

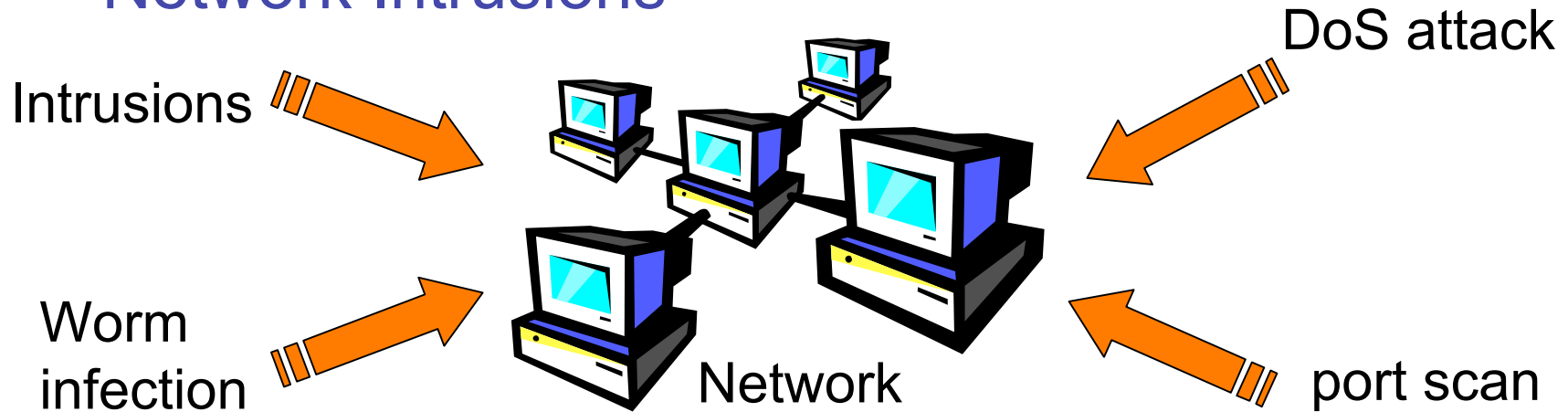
# ***VisFlowConnect-IP:*** An Animated Link Analysis Tool For Visualizing Netflows

**Xiaoxin Yin\*, William Yurcik, Adam Slagell**

*SIFT Research Group  
National Center for Supercomputing Applications (NCSA)  
University of Illinois at Urbana-Champaign*

# Motivations

- Network Intrusions



- Intrusion Detection Systems

- Misuse detection: find signatures of intrusions
- Anomaly detection: model normal behaviors

