



# The Return of the Cube: Spinning the Security of SCinet

Stephen Lau  
NERSC Center Division, LBNL  
November 10, 2004



# Background



- SCxy – Annual High Performance Computing and Networking conference
  - [www.sc-conference.org](http://www.sc-conference.org)
  - SC04 in Pittsburgh, PA, Nov 2004
  - SC03 in Phoenix, Arizona, Nov 2003
- SCinet – High Performance Network at SC conference
  - [scinet.supercomp.org](http://scinet.supercomp.org)



**SC**inet



# SC Conference



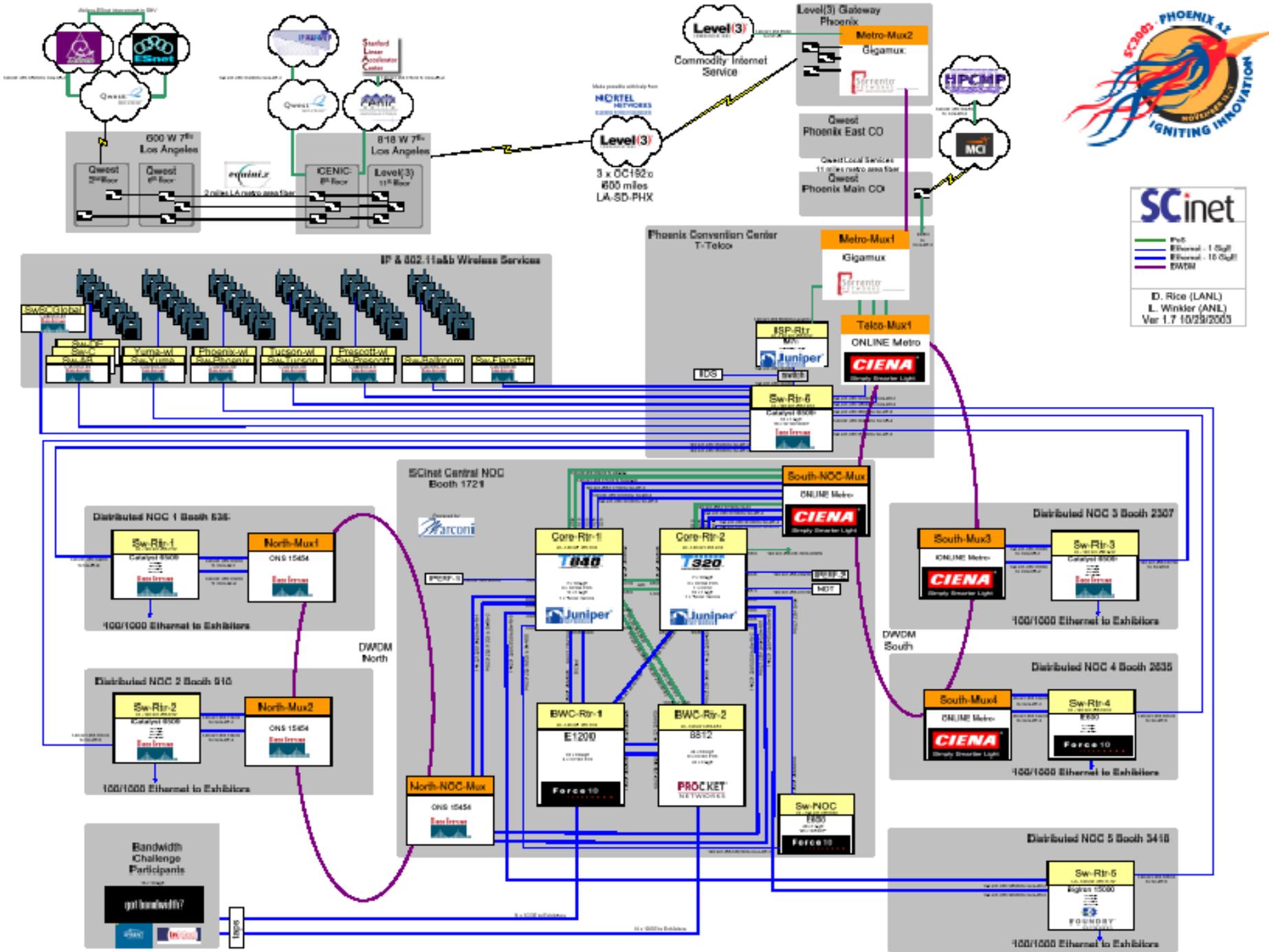
- Attracts academic, industrial and government attendees
  - ~8000 attended SC03
  - DOE very well represented
- Exhibition
  - Large research institute component
    - Government, academic
  - Many prototype systems and demonstrations



