



# GÉANT2 Security Activity Update

Christoph Graf, SWITCH

Claudio Allocchio, GARR

TF-CSIRT, Prague, 28 January 2008



Connect. Communicate. Collaborate

# About GÉANT2

- EU-sponsored project running Sept. 2004 to February 2009 (extended by half a year)
- Divided into several classes of activities, one of them:
  - JRA: Joint Research Activity
  - Goal: preparing the grounds for new services in GÉANT2 (and successor)
- JRA2 is about “Security”:  
Aiming at improving the overall security within the GÉANT2 community
- 12 partners total, main partners:  
CESNET, DANTE, GARR, GRNET, SURFnet, SWITCH





Connect. Communicate. Collaborate

# Main activities (1/2)

- FlowMon
  - Netflow exporting appliance by INVEA-TECH (CESNET spin-off)
  - New improved version being procured now
  - Upgrade to 10Gbps interfaces available soon
  - Results expected early summer
- Netreflex
  - Netflow-based anomaly detection system by GUAVUS (Anukool Lakhina)
  - Results expected early summer



Connect. Communicate. Collaborate

## Main activities (2/2)

- Toolset Training Workshop
  - Training on the use of FlowMon and nfsen/nfdump
  - Intended to be offered on similar terms as TRANSITS
  - First workshop planned for mid-March with priority given to JRA2 members
  - 1 day workshop with an optional 1/2 day train-the-trainer module (required for trainees wishing to offer workshops based on the same material)
- Investigating where we're going with the Toolset
  - (just wait for Simona's questions)

# GN2 TWS - toolset questions (1/2)



Connect. Communicate. Collaborate

- The main questions about what we are going to do with that data are:
- Automatic alerting?
- Automatic opening of incidents?
- Automatic filling models of mail in case to send to constituency ?

# WORKING TOGETHER

## toolset questions (2/2)



Connect. Communicate. Collaborate

- The main of the main questions is:
- Are we going to work together to find ways to track “bad” traffic?
- Could it be a matter of privacy to talk each other about “monitoring techniques” (we won't talk each other about “defense techniques”)?
- Are we going to work together to write the automatic tools to react to bad traffic?
- Who is doing what?



Connect. Communicate. Collaborate

# Continuing activities

- Security Handling improvement
  - Helping GN2 member NRENs to reach minimal required daily security handling
  - Improving procedures by using toolset and other new tools
- Relationship with TF-CSIRT
  - Security experts consultancy to other GN2 activities
- Relationship with non GN2 members
  - DICE (Dante, Internet2, Canarie, Esnet)
  - APAN (Asia Pacific Academic Networks)
  - All the other bodies dealing with security