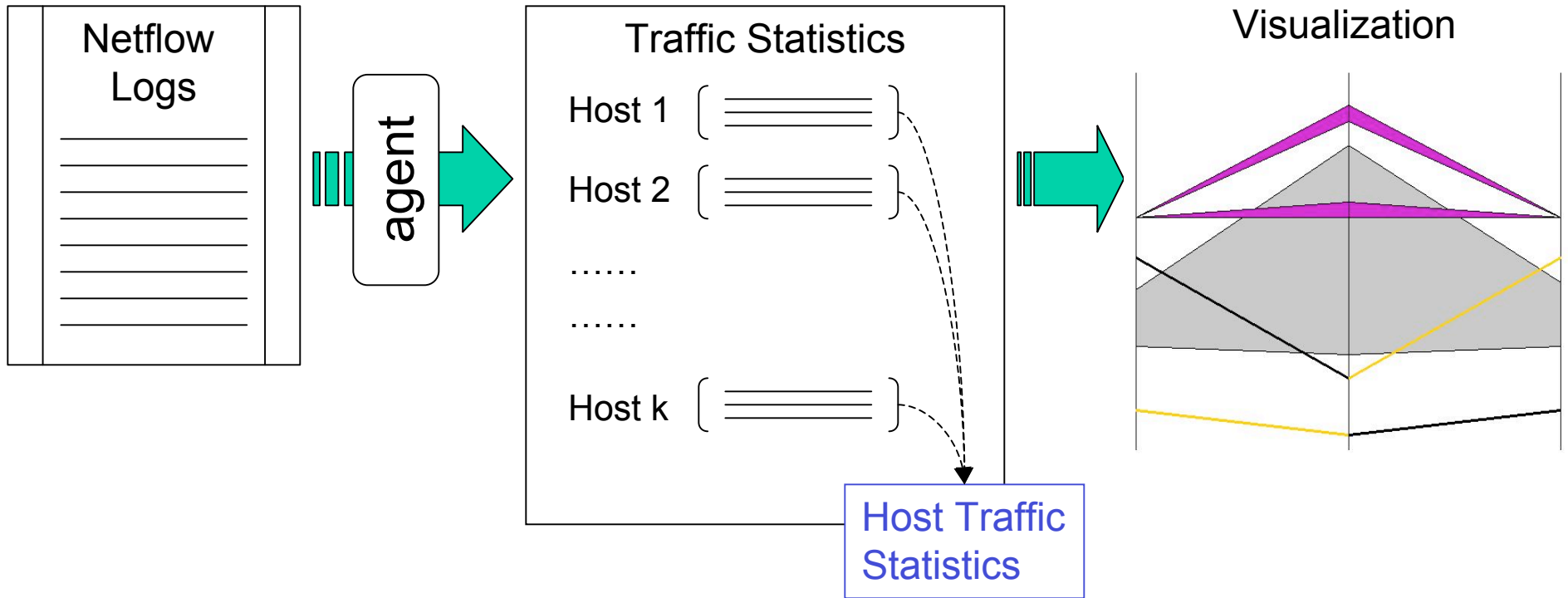
- Visualize network traffic

- So that intrusions are apparent to human

# Overview

- Visualizing network traffic as a graph
  - Hosts → nodes in graph
  - Traffic → flow in graph
  - other conceptual models are possible (i.e. NVisionIP)
- Visualizing by *animation*
  - Show network dynamics by animation
  - Visualize traffic within a user adjustable time window
- High scalability
  - Run continuously for long periods
  - Uses constant storage to process large data sets or high speed streaming data.

# VisFlowConnect System Design



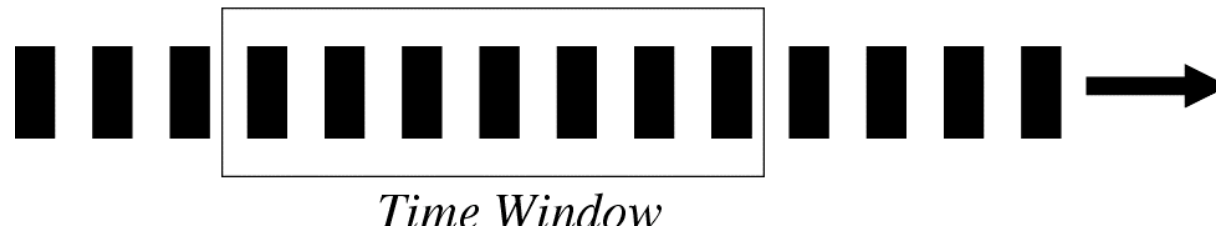
# Reading Netflow Logs

- An agent reads records from file or in real time
  - Send a record to VisFlowConnect when requested
- Reorder Netflow records with record buffer
  - Records are not strictly sorted by time stamps
  - Use a record buffer



# Time Window

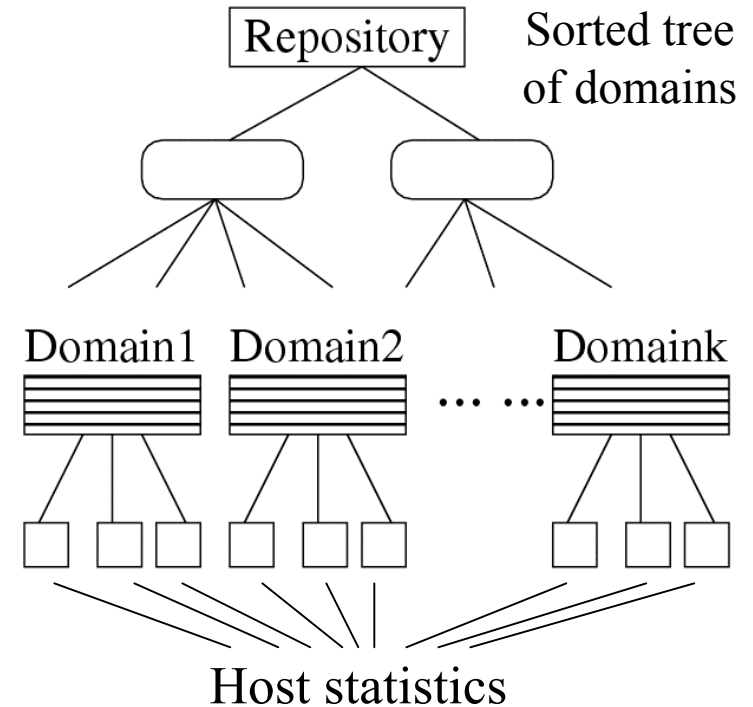
- User is usually interested in most recent traffic (e.g., in last minute or last hour)
- VisFlowConnect only visualizes traffic in a user adjustable time window



