PIRANHA
Protocol Implementation Robustness And Network Hardness Analysis

John Linwood Griffin
FTCS-29 • June 16, 1999

Carnegie Mellon
PIRANHA: what & why

• Problem:
  – Protocol implementations (TCP, …) must be robust
  – Bad network input is inevitable
  – Existing tools focus on behavioral correctness and performance only -- not robustness!

• Solution:
  – PIRANHA: Repeatable robustness testing of protocol implementations
Core technologies

• PIRANHA combines the *xio* TCP library...
  – Application-level protocol stack
  – Fine-grain but convenient packet control

• with the *Ballista* testing methodology.
  – Probe with invalid parameters at the interface

```c
malloc(-1)
fopen(NULL, NULL)
```
How PIRANHA works

• Network packets are the “interface”
• Create packet with invalid values

<table>
<thead>
<tr>
<th></th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Flags</th>
<th>Sequence Number</th>
<th>Acknowledgment Number</th>
<th>Length</th>
<th>Reserved</th>
<th>Window Size</th>
<th>Urgent Offset</th>
<th>Options (if any)</th>
<th>Data (if any)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

FTCS-29 Session 3B Griffin: PIRANHA
PIRANHA in action

• Position remote System under Test (SuT) in one of eleven TCP protocol states
  – Test support software runs on SuT

• Create exceptional packet

  
  Original Sequence Number
  31

  Modify
  -1

  Exceptional Sequence Number
  30

• Probe SuT with exceptional packet
• Capture and classify the response
PIRANHA taxonomy

• What is a robustness failure?
  – Failure to return a “reset” packet
  – Inability to progress to next protocol state
  – Dropped connection
  – Lost or modified data

• (Initial) focus is exception handling, not:
  – Packet timing issues
  – High-level protocol behavior
PIRANHA people

- Greg Ganger
- Garth Goodson
- Phil Koopman
- Laurel Fan

Piranha images courtesy of The Piranha Database [http://www.pcio.com/piranha].
• The following slides are available as an aid for answering questions:
  – Why protocol testing?
  – Ichthyology (related work)
Why protocol testing?

- Protocols = languages for networks
  - Implemented in both hardware and software
  - Implementations must conform and be robust
  - Unfortunately, bad network input is inevitable

- Implementations are tough to get right
  - Complex protocols have many rules
  - Communications substrates can corrupt bits
  - Systems malfunction and people misbehave
Ichthyology (related work)

• Active behavioral analysis
  – Active Probing [Comer94]
  – ORCHESTRA [Dawson96]

• Passive behavioral analysis
  – tcpanaly [Paxson97]

• Performance analysis