# SCinet



- Conference network
  - Attendees, speakers and exhibitors
- Volunteers from DOE Labs, industry and educational institutes construct and tear down network
- Focuses on high performance and unfettered access
  - *NO* firewall or filtering

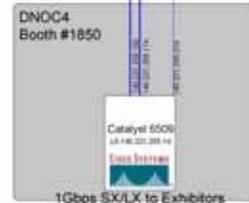
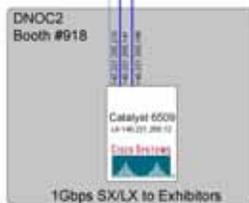
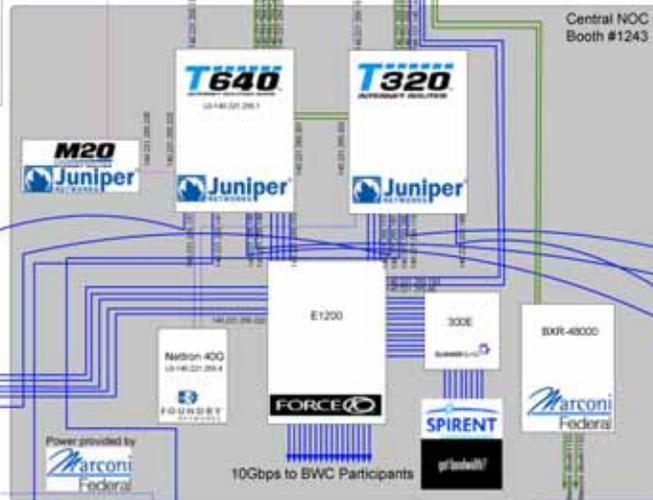
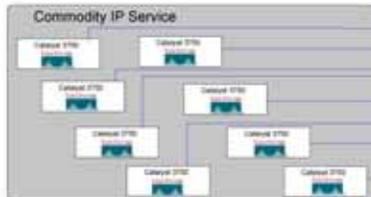
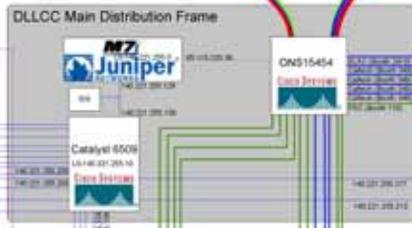
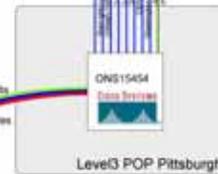


**SCinet**

— PoE  
 — Ethernet - 1 Gbps  
 — Ethernet - 10 Gbps  
 — DWDM

D. Rice (LANL)  
 L. Winkler (ANL)  
 Ver 1.7 10/29/2005

HPCMP



SCinet V1.2 Legend

- OC192 PoS
- 1G Ethernet
- 10G Ethernet
- OC48 PoS
- OC3 PoS
- L. Winter 10/29/2004



# SCinet 2003 NOC





# Result



- Many computer security incidents
- Sampling of SC03 security incidents
  - 3 root compromises
    - 2 on same system!
  - 63 *Welchia* infected systems
    - 2 repeat infections!
  - 6 Slammer worm infections
  - 10 Miscellany worm infections



# Problem



- The open Internet today is a *hostile* place
- Many exhibitors and attendees blissfully security unaware
  - Come from firewalled institutes
  - Unpatched demonstration systems
  - Just plain clueless
- Security compromises can bring the conference to a halt
- SCinet's high bandwidth network can be used against other sites



