GÉANT2 Security Activity Update

Christoph Graf, SWITCH
Claudio Allocchio, GARR
TF-CSIRT, Riga, 19 January 2009
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 and 10Gbps tested by project participants
  – Report on test results in review, expected Feb 2009

• Advanced Anomaly Detection
  – Several Nfsen-based plugin trials
  – Netflow-based anomaly detection system by GUAVUS (Anukool Lakhina)
  – Report on test results in review, expected Feb 2009
Activities (2/3)

• Toolset Training Workshop
  – Training on the use of FlowMon and nfsen/nfdump
    • 1 day workshop plus optional 1/2 day train-the-trainer module
  – Second workshop will be held 2-4 February 2009
    • Taking place at SWITCH in Zurich, Switzerland
    • Optional train-the-trainer module extended to 1 day
    • Registration was open to non-NREN participants
    • 11 people registered (9 NREN)
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
  – RoEduNet-CERT TI listed since October 2008!

• Relationship with TF-CSIRT
  – Security experts consultancy to other GN2 activities (currently no requests pending)
GÉANT3: The Crystal Ball

• GN3 proposal submitted on September 11th 2008, negotiations still ongoing…
• Security will have an important role throughout the project and activities (research and operational)
• “Security consideration audit” will likely happen for all GN3 activities
• Claudio Allocchio planned to act as Security Coordinator within the GN3 Project Office
• … stay tuned.