Security at Line Speed with NetFlows

William Yurcik

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

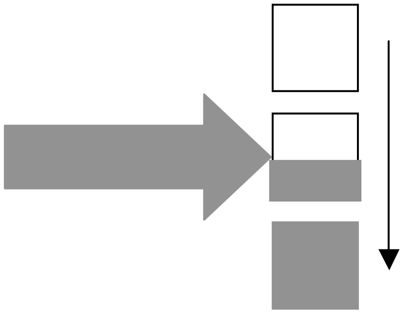
FloCon 2004

Level of Observation

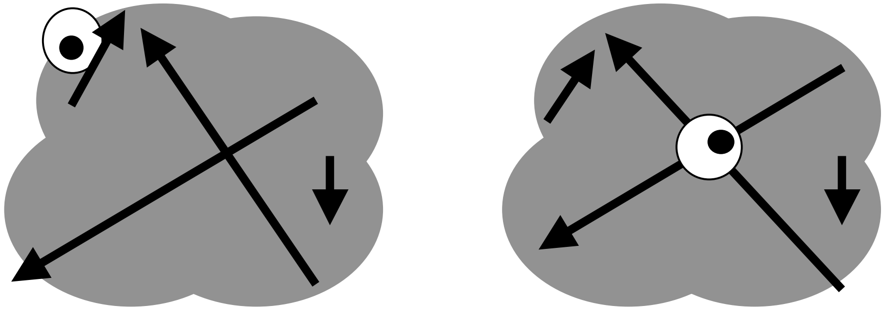
Data Source	Description	Advantage	Disadvantage
Packet	lowest level of granularity; all raw packets with all fields intact	most detailed data and statistics especially protocols; easiest to obtain	unscalable; protocol signaling needs to be decoded
NetFlows	IPs/ports/protocols/ Timestamps/data?	scalable for catching all traffic; multiple sources, uniform field formats	maybe no data field; context must be inferred
IDS	alerts of different formats	scalable; tunable	resource-intensive; misses; FPs
Load Levels	aggregate utilization levels that can be broken down to IP, protocol, port	high volume attacks (DOS, traffic); capacity planning; availability from routers & sniffers	details about SD pairs; no direction; low volume events obscured

