主动响应Active Response：

《An Analysis of TCP Reset Behaviour on the Internet》

# An Analysis of TCP Reset Behaviour on the Internet

## （SIGCOMM 2005）

- 结论：RSTs are surprisingly common on the Internet. They examined a year of SYN/FIN/RST packets from the University of Calgary's border and found that roughly 15% of all TCP flows were terminated by a RST packet after payload had already been sent in at least one direction. The reset rate was even higher for HTTP traffic, with 22% of the connections terminated by a client-side RST, and 3% by a server-side RST.
- 方法：Tcpdump截获报文，用Bro分析

# 主动响应Active Response：

## 《An Analysis of TCP Reset Behaviour on the Internet》

The measurement results in this paper focus on two traces.

The first covers the year-long period spanning October 1, 2003 through September 30, 2004. This trace contains 26,839,809,058 packets, comprising 7,893,035,860 TCP connections.

The second trace records all packets sent via the commercial Internet link between non-university clients and the campus Web server. There are 361,420 connections and 14,393,799 packets in this trace

REJECT
means that for every packet received an ICMP port unreachable packet is sent to the source address.

Example:  Port 23 is set to REJECT:

```
08:29:33.908826 reddwarf.xix.com.2876 > megahard.xix.com.23: S
    611071769:611071769(0) win 32120
    <mss 1460,sackOK,timestamp 8136624[|tcp]> (DF) [tos 0x10]

08:29:33.908826 megahard.xix.com > reddwarf.xix.com:
    icmp: megahard.xix.com tcp port 23 unreachable [tos 0xd0]
```

The response to the syn-packet (S) is an ICMP ``port unreachable''.

