Automatic Identification of the Amplifiers in DRDoS attacks
Shiqi Shen, Deli Gong, Muoi Tran

Motivation

Current Solutions
Manually analyzing existing protocols

Disadvantages
1) Numerous potential vulnerable protocols
2) Complex protocol designs
3) Unpublished protocol designs

Goals & Insights

Available Information
Anonymized traffic packets

Reduce the scale of target traffic
traffic packets of DRDoS attacks

O1: Client/server port is fixed
O2: Amplification Factor is high

Find the traffic pattern

Overview

C1: Data Source.
IPs are anonymized
Payloads are removed

C2: Data Volume.
Continuous real traffic capture on backbone link (CADIA passive 2015)

C3: Data noise.
Negative impact on the analyzing process

Challenges & Solutions

S1: Grouping Packets
Pairflow: \(< C_{IP}, S_{IP}, C_{port}, S_{port}, B_{2s}, B_{2c}, t >\>

S2: Identifying potential vulnerable protocols

Computing Amplification Factor (AF)
\[ AF = \frac{Traffic[Amplifier to Victim]}{Traffic [Attacker to Amplifier]} \]

Reducing the scale of target traffic
Only the traffic of which the AF is above threshold \( \alpha \) is utilized in the further steps

Finding the patterns among traffic
Certain AF ratio, fixed Payload size ...

S3: Confirming vulnerable protocols
Manually analyzing the protocol if the detail information is available

Key Results

Suspected vulnerable protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Confirmed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS IP SLA control</td>
<td>1967</td>
<td>Partial [1]</td>
</tr>
<tr>
<td>Steam</td>
<td>27015</td>
<td>Yes [2]</td>
</tr>
<tr>
<td>Battlefield 2 and mods</td>
<td>16567</td>
<td>No</td>
</tr>
<tr>
<td>SIP</td>
<td>5060</td>
<td>Yes [2]</td>
</tr>
<tr>
<td>IPSec NAT Traversal</td>
<td>4500</td>
<td>No</td>
</tr>
<tr>
<td>Quake III</td>
<td>27960</td>
<td>Yes [2]</td>
</tr>
</tbody>
</table>

Pairflows and AF summary

References

[1] CVE-2011-3272