Two Novel Systems: Clouseau and RAD

Clouseau enables routers to learn associations between hop-count or previous hop and a source IP, and use it to detect spoofed packets. RAD adds cryptographic marks to packets, enabling routers to filter spoofed traffic and sources to detect replies to spoofed traffic.

1. Clouseau routers learn associations by probing one-way TCP data traffic. Probing is performed by dropping randomly chosen packets and checking if they were repeated. Forwarded packets are recorded and they should not be repeated by source.

2. Information about hop-count and previous hops is extracted from compliant sources’ traffic. Probing repeats periodically.

3. RAD adds two cryptographic marks to packets.
   a) Request mark is added by source host, copied in replies. Source can differentiate replies to its requests vs replies to spoofed requests using this mark.
   b) Source mark is added by source host, replaced by source AS. Core routers use this mark to filter traffic spoofing participant’s addresses.

Clouseau and RAD can drastically reduce spoofed and reflected traffic for its participants and for all Internet hosts!

Approach and Impact

<table>
<thead>
<tr>
<th>Our approach</th>
<th>Research impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Clouseau and RAD are effective in sparse, isolated deployment; work in presence of asymmetric routing and route changes</td>
<td>• Spoofing defenses are most effective if deployed strategically by top ASes</td>
</tr>
<tr>
<td>• Deployment on top 50 ASes reduces spoofed and reflected traffic for everyone</td>
<td>• Out of eight defenses proposed so far, only HCF is effective in isolated deployment</td>
</tr>
</tbody>
</table>

Expected cost: Clouseau’s probing introduces minor delays into traffic. Clouseau and RAD routers must maintain per source IP or per source AS tables, each packet is compared against tables. RAD routers perform hash operation during comparison.

Resilience to attacks: Clouseau is resilient to attackers guessing what packets to repeat, or colluding with destinations to trick Clouseau into learning wrong associations. RAD is resilient to attackers that sniff traffic or probe to learn associations between traffic contents and marks.

EFFECTIVENESS OF EXISTING SPOOFING DEFENSES

Spoofed traffic filtering in isolated deployment
Spoofed traffic filtering in strategic deployment
Reflected traffic filtering in strategic deployment