

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

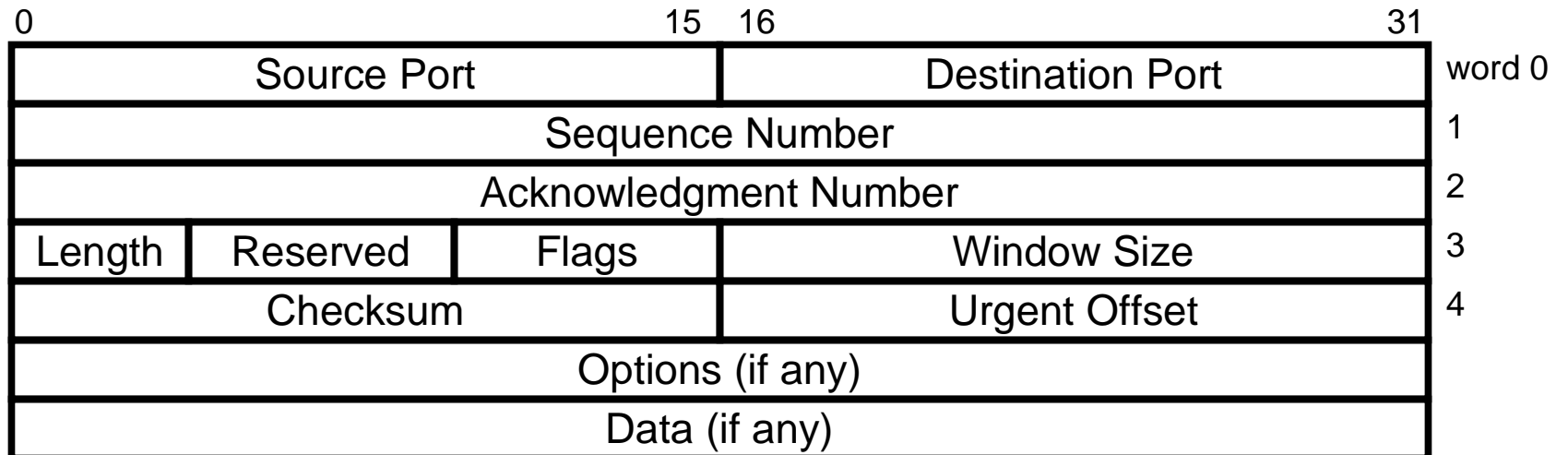
```
malloc(-1)
```

```
fopen(NULL, NULL)
```

How PIRANHA works



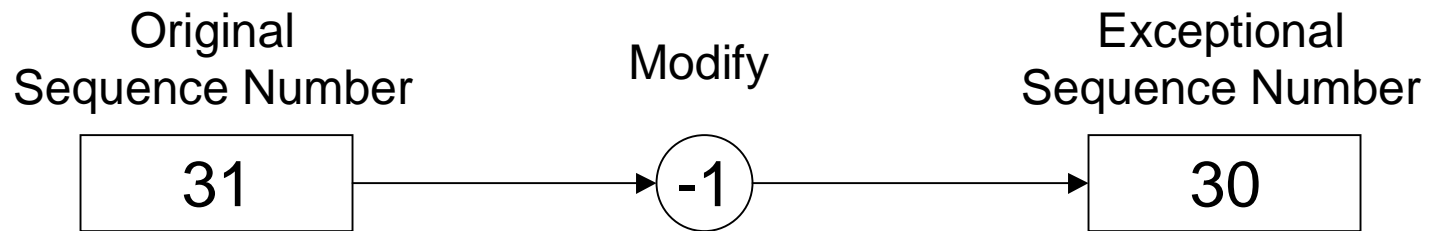
- Network packets are the “interface”
- Create packet with invalid values



PIRANHA in action



- Position remote **S**ystem **u**nder **T**est (SuT) in one of eleven TCP protocol states
 - Test support software runs on SuT
- Create exceptional packet



