TCP Reset Cookies

Patrik Goldschmidt
xgolds00@stud.fit.vutbr.cz

#57

HIGH-LEVEL OVERVIEW

Unknown client

<table>
<thead>
<tr>
<th>Client (unknown)</th>
<th>RST cookies</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish connection</td>
<td><em>drop segment</em></td>
<td>Validate yourself first!</td>
</tr>
</tbody>
</table>

Known client

<table>
<thead>
<tr>
<th>Client (known)</th>
<th>RST cookies</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish connection</td>
<td>Forward segment</td>
<td></td>
</tr>
</tbody>
</table>

WHY SHOULD I CARE?

- Bad guys like to DDoS (Cisco prognosis - 14.5M p.a by 2022).
- TCP is a popular target.

WHAT IS IT?

TCP Reset cookies is a heuristic DDoS mitigation technique, which utilizes the three-way-handshake mechanism. The main idea is to establish a security association with clients before allowing their connection requests. This is achieved by intentionally crafting an invalid SYN-ACK response to the first SYN received from a client.

WHY SHOULD I USE THAT?

- Blocks regular as well as more sophisticated DoS SYN Floods.
- Limits and blocks attackers who are somehow able to bypass the security mechanism.
- Able to create lists of both trusted and untrusted hosts.

WHAT IS THE COST?

- First attempt to establish a session always fails.
- And TCP SYN retransmission takes some time...
- Up to 1 second, dependent on the host OS.

WHERE DOES THAT RUN?

Integrated into DDoS protection solution by CESNET, deployed on CESNET's backbone and NIX.CZ.

Figure 3: Distribution of DDoS attacks by type. Q4 2018. by Kaspersky Lab (DDoS report on securelist.com)

Figure 4: RST Cookies functionality

Figure 5: Transaction time performance comparison (Scientific Linux 7.4)