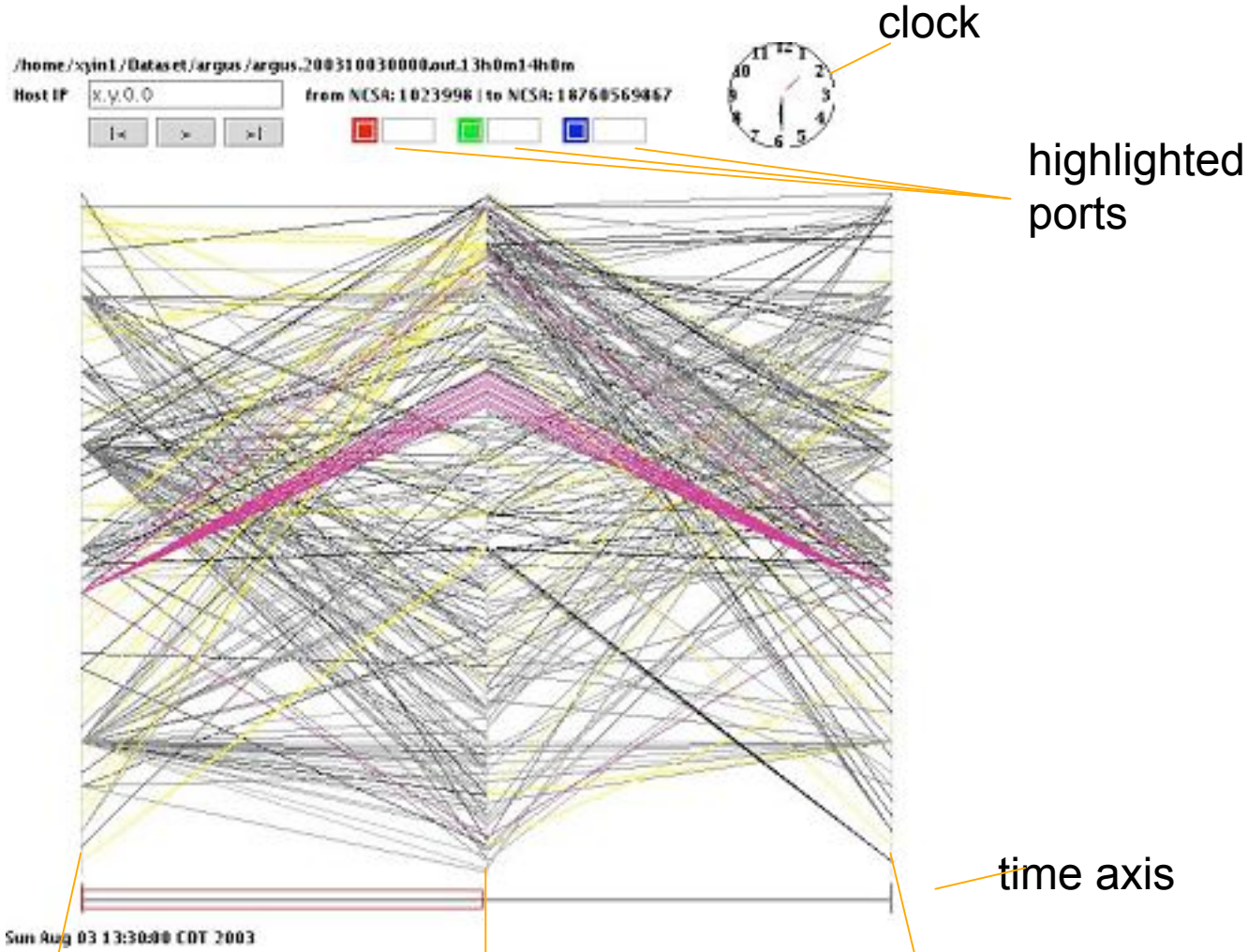
- Update traffic statistics when
  - A record comes into time window
  - A record goes out of time window

# Storing Traffic Statistics

- Store traffic statistics involving each domain by a sorted tree
  - Only necessary information for visualization is stored
  - Statistics for every domain or host can be updated efficiently