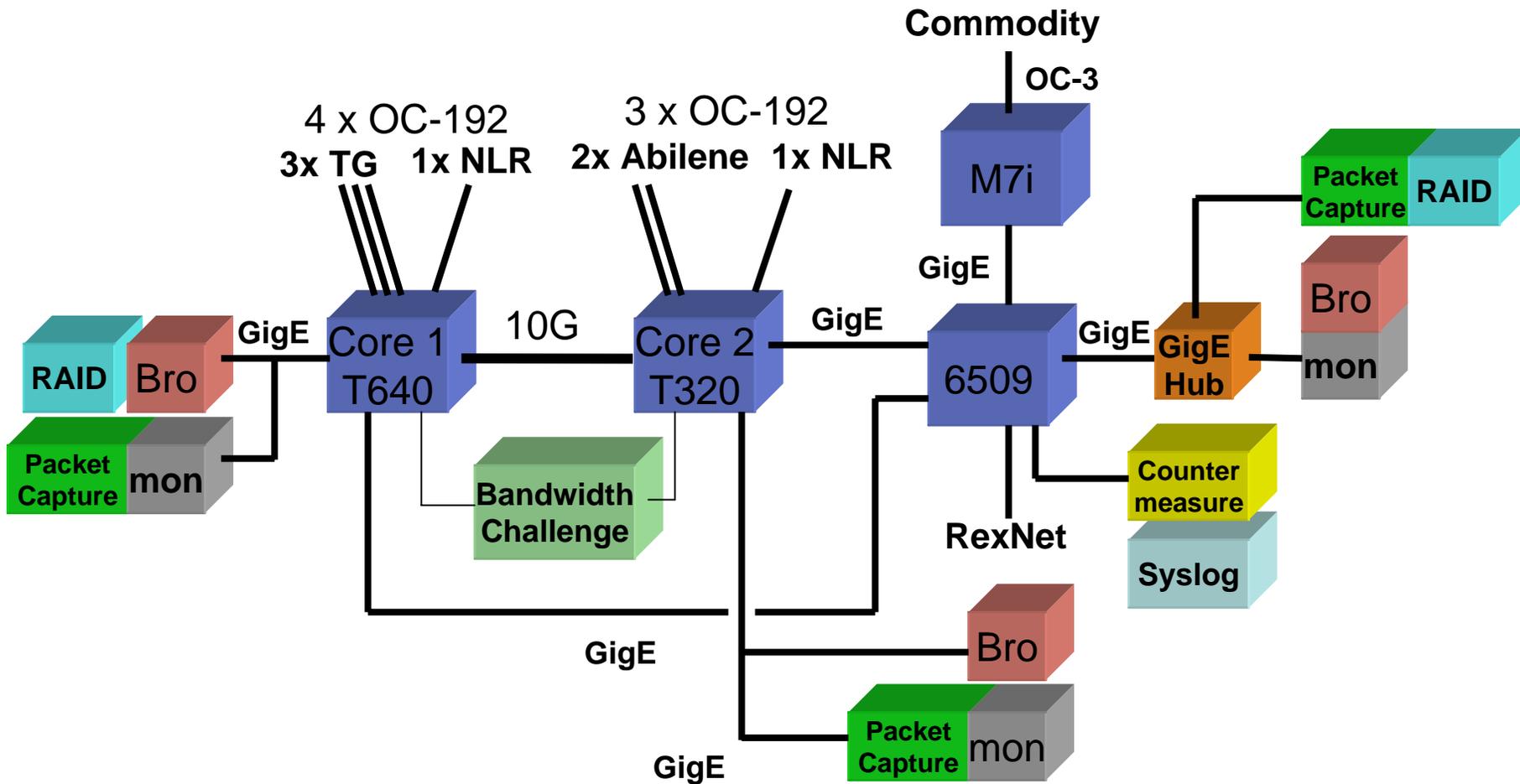
# (Partial) Solution



- Network security group within SCinet
  - Track down and remove 0nw3d systems (and some users)
    - Gets real old, real fast
- Deploy passive monitoring systems
  - Bro (LBNL)
  - mon (Sandia-CA)
  - Wireless monitoring
- Filter some SC infrastructure networks
  - Registration, SC office, etc
- Deploy active wireless “jails”
  - Infected wireless systems are restricted from network access
- Active counter measure system
  - Sandia-CA developed tool
  - Honeypot to detect and thwart malicious attackers



