Panel
Aspects of high speed monitoring
Philippe Owezarski
LAAS-CNRS
Toulouse, France
owe@laas.fr
First words...

- Issue with high speed networks monitoring
- How to compute so much data in so little time?

- Here, the issues for a networking guy who is happy of having multi Gbps links, but does not know how to monitor and manage it...
On-line vs. Off-line monitoring

- Both require dedicated hardware for monitoring packets (as DAG cards)
  - On-line monitoring
    - Requires additional dedicated and expensive hardware for computing packets on the fly
  - Off-line monitoring
    - Once captured and stored, traffic traces can be analyzed with software tool
      - cheap and slow
    - Given the complexity, the analysis of a one hour trace can take several hours

- Is it economically acceptable for a wide deployment?
Importance of Off-line monitoring

- Keep a trace for late analysis
  - In case of a new, still unknown, worm, virus or attack $\rightarrow$ allows a late analysis of the worm or virus spread / attack strategy / etc.
  - Allows the creation of attack databases for defense system validation
  - Help the design of suited new defense mechanisms (ex. a profile based IDS)
Ex. Profile based IDS

Traffic profiles in IDS do not consider such variability

False positive rate is high

→ Impossible to fix reliable thresholds

A traffic model cannot be based only on mean and standard deviation

→ Using non Gaussian marginals / short & long range correlation is better
Consequences on filters

- Filters do not only count bytes, packets and flows
- Filters must integrate complex processing
- Sometimes they must also work on several minutes of time series

→ Not a good news for on-line monitoring of high speed networks
Approaches for on-line monitoring

**Sampling**
- Bad for detecting exploit attacks
- Good for flooding attacks

- Is sampling compatible with security enforcement techniques?
- Is sampling applicable at the edge as well as in the core of the network?
- Does it worth to store such sampled traces for late analysis?
Privacy issues

• We are forced by law to anonymize traces (IP addresses, payload of layer 4 and over)
  → Need of not too stupid anonymization procedures

→ We need laws which do not protect too much hackers/black hats!
The race to the grail in monitoring

➔ A global monitoring system
  • Real-time monitoring and analysis
  • Exchange of analysis results between probes to get a complete vision of the network

➔ Distributed security components collaborating