# VisFlowConnect External View



outside domains

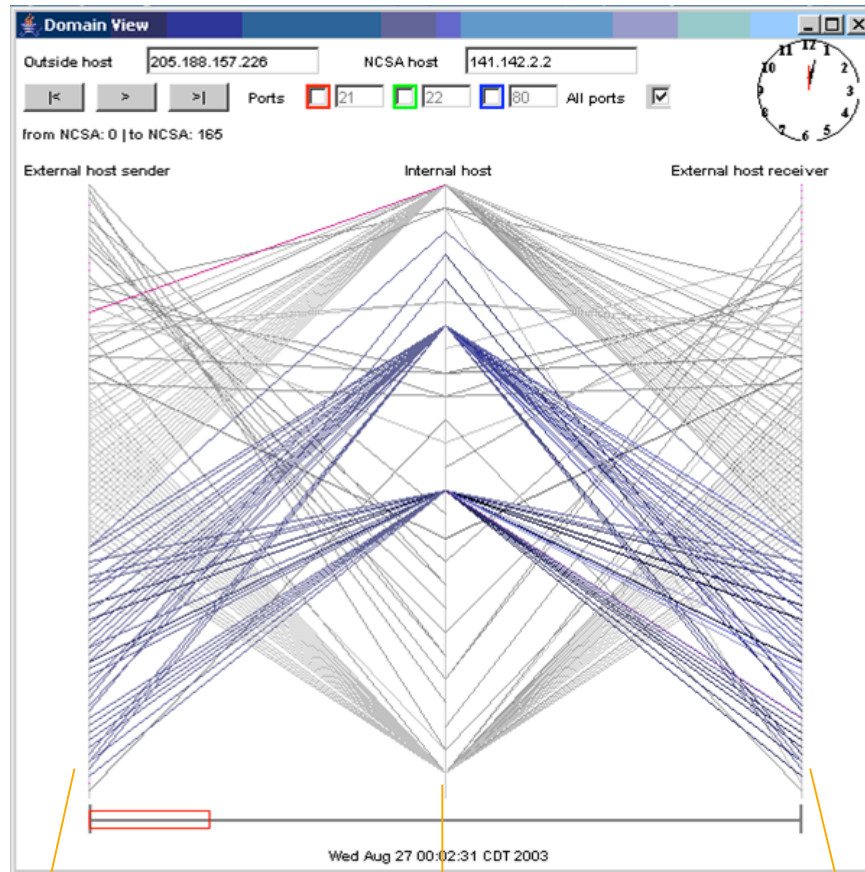
inside hosts

outside domains





# VisFlowConnect Domain View



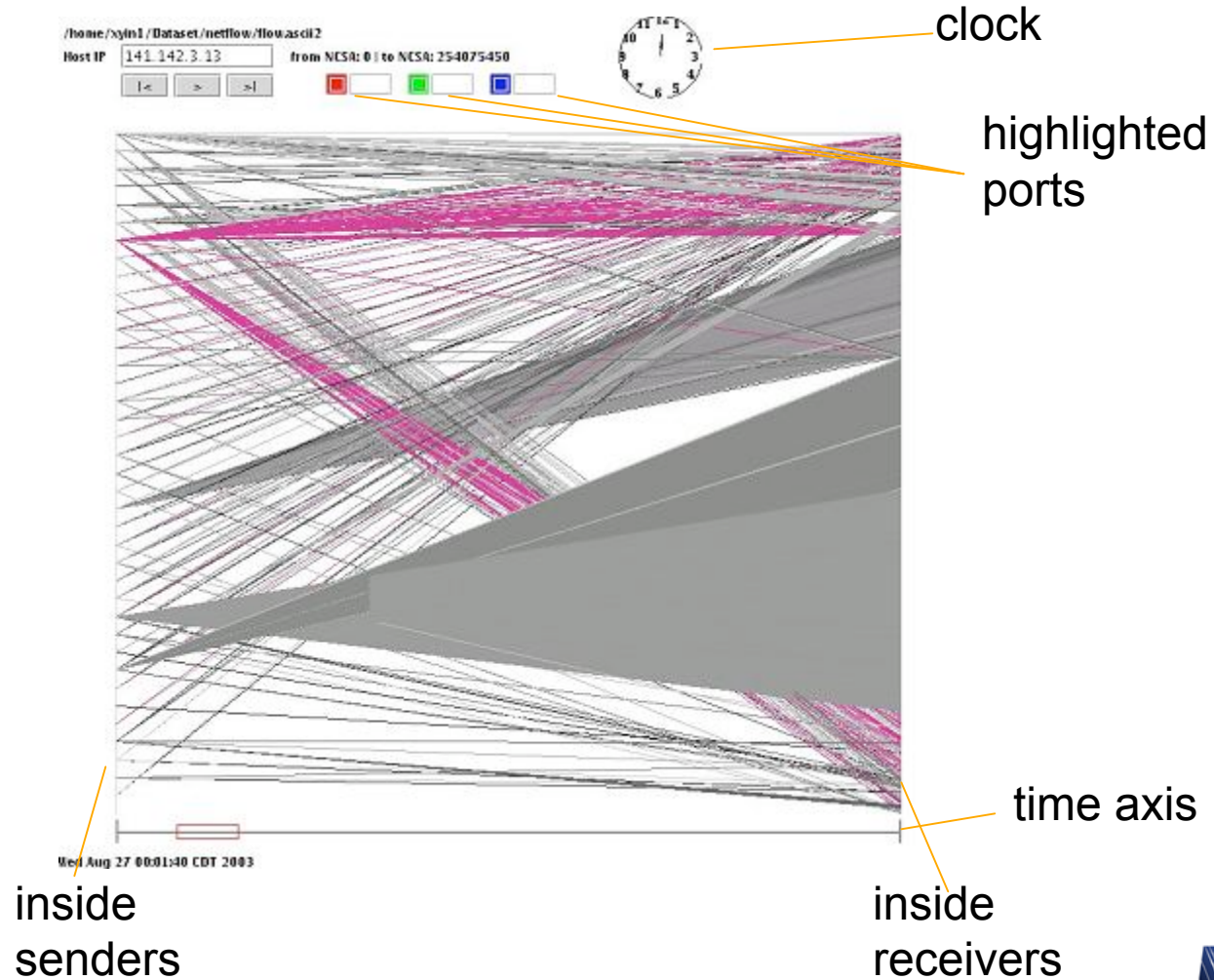
outside domains

inside hosts



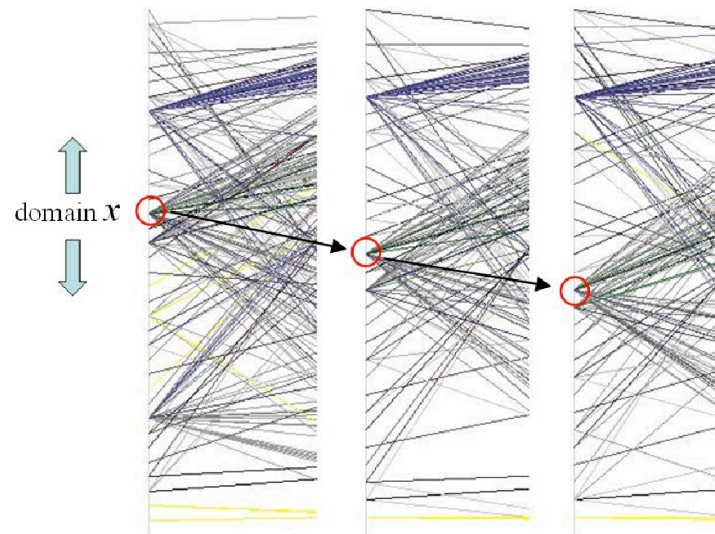
outside domains

# VisFlowConnect Internal View



# Creating Animation

- Visualizing traffic statistics with time
