CINBAD

Major Review Meeting
28 January 2010

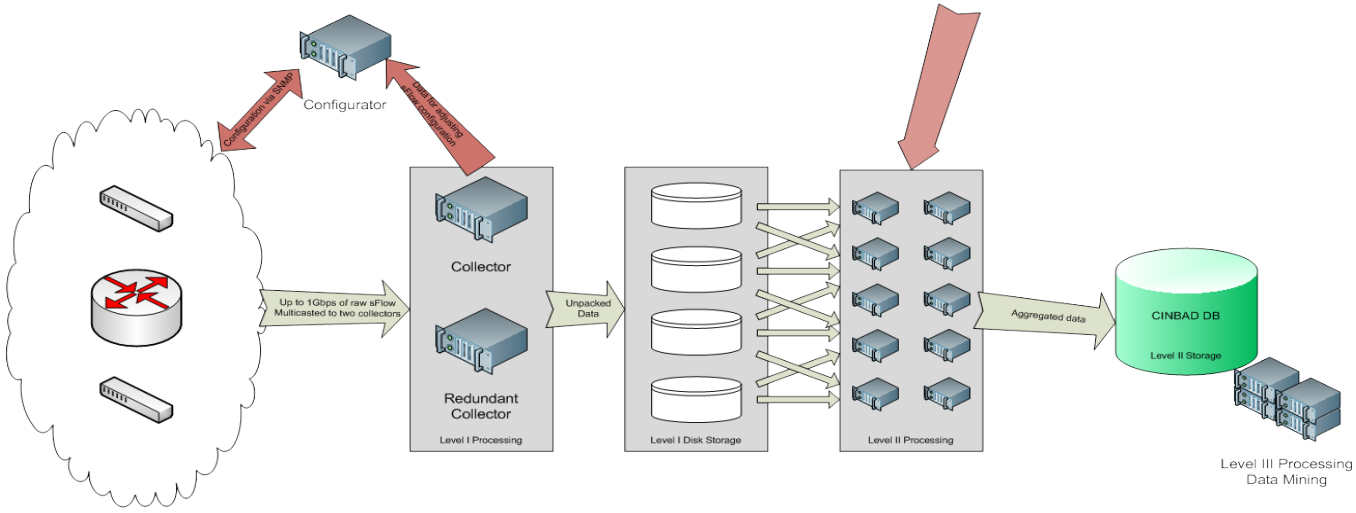
Ryszard Erazm Jurga - CERN
Milosz Marian Hulboj - CERN

Outline

- Update on
  - CINBAD data collection
  - Anomaly detection
- CINBAD tools for CERN Network Monitoring
- Collaborations

