

MONAM 2006

Panel: Aspects of high-speed network  
monitoring

Hervé DEBAR

France Télécom Division R&D

September 28<sup>th</sup>, 2006



research & development



# Assumptions

- Network monitoring is a desirable goal
  - Boundaries
  - Attacks
- Trend towards more complex services will continue
  - P2P
  - Multicast and broadcast
- Bandwidth usage will continue to grow with technology

# Points for discussion

- Impact of high speed monitoring on detection ?
  - More data -> more alerts or logs ("operator bandwidth")
  - Link between accuracy and complexity of the detection mechanisms
- How much knowledge is required for filtering ?
  - Policy knowledge (i.e. organization's goals)
  - Usage knowledge (a.k.a. anomaly detection)
  - Attack knowledge (a.k.a. misuse detection)
  - Global knowledge (what is happening "outside")
  - And how do these impact high-speed monitoring ?
- Responses: going beyond blocking ?
  - QoS and traffic shaping
  - Traffic scrubbing
  - Quarantine

# Panelists

- Prof. Atta Badii, University of Reading
  - Director of the Intelligent Media Systems & Services Laboratory (IMSS)
  - Project manager of IST-027095-Fastmatch
  - Interests: FPGAs, alternative programming techniques
- Philippe Owezarski, LAAS-CNRS
  - Researcher at LAAS-CNRS
  - Interests: Traffic characterization and modeling, traffic anomalies, intrusion detection, honeypots
- Yacine Bouzida, Mitsubishi Electric
  - Postdoc and research engineer at Mitsubishi Electric Information Technology Center Europe
  - Interests: intrusion detection, VoIP security
- Prof. Dr. Georg Carle, University of Tuebingen
  - Chair for Computer Networks & Internet , University of Tuebingen
  - Representative of DIADEM FIREWALL
  - Interests: Internet, measurements, security

# Organization

- Panelists presentations (5 mn each)
- Discussion
- Summary
  - Questions
  - Points of interest
  - Future orientations