  - Update visualization after each time unit
- How to arrange domains/hosts?
  - Only hundreds of domains/hosts can be put on one axis
  - Domains/hosts may be added or removed with time
  - The position of each domain/host must be fairly stable
- Solution: sort domains/hosts by IP
  - Each domain/IP may move up or down

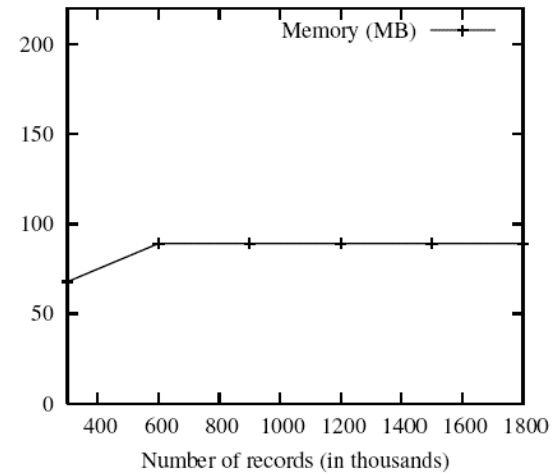
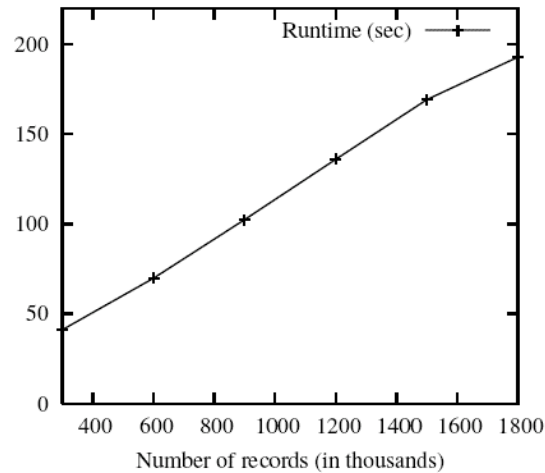