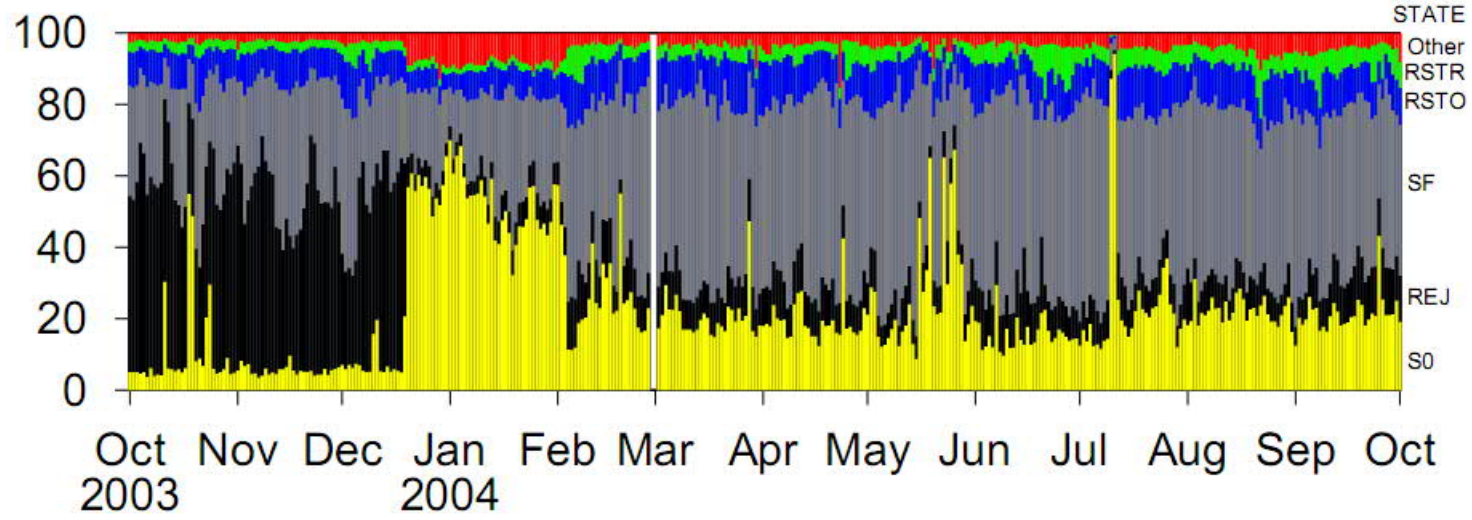
# 主动响应Active Response：

《An Analysis of TCP Reset Behaviour on the Internet》

RSTR: Reset from Server, RSTO: Reset from client

SF: normal,  S0 and REJ: only syn or reject connection

All TCP Connections

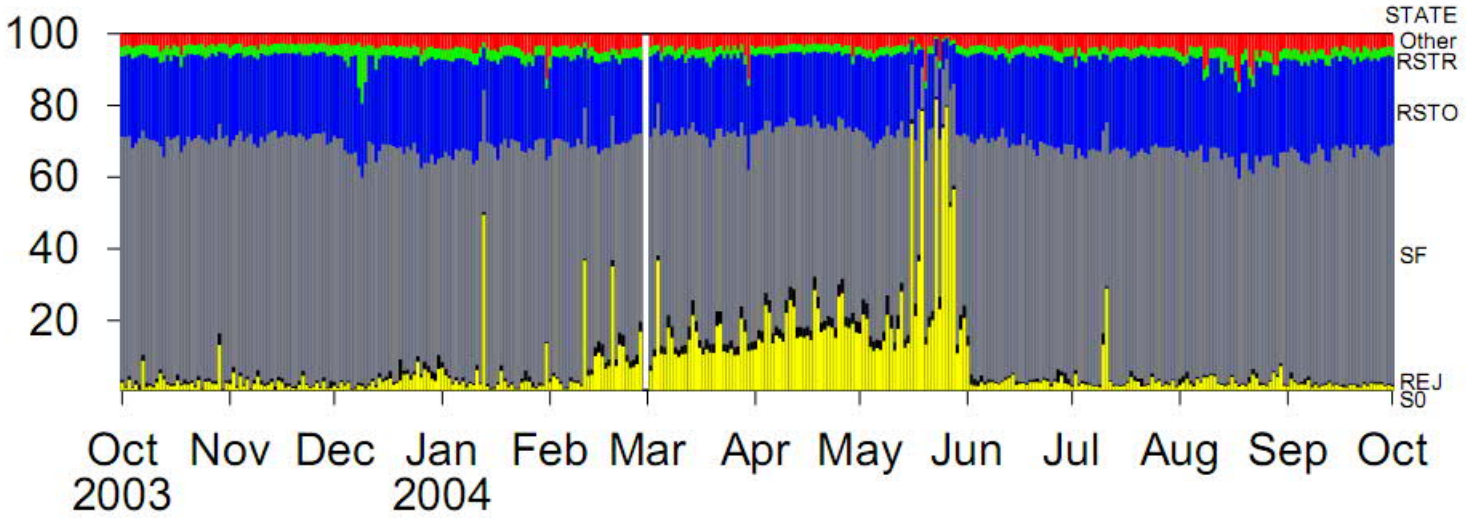


# 主动响应Active Response：

《An Analysis of TCP Reset Behaviour on the Internet》

RSTR: Reset from Server, RSTO: Reset from client

SF: normal, S0 and REJ: only syn or reject connection



# 主动响应Active Response：

## 《An Analysis of TCP Reset Behaviour on the Internet》结论：

The most prevalent anomaly is the absence of the normal FIN handshake for connection termination. Instead, connections are often reset by the client.

We believe that particular implementations of HTTP/TCP connection management cause this global trend.

