



GÉANT2 Security Activity Update

Christoph Graf, SWITCH

TF-CSIRT, Oslo, 14 May 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): <http://www.invea-tech.com/>
 - New improved version being shipped now to project participants (1Gbps version)
 - Upgrade to 10Gbps interfaces later
 - First results expected early summer 2008
- Netreflex
 - Netflow-based anomaly detection system by GUAVUS (Anukool Lakhina)
 - Results expected early summer



Connect. Communicate. Collaborate

Main activities (2/2)

- First Toolset Training Workshop delivered 18-19 March '08
 - http://www.terena.org/news/fullstory.php?news_id=2246
 - Training on the use of FlowMon and nfsen/nfdump:
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)
 - Very positive feedback received from participants!
 - Intended to be offered on similar terms as TRANSITS, but currently restricted to NREN staff
 - Second workshop planned for late 2008
 - Is there interest beyond the NREN community?



Connect. Communicate. Collaborate

Continuing activities

- Policy and support activities
 - Helping GN2 member NRENs to establish CERT function
 - Pushing towards making CERT function a mandatory prerequisite for GÉANTx partners
- Relationship with TF-CSIRT
 - Security experts consultancy to other GN2 activities (currently no requests pending)