# Filtering Capability

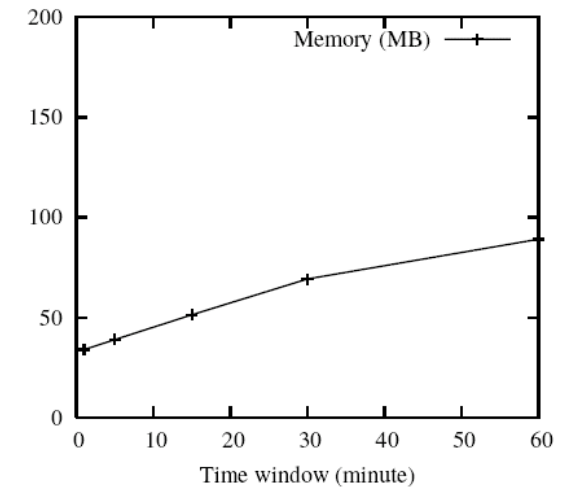
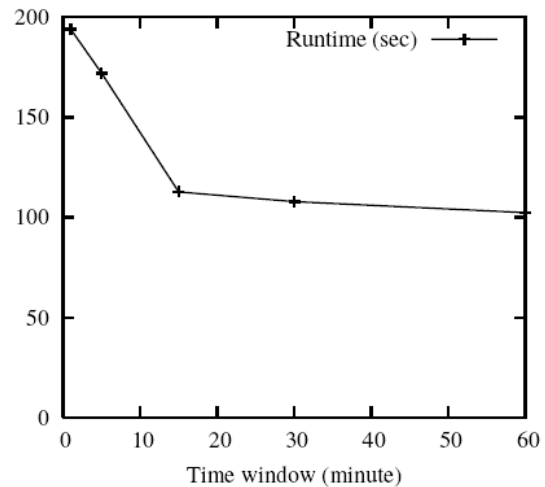
- Filter out regular traffic
  - E.g., DNS traffic, common HTTP traffic
- Work like a spam-mail filter
  - User specifies a list of filters:
    - + : (SrcIP=141.142.0.0–141.142.255.255), (SrcPort=1–1000)  
//keep all records from domain 141.142.x.x, from port 1 – 1000
    - : (SrcPort=80)
    - : (DstPort=80)  
//discard records of http traffic
  - Each record is passed through each filter
  - Last match is used to decide whether keep this record or not

# Scalability Experiments

Runtime and memory w.r.t. number of records



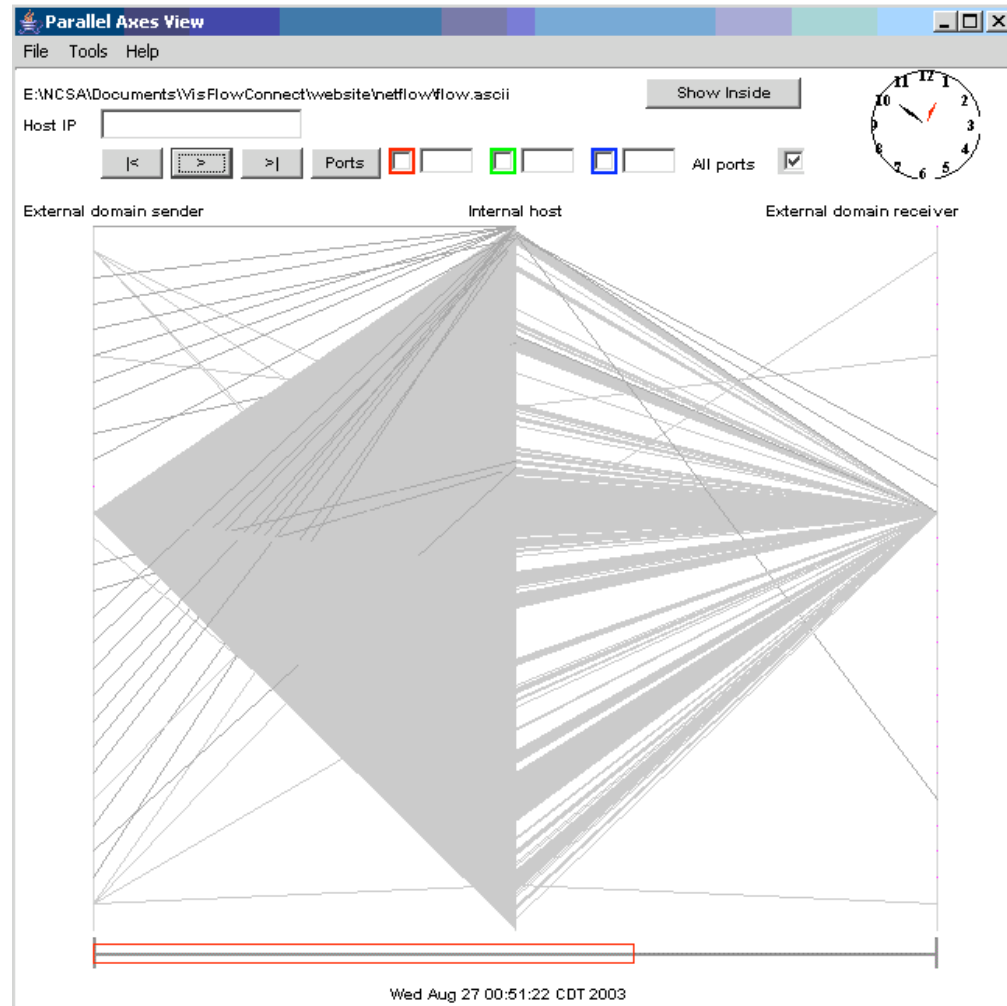
Runtime and memory w.r.t. size of time window