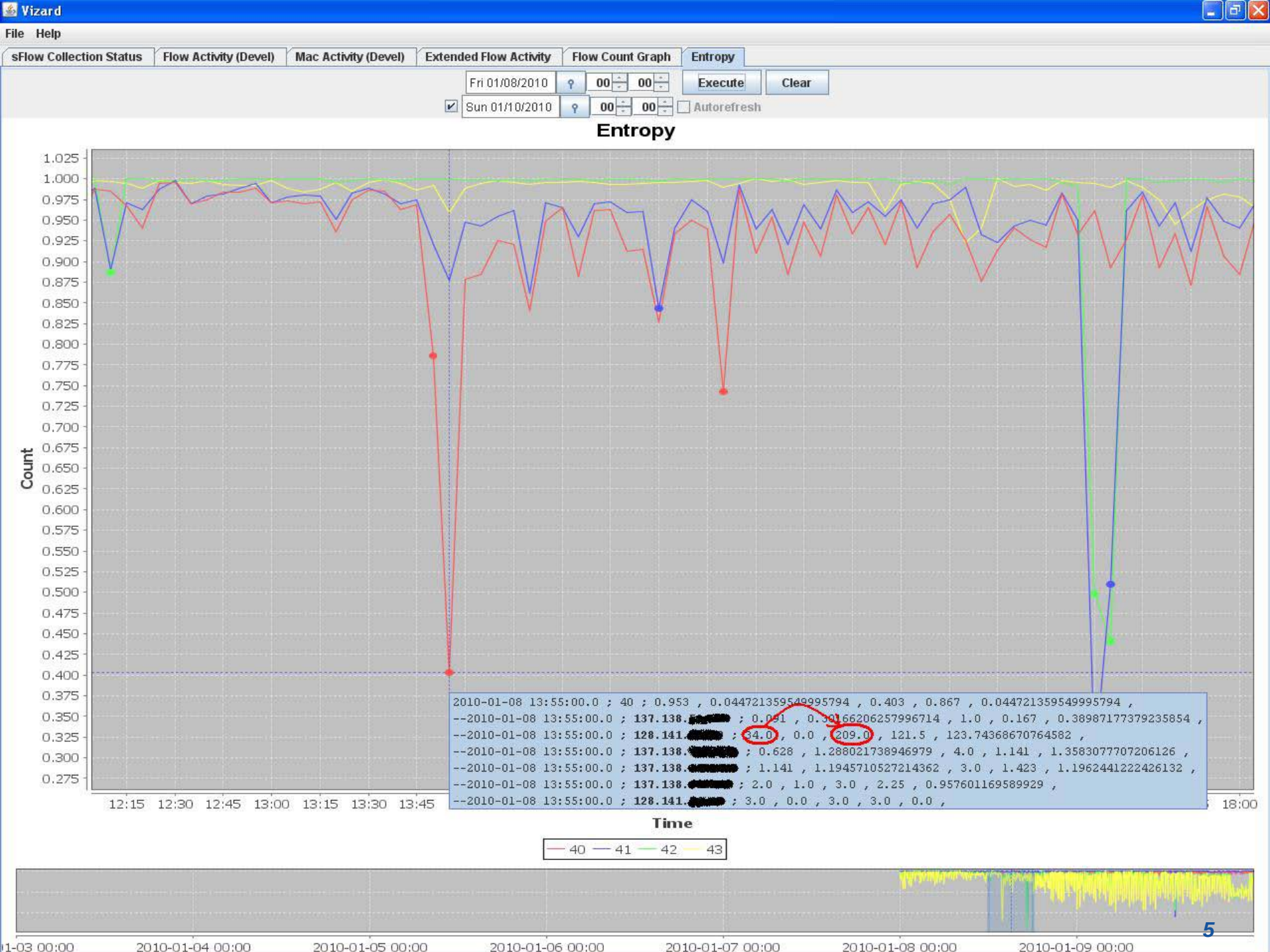
CINBAD data collection

- ~**20TB** data in 2009 (received, stored, analyzed)
- Currently
  - ~200-400mln sampled packets per day
  - ~900/10000 active switches/interfaces
  - ~80/4GB disk/oracle storage per day



Anomaly detection

- Both statistical analysis and pattern matching techniques in use
- Enhancements to detection tools:
  - Daily e-mail report from entropy analysis pointing out malicious hosts
  - New tool for visualizing and browsing anomaly alerts
- Anomalies
  - ~5M snort events in 2009 (60% IM, 15% P2P)
  - Recent anomalies found:
    - Conficker infections,
    - Printer abuser,
    - Internal network scans,
    - p2p, im, …


Vizard
File Help
sFlow Collection Status
Flow Activity (Devel)
Mac Activity (Devel)
Extended Flow Activity
Flow Count Graph
Entropy
Fri 01/08/2010
Sun 01/10/2010
Execute
Clear
Autorefresh
Entropy
Count
Time
40 41 42 43
2010-01-08 13:55:00.0 ; 40 ; 0.953 , 0.044721359549995794 , 0.403 , 0.867 , 0.044721359549995794 ,
--2010-01-08 13:55:00.0 ; 137.138.[redacted] ; 0.091 , 0.30166206257996714 , 1.0 , 0.167 , 0.38987177379235854 ,
--2010-01-08 13:55:00.0 ; 128.141.[redacted] ; 34.0 , 0.0 , 209.0 , 121.5 , 123.74368670764582 ,
--2010-01-08 13:55:00.0 ; 137.138.[redacted] ; 0.628 , 1.288021738946979 , 4.0 , 1.141 , 1.3583077707206126 ,
--2010-01-08 13:55:00.0 ; 137.138.[redacted] ; 1.141 , 1.1945710527214362 , 3.0 , 1.423 , 1.1962441222426132 ,
--2010-01-08 13:55:00.0 ; 137.138.[redacted] ; 2.0 , 1.0 , 3.0 , 2.25 , 0.957601169589929 ,
--2010-01-08 13:55:00.0 ; 128.141.[redacted] ; 3.0 , 0.0 , 3.0 , 3.0 , 0.0 ,

