GÉANT2 Security
(aka JRA2)

Christoph Graf, SWITCH
TF-CSIRT, Espoo
21 September 2006
Introduction

• GÉANT2: EU-sponsored project running Sept. 2004 to August 2008
• 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
Introduction

JRA2 consists of the following Work Items:

- WI-0: Management (SWITCH)
- WI-1: Securing GÉANT2 network elements and services (DANTE)
- WI-2: Building of security services (SURFnet)
- WI-3: Designing and establishing an infrastructure for co-ordinated security incident handling (GARR)
- WI-4: Relationship with TF-CSIRT (SWITCH)
- WI-5: Establishment of advisory panel (SWITCH)
JRA2 to date

- Security Policy for GÉANT2 (not publicly available)
- “The Toolset” (FlowMon, nfsen): requirement doc released, focussing now on advanced anomaly detection
- Co-ordination infrastructure: pilot report with recommendations released. Will be used to as a “GN2 Security Service Spec”.
- Formalised “security advice” from TF-CSIRT to GÉANT2: first case concluded and available as deliverable
- Advisory panel report update released
Security-Level of GÉANT2 partners

Leading edge team

Typical JRA2 participants

“old” focus

+ “new” focus

GÉANT2 minimum security level

Connect. Communicate. Collaborate

No CERT

security capabilities

time
JRA2 outlook (Y3 of GÉANT2)

- Focus on implementation and advanced services
- Service implementation: (relevant for all GÉANT2 partners)
  - set minimum standards for all GÉANT2 partners
  - Help partners to reach them
  - Make use of existing initiatives wherever possible
- Advanced services: (relevant for leading edge partners)
  - Advanced anomaly detection on the GÉANT2 network
  - Further developing the flow probe
Next steps

• JRA2 meeting tomorrow
• The GN2 Security Service deliverable due soon:
  – Will define “how much security” is required for GÉANT2
• Drafting the roadmap for all partners to live up to those recommendations/requirements
  – All GÉANT2 partners should be up to standard within the lifetime of GÉANT2 (August 2008), or earlier
  – Coloured maps help! Criteria: Memberships in TF-CSIRT+FIRST, level of listing in TI, maybe also some peer assessment value?