Data Range: Fri Feb 11 08:16:52 EST 2005 to Sat Dec 7 14:52:10 EST 2013
Total Tests: 19181
Unique IPs tested: 15132
Unique Routed Prefixes tested from: 8258
Unique ASes tested from: 2582

Announced Address Space
- UnSpoofable: 332M (82.1%)
- Spoofable: 33.1M (8.2%)
- Inconsistent: 39.3M (9.7%)

Prefixes
- UnSpoofable: 3092 (75.4%)
- Spoofable: 940 (22.9%)
- Inconsistent: 68 (7.7%)

Autonomous Systems
- UnSpoofable: 1026 (61.6%)
- Mostly spoofable: 409 (24.6%)
- Partly spoofable: 117 (6.8%)
- Fully spoofable: 113 (7.0%)
Send k fragments into network
for \( d := 0 \) to \( \max d \) for all ordered combinations of fragments at distance \( d \)

construct edge \( z \)

if \( d \neq 0 \) then

\( z := z \oplus last \)

if \( \text{Hash(EvenBits}(z)) = \text{OddBits}(z) \) then

insert edge \((z, \text{EvenBits}(z), d)\) into \( G \)

\( last := \text{EvenBits}(z) \);
<table>
<thead>
<tr>
<th></th>
<th>Management overhead</th>
<th>Network overhead</th>
<th>Router overhead</th>
<th>Distributed capability</th>
<th>Post-mortem capability</th>
<th>Preventative/ reactive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress filtering</td>
<td>Moderate</td>
<td>Low</td>
<td>Moderate</td>
<td>N/A</td>
<td>N/A</td>
<td>Preventative</td>
</tr>
<tr>
<td>Link testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input debugging</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Good</td>
<td>Poor</td>
<td>Reactive</td>
</tr>
<tr>
<td>Controlled flooding</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Poor</td>
<td>Excellent</td>
<td>Reactive</td>
</tr>
<tr>
<td>Logging</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Excellent</td>
<td>Good</td>
<td>Reactive</td>
</tr>
<tr>
<td>ICMP Traceback</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Excellent</td>
<td>Excellent</td>
<td>Reactive</td>
</tr>
<tr>
<td>Marking</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Good</td>
<td>Excellent</td>
<td>Reactive</td>
</tr>
</tbody>
</table>

Table 1: Qualitative comparison of existing schemes for combating anonymous attacks and the probabilistic marking approach we propose.
Figure 3. Example of our initial marking scheme. The packet travels from the attacker A to the victim V across the routers R1 to R5. Each router uses the TTL value of the packet to index into the IP identification field to insert its marking. In this example we show a 1-bit marking in a 4-bit field for simplicity.
**Diffuse DDoS: Reflector Attack**

Request: $src = \text{victim}$  
$dst = \text{reflector}$

Control traffic directs slaves at victim & reflectors

Reflectors send streams of non-spoofed but unsolicited traffic to victim

Reply: $src = \text{reflector}$  
$dst = \text{victim}$