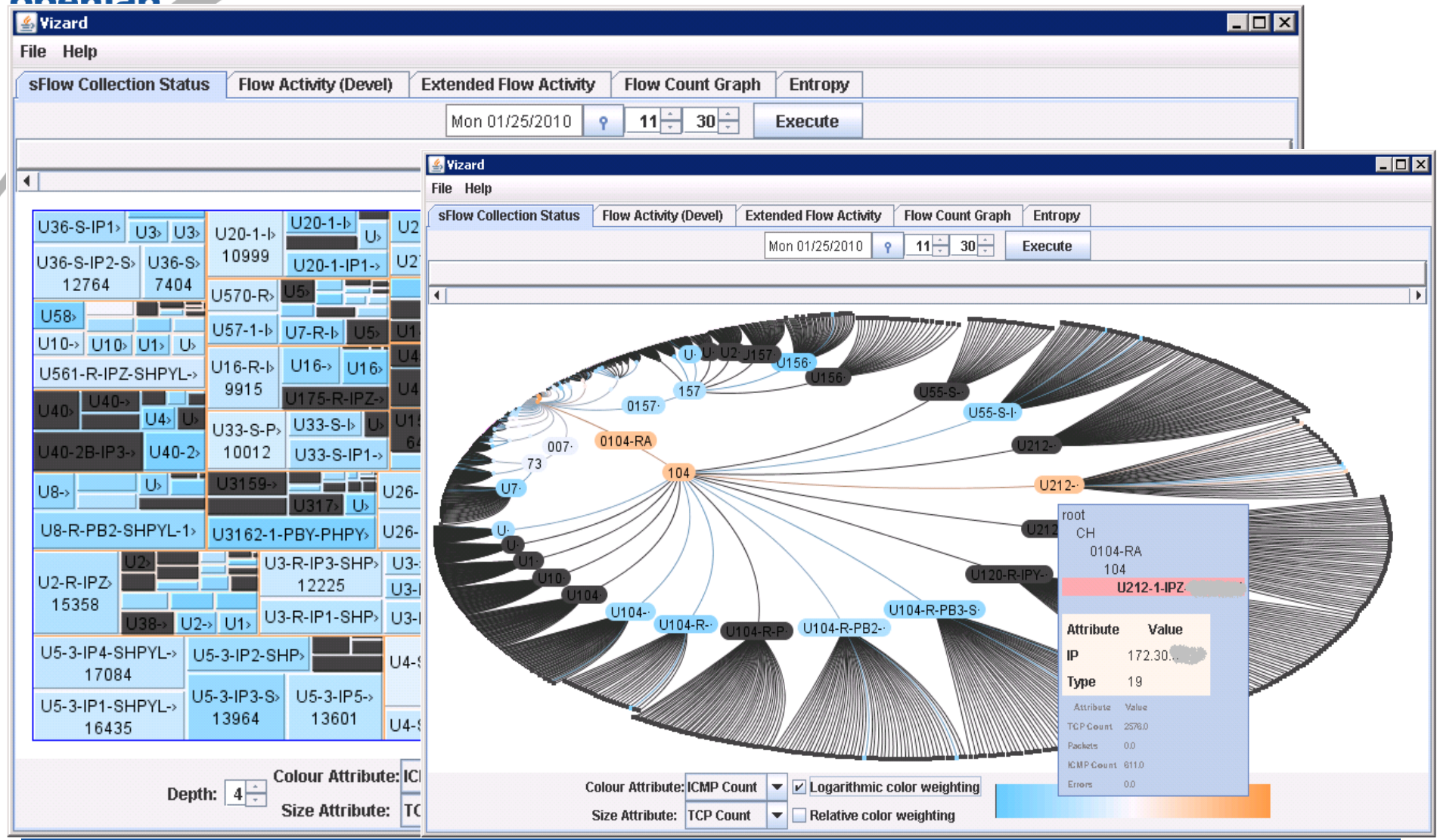
CINBAD network monitoring tools

CINBAD tools for network monitoring

- N-tier architecture:
  - back-end tools – collect, filter and aggregate into database
  - application server – exposes this data to clients
  - front-end clients – visualize the data
  - periodic jobs – compute statistics

- Available tools and users:
  - CINBAD CERN-wide tcpdump (Network Eng.)
  - sFlow data collection monitor (CINBAD)
  - **Host activity monitor** (Network Oper.)