NetFlows Instrumentation Issues

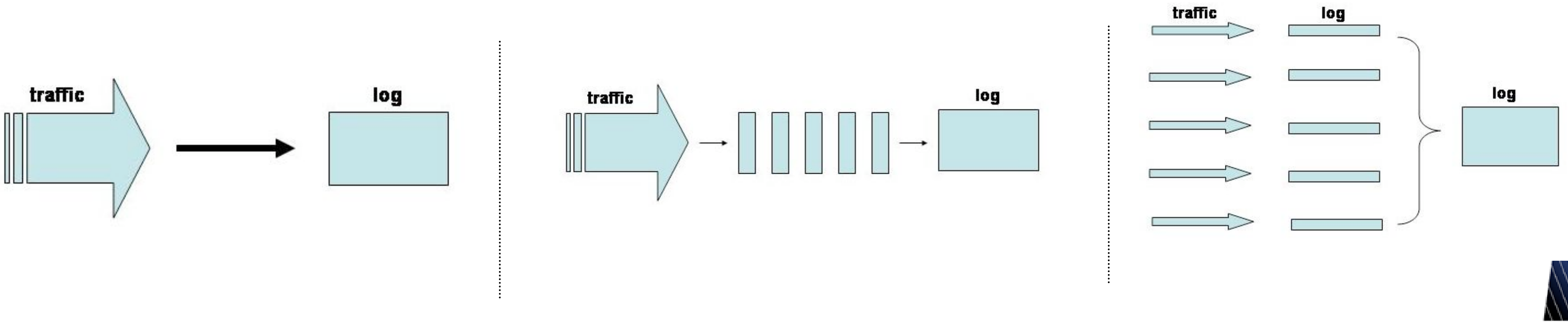
- Streaming Data



- Vantage Point



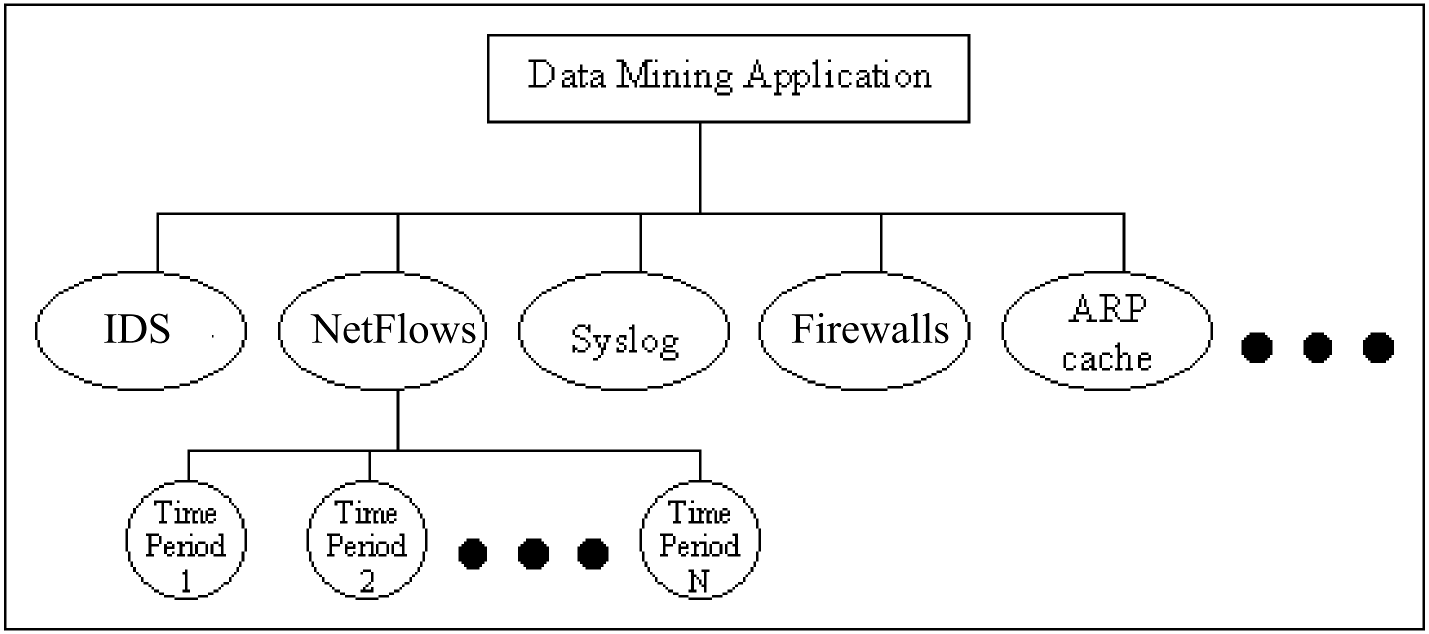
- High Line Rates



Flavors of NetFlows

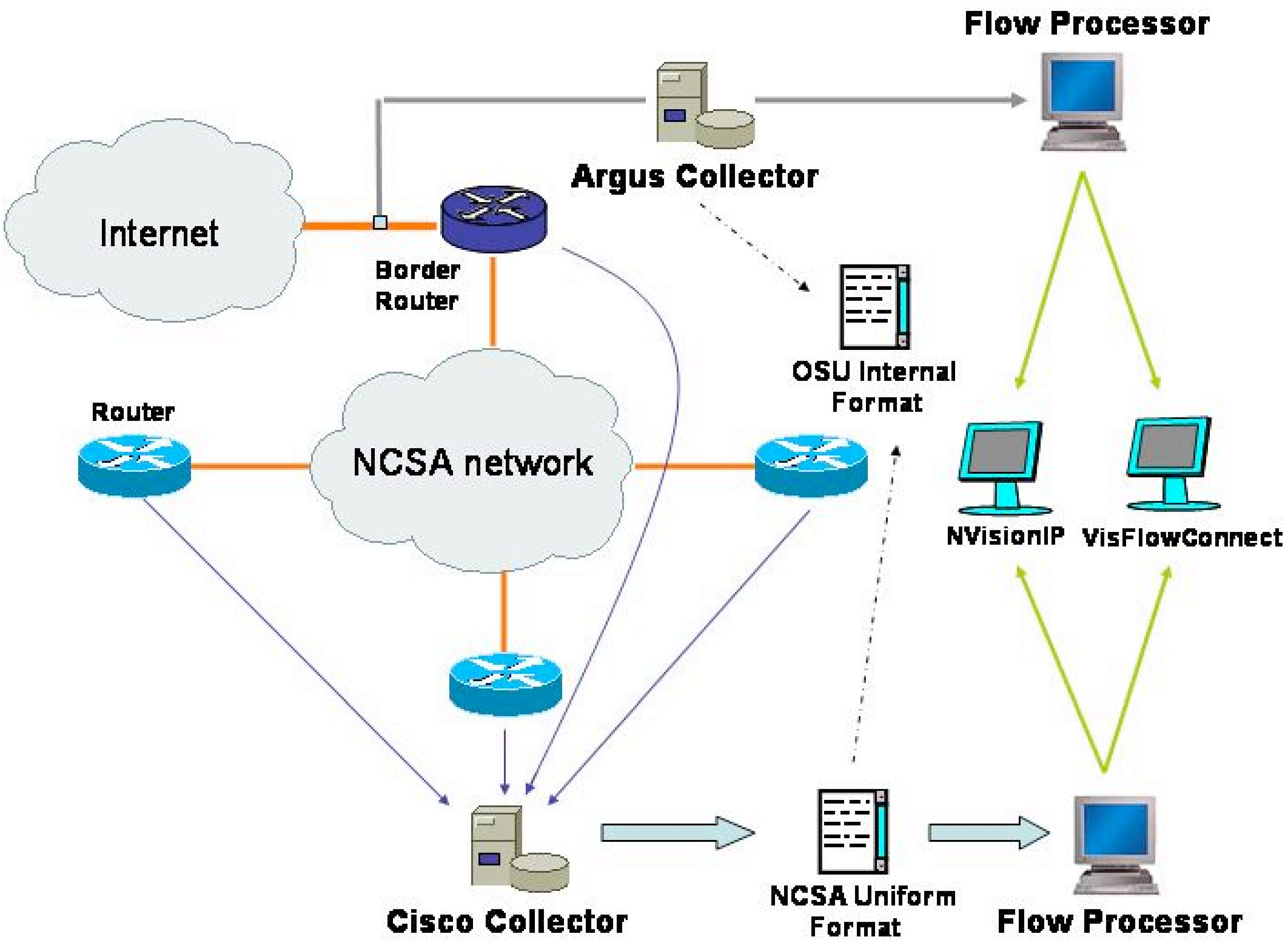
- **Router-Based (Cisco, Juniper, etc.)**
  - Cache timeout
  - Configuration
  - Sampling
- **Argus <*http://www.qosient.com/argus/*>**
  - Open Source
  - Platform Independent
  - Configuration (data field)
- **Home Grown NetFlows**
  - Many, for instance, Tom Daniels, Iowa State University …..

