GÉANT2 Security Activity Update

Christoph Graf, SWITCH
Claudio Allocchio, GARR
TF-CSIRT, Vienna, 26 September 2008
About GÉANT2

- EU-sponsored project running Sept. 2004 to March 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
Activities (1/3)

• FlowMon
  – Netflow exporting appliance by INVEA-TECH (CESNET spin-off): http://www.invea-tech.com/
  – New improved 1Gbps version shipped to project participants (Upgrade to 10Gbps interfaces ongoing)
  – Report on test results due October 2008

• Advanced Anomaly Detection
  – Several Nfsen-based plugin trials
  – Netflow-based anomaly detection system by GUAVUS (Anukool Lakhina)
  – Report on test results due November 2008
Activities (2/3)

- Toolset Training Workshop
  - Training on the use of FlowMon and nfsen/nfdump
    - 1 day workshop
    - Optional 1/2 day train-the-trainer module
  - Second workshop planned for 2-4 February 2009
    - Taking place at SWITCH in Zurich, Switzerland
    - 1 day workshop
    - Optional 1 day optional train-the-trainer module
    - 1st call for NREN participants only
Activities (3/3)

• Policy and support activities
  – Helping GN2 member NRENs to establish CERT function
  – Site visits to Bulgarian and Romanian NRENs in July and August resulted in concrete plans for establishing CERTs for BREN and RoEduNet

• Relationship with TF-CSIRT
  – Security experts consultancy to other GN2 activities (currently no requests pending)
The Crystal Ball

• GN3 proposal submitted on September 11th
• A stress in moving services and activities toward users
  – Users are victims and sources of security problems
• A research activity in security (integrating existing tools and correlating results)
• A service activity in security (federated CSIRTs activity, tools to exchange information,…)
• A global Security Coordination service (make all components of GN3 activities security aware and security proof)
• … stay tuned.