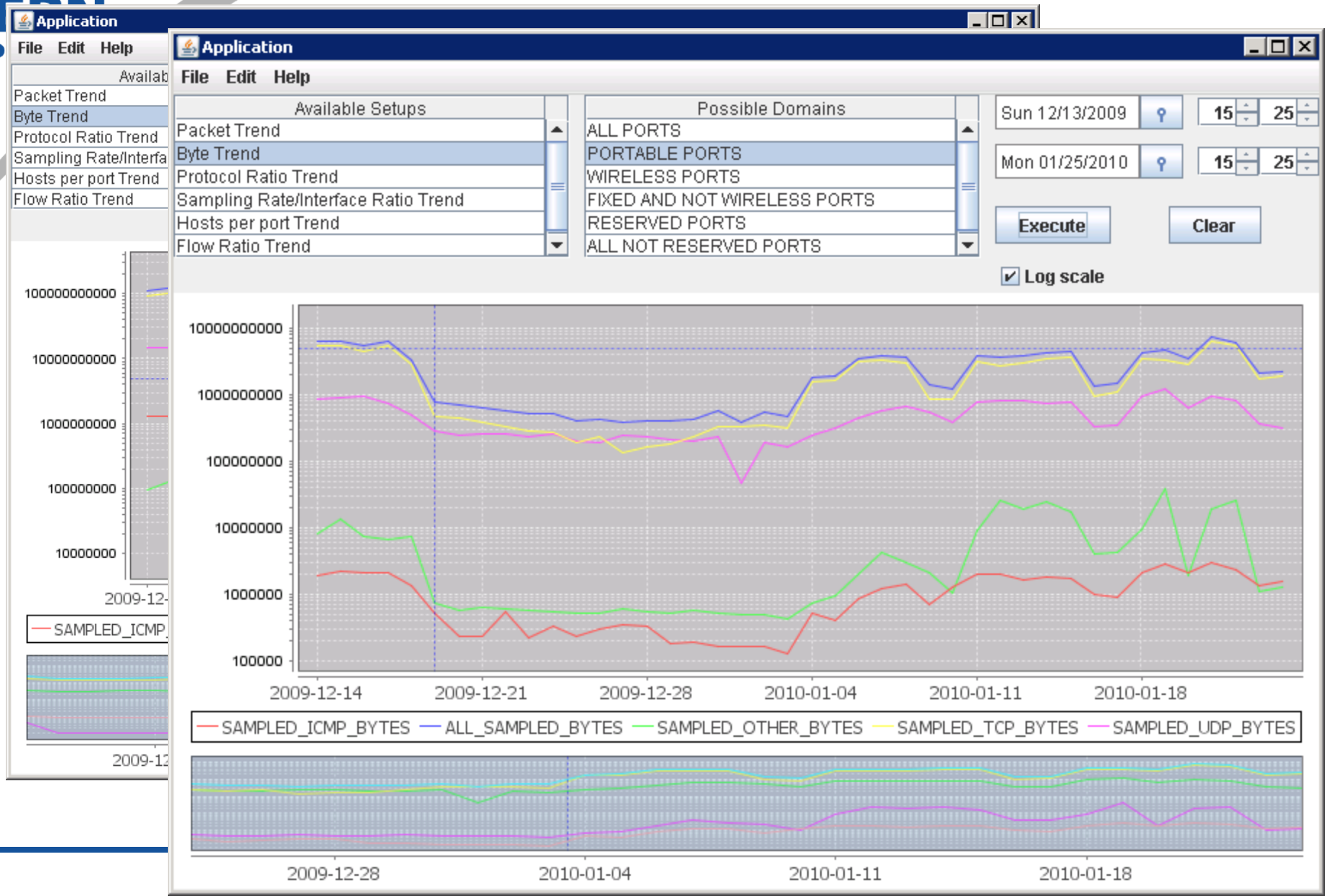
Video


Vizard
File Help
sFlow Collection Status
Flow Activity (Devel)
Extended Flow Activity
Flow Count Graph
Entropy
Mon 01/25/2010
11
30
Execute
U36-S-IP1
U36-S-IP2-S
12764
U36-S
7404
U20-1-I
10999
U20-1-IP1
U570-R
U57-1-I
U7-R-I
U16-R-I
9915
U16
U175-R-IPZ
U561-R-IPZ-SHPYL
U40-2B-IP3
U40-2
U33-S-P
10012
U33-S-I
U33-S-IP1
U3159
U317
U3162-1-PBY-PHPY
U8-R-PB2-SHPYL-1
U2-R-IPZ
15358
U3-R-IP3-SHP
12225
U3-R-IP1-SHP
U5-3-IP4-SHPYL
17084
U5-3-IP2-SHP
U5-3-IP1-SHPYL
16435
U5-3-IP3-S
13964
U5-3-IP5
13601
Depth: 4
Colour Attribute:
Size Attribute:
Vizard
File Help
sFlow Collection Status
Flow Activity (Devel)
Extended Flow Activity
Flow Count Graph
Entropy
Mon 01/25/2010
11
30
Execute
157
0157
0104-RA
104
007
73
U7
U156
U55-S
U55-S-I
U212
U120-R-IPY
U104
U104-R-PB3-S
U104-R-PB2
root
CH
0104-RA
104
U212-1-IPZ
Attribute Value
IP 172.30.
Type 19
Colour Attribute: ICMP Count
Logarithmic color weighting
Size Attribute: TCP Count
Relative color weighting

CINBAD Trends

- Help to understand the global behaviour of the network and users
  - e.g. #flows, traffic volume,…
- Support design of the future infrastructure
  - e.g. #active ports, average number of hosts per switch port,…

Video


Application
File Edit Help
Packet Trend
Byte Trend
Protocol Ratio Trend
Sampling Rate/Interfa
Hosts per port Trend
Flow Ratio Trend
100000000000
10000000000
1000000000
100000000
10000000
2009-12-
SAMPLED_ICMP
2009-12
Application
File Edit Help
Available Setups
Packet Trend
Byte Trend
Protocol Ratio Trend
Sampling Rate/Interface Ratio Trend
Hosts per port Trend
Flow Ratio Trend
Possible Domains
ALL PORTS
PORTABLE PORTS
WIRELESS PORTS
FIXED AND NOT WIRELESS PORTS
RESERVED PORTS
ALL NOT RESERVED PORTS
Sun 12/13/2009
Mon 01/25/2010
15
25
Execute
Clear
Log scale
10000000000
1000000000
100000000
10000000
1000000
100000
2009-12-14
2009-12-21
2009-12-28
2010-01-04
2010-01-11