- Probe SuT with exceptional packet
- Capture and classify the response

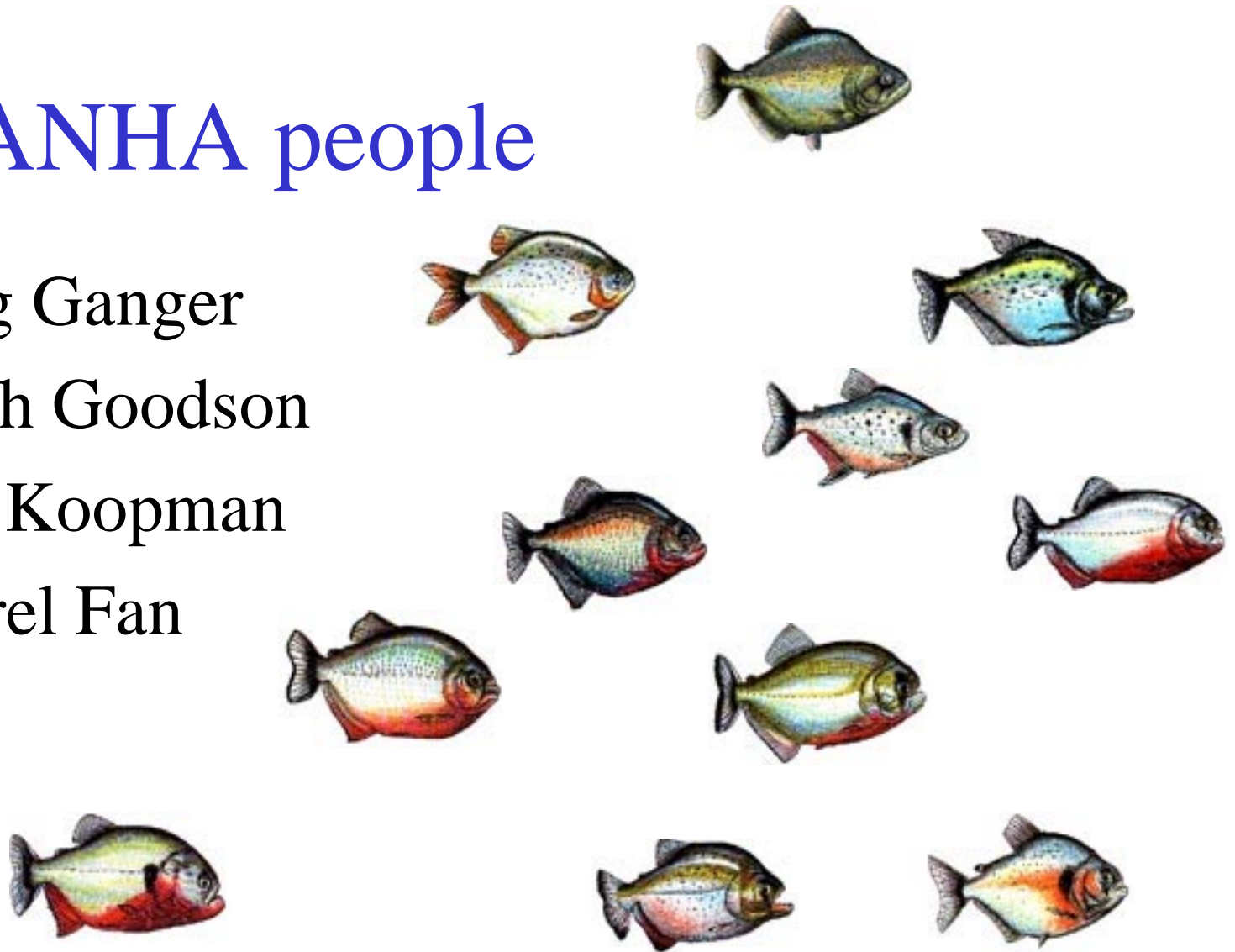
PIRANHA taxonomy



- 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