A Framework for
Classifying Denial of Service Attacks

Bob Callaway    William Gates

North Carolina State University
CSC/ECE 573 - Internet Protocols
Semester Research Project

December 3, 2003

Based on A Framework for Classifying Denial Of Service Attacks by Hussain, et al, in ACM SIGCOMM 2003, Karlsruhe, Germany
Introduction

- Classification vs Detection
- Classification Framework
- Results of Analysis
- Conclusions
Detection

- Detection consists of monitoring arrival rates of traffic to single destination address
- If the number of sources detected exceeds a certain threshold, then the traffic is flagged as a possible DoS attack

Classification

- Classification consists of determining the structure of the attack (i.e. single source, multiple sources, etc.)
- Classification techniques are essential for implementing effective mitigation schemes
- Possible classification techniques include header analysis, ramp-up behavior analysis, and spectral analysis
Several fields within the IP header are analyzed in order to classify an attack sequence

- **Identification Field**
  - 16 bit field, used for reassembling fragments
  - Most operating systems increment this field for every packet sent out
  - *Field can be randomized, also susceptible to bit ordering issues*

- **Time To Live (TTL)**
  - 8 bit field, used for routing loop detection
  - We assume stable routing conditions (i.e. TTL is constant for src/dst pair)
A more robust method for classifying attacks as single or multi-source is to consider their spectral characteristics.

\[
S(f) = \sum_{k=0}^{M} r(k)e^{-j2\pi fk}
\]

\[
P(f) = \sum_{i=0}^{f-1} \frac{(S(i) + S(i + 1))}{2}
\]

\[
C(f) = \frac{P(f)}{P(f_{max})}
\]
We wrote a C program using the libpcap libraries that analyzed the headers of attack traffic traces. We had three traces to analyze, and counted the number of unique sequences which could possibly represent an DoS attack.

<table>
<thead>
<tr>
<th>Trace File</th>
<th>Attack Traces Identified with id</th>
<th>Attack Traces Identified with ntohs(id)</th>
<th>Attacks Reported in Paper</th>
</tr>
</thead>
<tbody>
<tr>
<td>attack4</td>
<td>39</td>
<td>55</td>
<td>16</td>
</tr>
<tr>
<td>attack18</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>attack29</td>
<td>11</td>
<td>6</td>
<td>15</td>
</tr>
</tbody>
</table>
Results for Spectral Analysis - Single Source

**Plot from Paper**

**Plot from Our Analysis**

(a) Single-source
Results for Spectral Analysis - Multiple Sources

Plot from Paper

Plot from Our Analysis

(b) Multi-source
Conclusions

- Header analysis is susceptible to many different spoofing techniques which makes it ineffective as standalone classification technique.
- Spectral analysis is more difficult to spoof and provides a more robust classification tool.
- A combination of different classification techniques will likely provide the optimum tool for DoS attack classification.