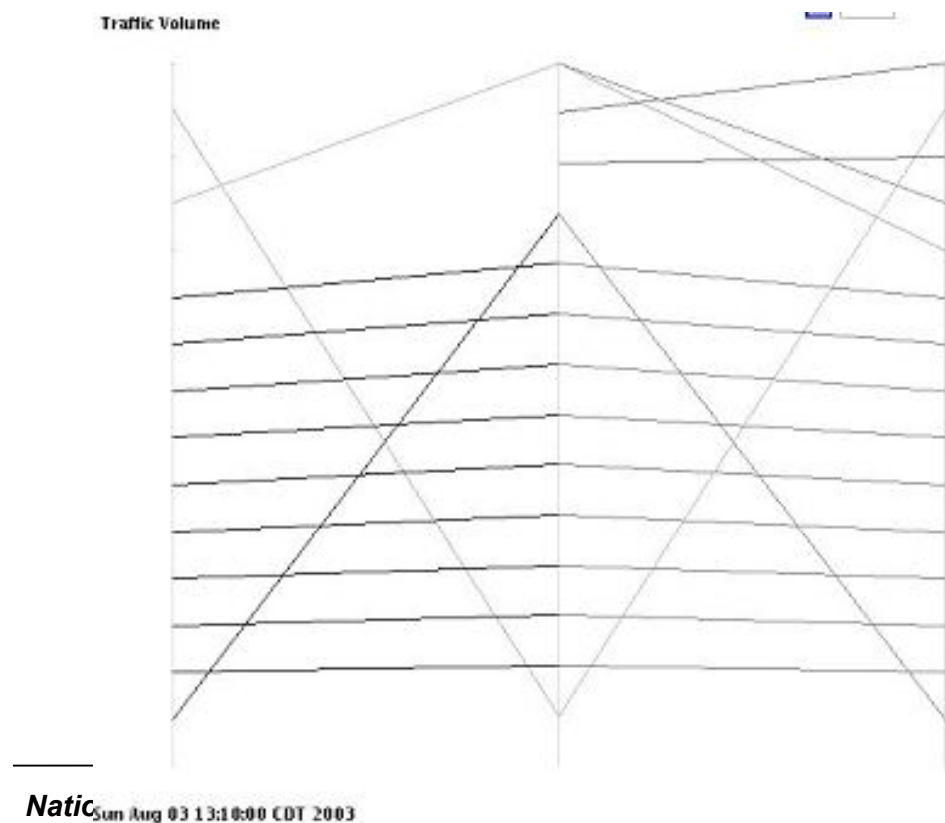
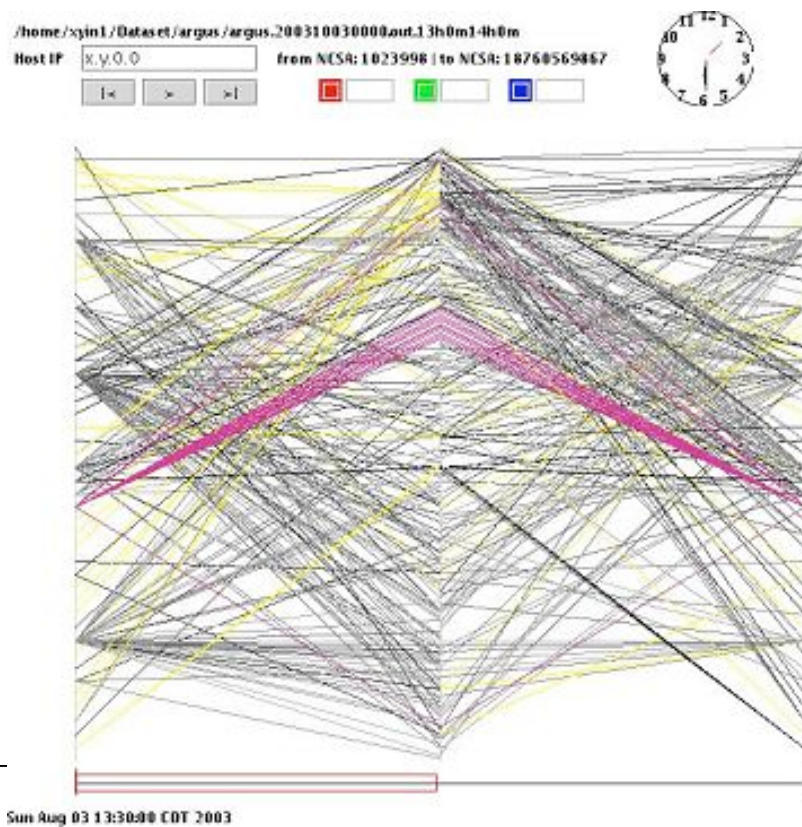
# Example 1: MS Blaster Virus

