
Next

Capture Decoding Times

Experiment Group Storage Sizes

Read Query Times
<table>
<thead>
<tr>
<th>Table Name</th>
<th>PostgreSQL</th>
<th>ClickHouse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table A</td>
<td>1,394 MB (99.7%)</td>
<td>207 MB (99.9%)</td>
</tr>
<tr>
<td>Table B</td>
<td>4 MB (&lt; 0.5%)</td>
<td>135 KB (&lt; 0.01%)</td>
</tr>
<tr>
<td>Table C</td>
<td>32 KB (&lt; 0.01%)</td>
<td>945 B (&lt; 0.01%)</td>
</tr>
<tr>
<td>Table D</td>
<td>32 KB (&lt; 0.01%)</td>
<td>3 KB (&lt; 0.01%)</td>
</tr>
<tr>
<td>Table E</td>
<td>32 KB (&lt; 0.01%)</td>
<td>357 B (&lt; 0.01%)</td>
</tr>
<tr>
<td>Table F</td>
<td>32 KB (&lt; 0.01%)</td>
<td>382 B (&lt; 0.01%)</td>
</tr>
<tr>
<td>Table G</td>
<td>32 KB (&lt; 0.01%)</td>
<td>569 B (&lt; 0.01%)</td>
</tr>
<tr>
<td>Table H</td>
<td>24 KB (&lt; 0.01%)</td>
<td>1 KB (&lt; 0.01%)</td>
</tr>
</tbody>
</table>
Next

Capture Decoding Times

Experiment Group Storage Sizes

Read Query Times
Conclusion

- Packet capture has low overhead
  - 3% CPU and 0.5% memory utilization
- But it introduces complexity in processing
  - Introduces decoding and transformation stages
  - Decoding stage is a bottleneck, 6+ mins for 1.5 min attack
  - We need faster but still flexible packet capture decoders
- ClickHouse is a fantastic choice for grouping experiments
  - Fast writes and reads
  - Saves 85%+ in storage