# SCinet 2004 Security Infrastructure





# Bro



- High performance intrusion detection system developed at LBNL and ICRI
  - Vern Paxson primary developer
- Grew out of tools developed to optimize and analyze network traffic
  - Based on operational experience with high performance networks
- Bro development goals
  - High speed network monitoring
  - Low packet loss rate
  - Mechanism separate from policy



# Bro



- Bro maintains and analyzes state
  - Not like signature based systems, i.e. Snort
- Keeps track of all network connections
  - Reacts to network behavior patterns
  - Allows for in depth analysis and forensics
- Used as SCinet's primary security tool since SC2001



# User Education



- Painfully obvious that attendees are security unaware
  - See previous re: security incidents
- But how to educate ~8000 wandering attendees?



# Capture Their Passwords!



- Use Bro to capture and display clear text passwords
  - telnet, ftp, rlogin
- Started at SC2001 in Denver, CO
  - Large screen display of scrolling passwords
  - No system names or user names
  - Filtered for bogus (or non G rated) entries





# Results



- Predominantly positive
  - Attendees have come to “expect” it
  - Some complaints – “That’s my password!”
- Some attempts to thwart system
  - Embedded images
  - Passwords such as “HiScinet!” (or worse)
- **Key Result:** Many attendees “shocked” that their passwords could be captured



# Wall of Shame



	Passwords	Root Passwords	NO Passwords	Scans
SC01 	1935	70	95	266
SC02 	486	6	N/A	756
SC03 	235	2	20	1118



# Patch, patch, patch...



- But why?
  - Because the open Internet is a hostile place!
- Scans
  - Directed searches for vulnerable services
- Worms
  - Constantly looking for new victims
- Problem:
  - How do you get this point across to attendees?



# Use Pretty Colors That Move



- Display Bro data in a graphical format
- Many “visualization” tools for network and security information
  - However most developed *for* network and security types
- Primary goal: Educate those who are *not* necessarily security aware



# The Cube



- Displays captured Bro data in 4D
  - Replayed over time
  
- TCP connection information
  - Complete connections
    - SYN/FIN
  - Rejected or incomplete connections
    - SYN/RST
    - SYN and no response



# The Cube Axes



- X Axis (red)
  - SCinet IP address space
- Z Axis (blue)
  - Global IP address space
  - 0.0.0.0 – 223.255.255.255 (no multicast)
- Y Axis (green)
  - Port number (0 – 65535)
  - Well known port numbers (22/ssh, 80/http, etc.)