# “Strange Attractors and TCP/IP Sequence Number Analysis”

A paper by Michal Zalewski in 2001

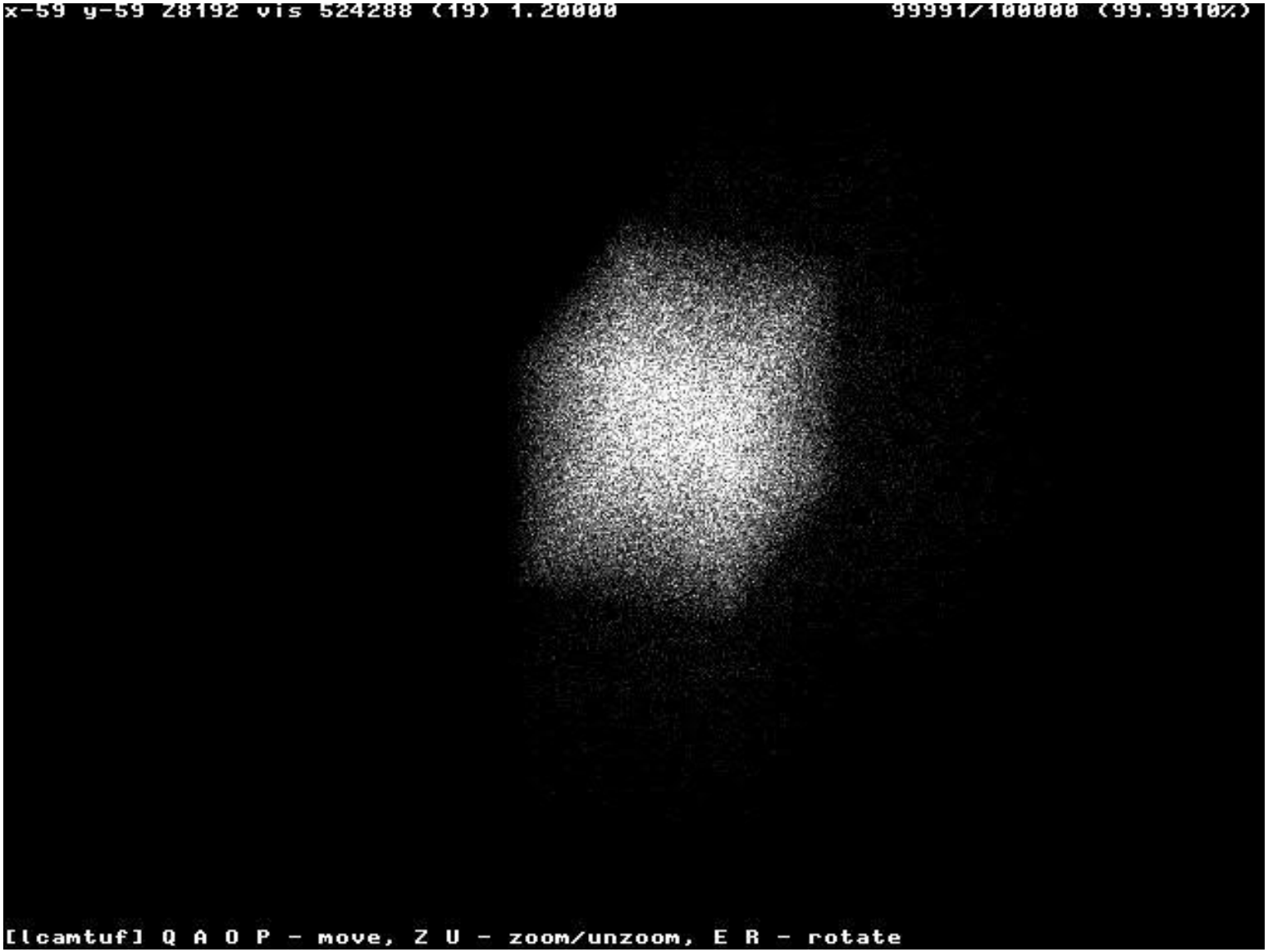
- Studied, and graphed the randomness of Initial Sequence Numbers of various operating systems.
- Graphs the output of 100,000 ISNs for each OS.
- Attempts an ISN attack on each OS, and lists the difficulty for each.

Final Verdict:

OpenBSD is great, Linux is pretty good. Others have big problems.