2010-01-18
SAMPLED_ICMP_BYTES
ALL_SAMPLED_BYTES
SAMPLED_OTHER_BYTES
SAMPLED_TCP_BYTES
SAMPLED_UDP_BYTES
2009-12-28
2010-01-04
2010-01-11
2010-01-18

CINBAD Domain Specific Tools

- Inventory of HTTP and SSL services
  - passive approach: information retrieved from packets,
  - service IP address, port, operating system,
  - more than 2500 active services last week (80% SSL),
  - used by the CERN Security Team to cross-check data from their vulnerability scanners
- Wireless tools (proof of concept)
  - Detection of possible unregistered access points
  - Detection of areas with high IP roaming rate

Collaborations

Meetings and Discussions (I)

- HP Labs (Palo Alto):
  - They are attempting to use entropy for detecting anomalies in huge computer centers
  - There are some similarities in our approaches
  - We have exchanged information about our research and will meet in US soon
- Presentation about CINBAD to CTI (Le Centre des technologies de l'information)

Meetings and Discussions (II)

- Collaboration with Oracle openlab team
  - The newest Oracle databases support data compression
  - We have agreed to test the basic compression on our data
  - Initial results are surprising, more detailed ones are expected soon
- Initial discussion with Siemens Team about PLC security issues

Publications

- Internal report describing our data mining approaches
  - Confidential
  - Constitutes the basis for the final report to ProCurve
- Submitted an abstract for the internal HP conference “Tech Con '10”
  - Decision in February 2010
  - Publication will be a part of the final report concluding the project

Conclusions and plans

- CINBAD tools
  - Proved to be useful in resolving problems
  - Trend module could help in planning
  - Continuously searching for new ideas

- Visit the HP ProCurve in Roseville in March
  - Transfer our knowledge
  - Deliver code and algorithms
  - Meet HP Labs researchers