- MS Blaster virus causes machines to send out packets of size 92 to many machines



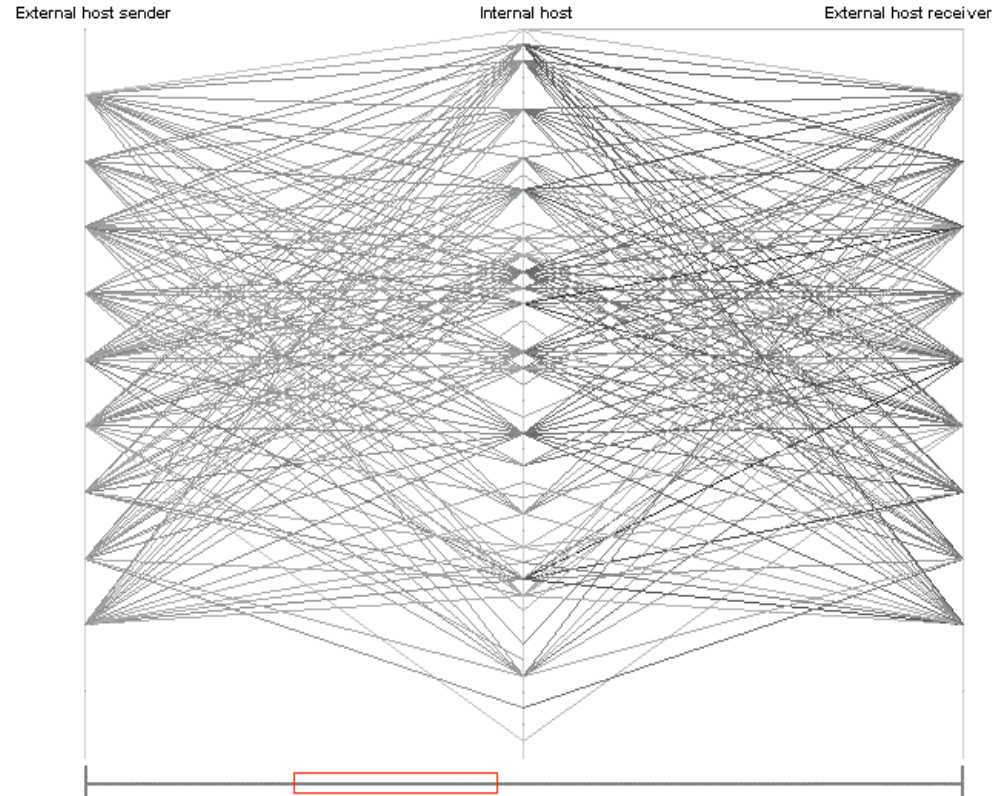
## Example 2: 1-to-1 Communication of Clusters

- We found there are two sets of hosts of continuous IPs have 1-to-1 communications with each other. Finally we found they are two clusters.



# Example 3: Web Crawlers

- We found 9 hosts in a domain connecting to many http servers in our network
  - Their IPs are from Google.com: Web crawling





## More Information

- VisFlowConnect is being ported to other specialized security domains
  - Storage security (two publications pending)
  - Cluster security
- Distribution Website
  - <http://security.ncsa.uiuc.edu/distribution/VisFlowConnectDownload.html>  
VisFlowConnect are downloadable there
- Publications of SIFT Group
  - <http://www.ncassr.org/projects/sift/papers/>



# Thank You!

**Xiaoxin Yin**

*<xyin1@uiuc.edu>*

*NCSA SIFT Group  
University of Illinois*