Polymorphic Worm Filtering (cont.)

- Structured nature of buffer overflow worms:
  - protocol embedding
    - must remain hidden until critical trigger point: affects localization
  - length invariance
    - must trigger buffer overflow: abnormal length

(difficult to hide)
Example Signatures

**CodeRed1**

```
HTTP Request:
GET /default.ida?<224 chars %u9090...%u00=a HTTP/1.0 <worm code>
```

**Slammer**

```
create registry entry(0x04) and payload size > 16 B
```

**Slapper**

```
type of packet = 0x02(client_master_key) and size of key (0x80) > 8
```
Problem Domain: Worm Attack

David Moore (dmoore@caida.org)
Problem Domain: Worm Attack

Sapphire

David Moore (dmoore@caida.org)
DoS Attack

Periodic Attack
1 hour per day

Punctuated Attack
every minute
Base Benchmark Workload

- **Composition**
  - 32 types of worm traffic (26.3%)
  - TCP/UDP non-worm traffic (65.3% / 8.4%)

- **Worm**
  - BO & non-BO

- **Run-time**
  - 300 seconds

- **Logs**
  - per-hop
  - end-to-end
Experimental Testbed

- **Physical set-up**
  - 5 x86 attack hosts, 5 x86 victim hosts, 1 Gbps NICs
  - 2 GigE switches
  - IXP1200 worm filter network appliance: layer-2 relay

CBR & VBR worm workload

trace-based & artificial
Base Benchmark Filtering Performance

- Comparison: worm filter on vs. off
  - software on/off switch
  - packet loss rate, false positive, false negative

<table>
<thead>
<tr>
<th></th>
<th>Filter Off</th>
<th></th>
<th>Filter On</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Send-Rate</td>
<td>Recv-Rate</td>
<td>Loss-Rate</td>
<td>Send-Rate</td>
</tr>
<tr>
<td>Gen-1 (TCP)</td>
<td>220 Mbps</td>
<td>220 Mbps</td>
<td>0 %</td>
<td>220 Mbps</td>
</tr>
<tr>
<td>Gen-2 (TCP)</td>
<td>220 Mbps</td>
<td>220 Mbps</td>
<td>0 %</td>
<td>220 Mbps</td>
</tr>
<tr>
<td>Gen-3 (TCP)</td>
<td>220 Mbps</td>
<td>220 Mbps</td>
<td>0 %</td>
<td>220 Mbps</td>
</tr>
<tr>
<td>Gen-4 (TCP)</td>
<td>220 Mbps</td>
<td>220 Mbps</td>
<td>0 %</td>
<td>220 Mbps</td>
</tr>
<tr>
<td>Gen-5 (UDP)</td>
<td>97 Mbps</td>
<td>97 Mbps</td>
<td>0 %</td>
<td>60.5 Mbps</td>
</tr>
<tr>
<td>Total (80,733 PPS)</td>
<td>977 Mbps</td>
<td>977 Mbps</td>
<td>0 %</td>
<td>940 Mbps</td>
</tr>
<tr>
<td>Overload (82,581 PPS)</td>
<td>999.2 Mbps</td>
<td>2.9 %</td>
<td>999.2 Mbps</td>
<td>1.8 %</td>
</tr>
</tbody>
</table>

Table 2: Gigabit IXP1200 worm filter performance: filter turn off and on.

loss free zero false positive/negative: 940 Mbps