# ISN Graph of: Linux 2.2

# ISN Graph of: OpenBSD 2.8



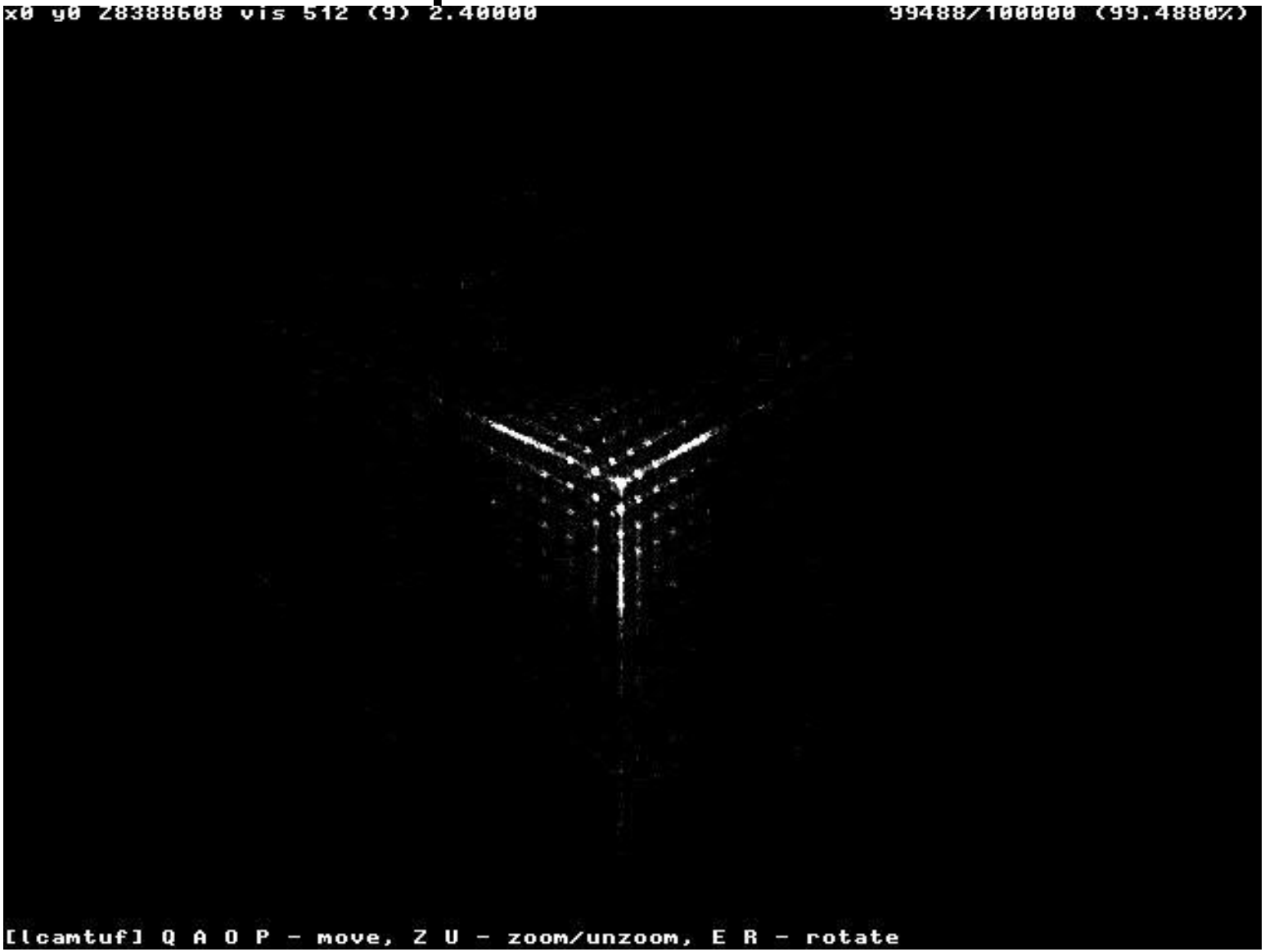
# ISN Graph of: OpenBSD 2.9 rewritten by Niels Provos

# ISN Graph of: Solaris, weak mode

# ISN Graph of: Solaris, strong mode

# ISN Graph of: Windows 95

# ISN Graph of: Windows 98SE



# ISN Graph of: Windows 2000