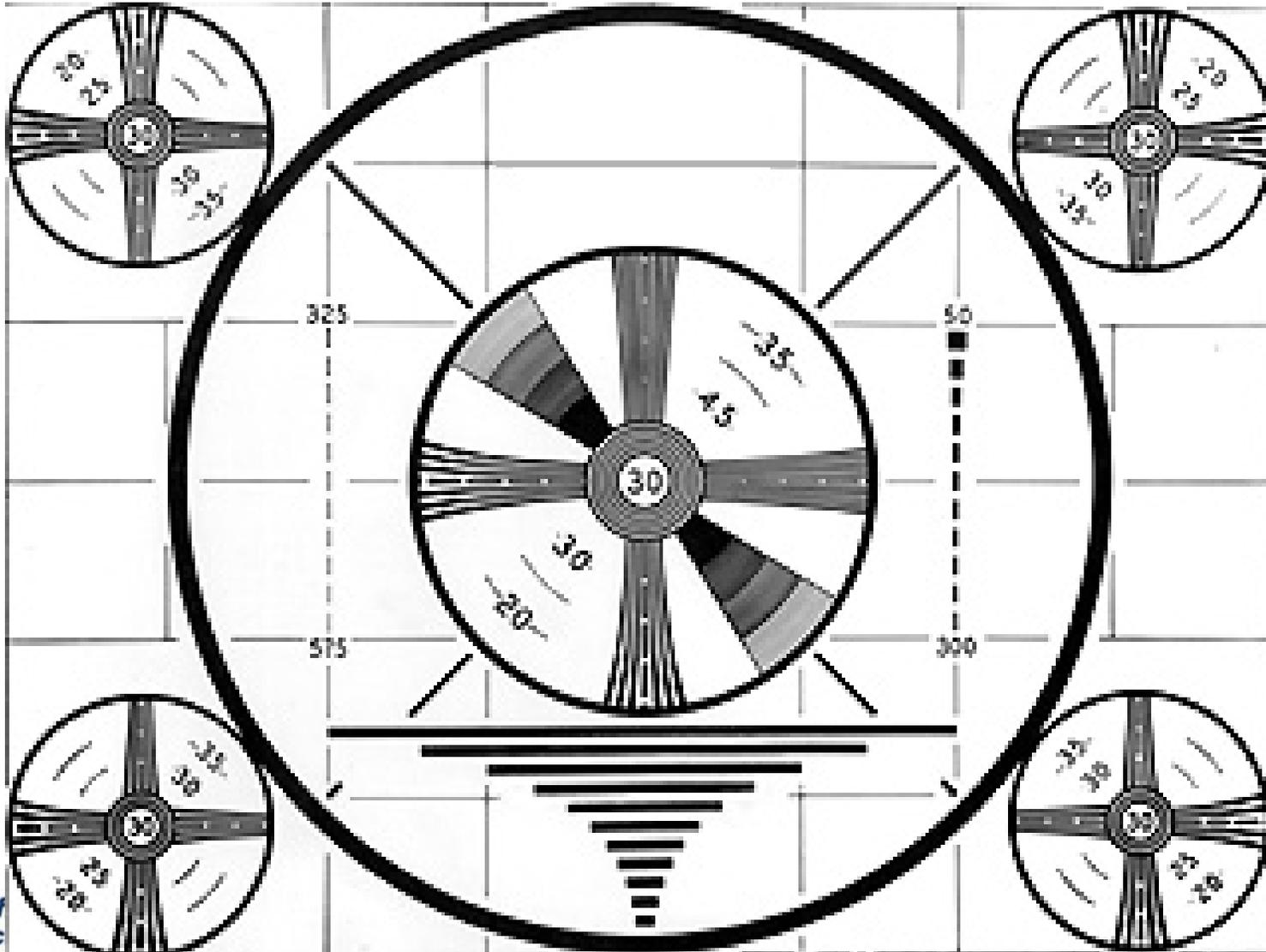


# The Data



- TCP connection instances represented by a point
  - (src IP addr, dst IP addr, port number)
- Rainbow colormap for points
  - Easier to locate in 3 space
  - Color of points have no meaning
  - Except: Grey points are *completed* connections