The Data Management Problem

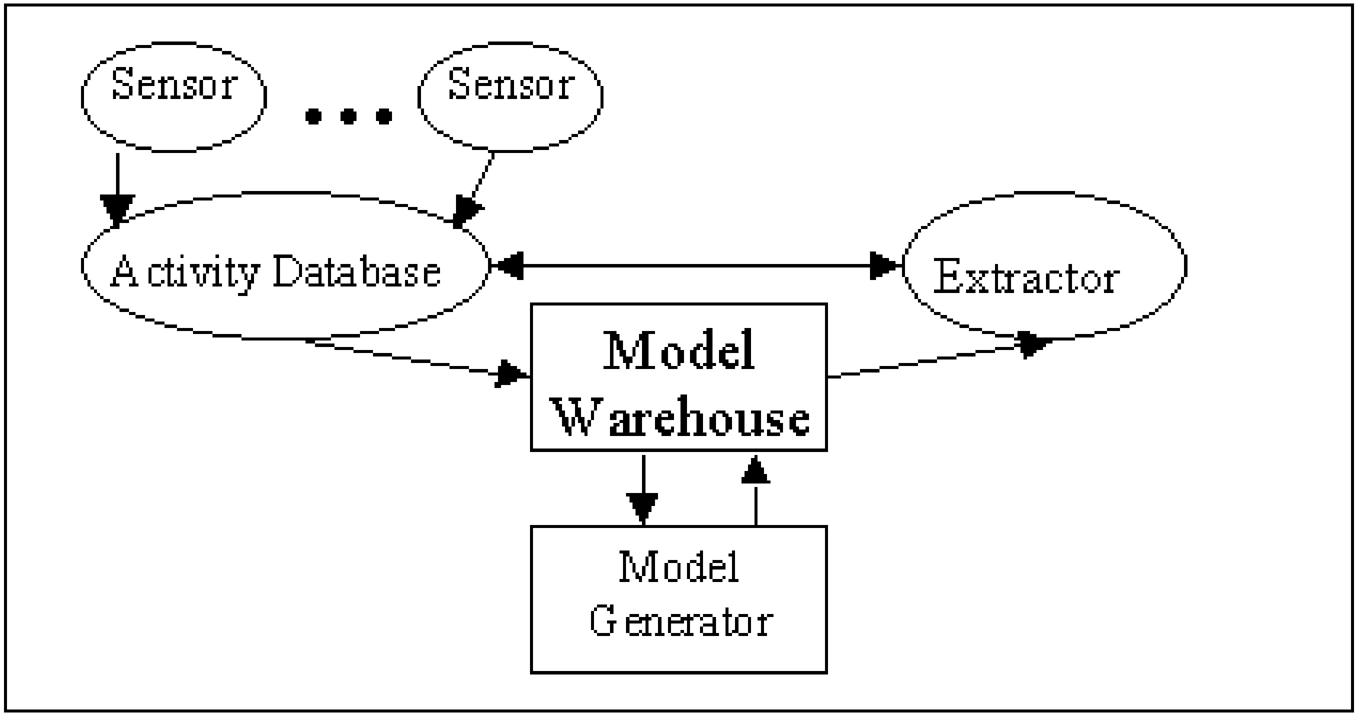


time dimension

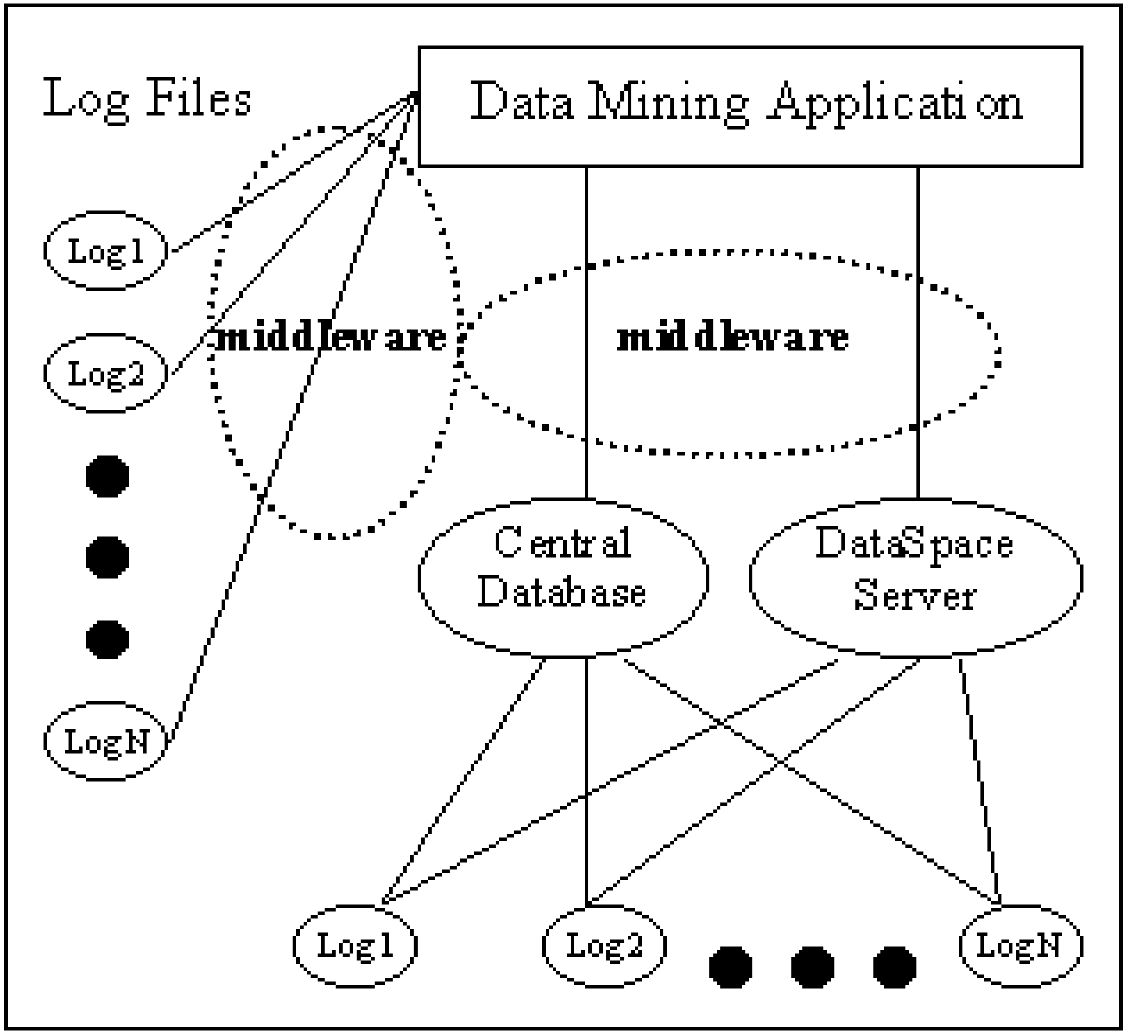
NCSA’s NetFlows Architecture



(1) Central Database Architecture



(2) Middleware Architecture


Log Files
Data Mining Application
Log1
Log2
LogN
middleware
middleware
Central Database
DataSpace Server
Log1
Log2
LogN