# INSERT DEMO HERE



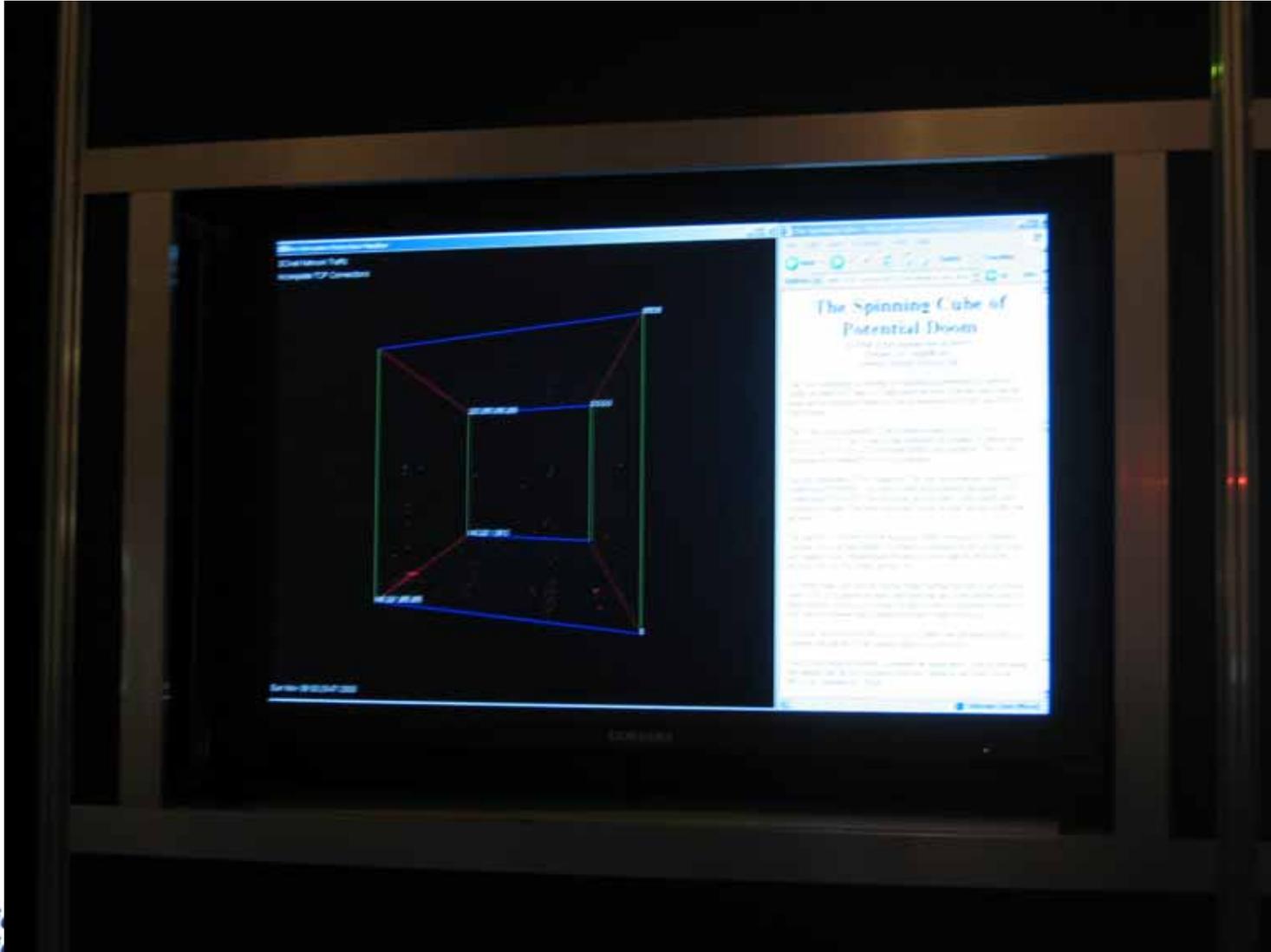


# Under the Hood



- Written in C++
- Uses OpenGL
  - Runs on platforms that support OpenGL
  - Either hardware or software emulation
- Runs on FreeBSD, OSX, Linux, Windows
- Uses Bro data files for source data
- No real time data updates during SC03

# The Cube at SC03



# Such Pretty Colors...



# Cube Mesmerization



It may turn you translucent  
if you are not careful!



# Lessons Learned



- People like pretty colors that move
- **Key Result:** Many attendees stated they never realized malicious traffic constantly occurred on the open Internet
- The Cube can be useful for security analysis
  - Lots and lots of interesting patterns
  - Potential for use as security analysis tool
- Can't please everyone
  - Several complaints lodged against the Cube



# The Future



- Many requested features
  - #1 requested: Screensaver mode
  - Ability to modify time playback
  - Logarithmic axes
  - Ability to “drill down” into the data
- SC2004
  - Cube on display at SCinet booth
  - Real Time monitoring of SCinet traffic at SC04



# Contact Information



Stephen Lau

Lawrence Berkeley National Labs / NERSC

1 Cyclotron Road, M/S 943

Berkeley, CA 94720

Phone: +1 (510) 486-7178

Email: [slau@lbl.gov](mailto:slau@lbl.gov)

PGP: 44C8 C9CB C15E 2AE1 7B0A

544E 9A04 AB2B F63F 748B

Cube Info:

<http://www.nersc.gov/security/TheSpinningCube.html>