TF-CSIRT relation with GN2

Christoph Graf
<christoph.graf@switch.ch>
About GN2

Sixth Framework Project:
- Title: Multi-Gigabit European Academic Network
- Project acronym: GN2, it is spelt “GN2” but often pronounced “GÉANT2”
- Successor of project GN1, which produced the GÉANT network

Project partners:
- DANTE, co-ordinating partner
- Consortium of NRENs (29)
- TERENA

Project structure, work packages
- 7 Network activities
- 4 Service activities
- 5 Joint research activities

Timelines
- Project start: September 2004
- Duration: 4 years
- Reporting period: 1 year
- Detailed planning to date: first 18months, updated yearly
Summer 2003: First ideas outlined
1 Feb 2004: proposal (second) deadline
19 Mar 2004: formal negotiations
1 Sep 2004: project start (day 0)
31 Aug 2008: project end (day 1,461)
30 Sep 2004: end of GÉANT (1) project
Context of JRA2

GN2 (in terms of cost)
– Total projected cost: about 180M€
– Co-financing request: 93M€

GN2 (in terms of manpower investment)
– Network Activities 25%
– Service Activities 27%
– Joint Research Activities 48% = 100%
  » JRA1: Measurement & Mgmt 25%
  » JRA2: Security 25%
  » JRA3: New Services Development 25%
  » JRA4: Technology & Service Testing 8%
  » JRA5: Ubiquity and Roaming Access 17%
JRA2 work item overview

WI1: Securing GN2 network elements and services
  – recommendations and policies for GN2 & NRENs
  – implementation on backbone and access links

WI2: Building of security services
  – Introducing “The Toolset”©
  – deployment of eCSIRT.net results

WI3: Designing and establishing an infrastructure for co-ordinated security incident handling
  – Making use of “The Toolset”© and provide operational feedback to WP2
  – Several partners to trial each new service

WI4: Relationship with TF-CSIRT
  – Acknowledge the overlap in membership and interests
  – Ad-hoc groups of TF-CSIRT experts for advice to GN2

WI5: Establishment of advisory panel
  – Clearly defined role of TF-CSIRT
WI4: Relationship with TF-CSIRT (1)

Motivation

– In terms of membership and areas of interest: GN2/JRA2 subset of TF-CSIRT
– The broader view of TF-CSIRT could be useful to GN2/JRA2

Contents of work item “Relationship with TF-CSIRT”

– Communication channels for information exchange between both bodies
– JRA2 progress reports to be presented to TF-CSIRT
– Ad-hoc groups of TF-CSIRT experts for specific advice to GN2/JRA2
– Side-by-side or joint TF-CSIRT/JRA2 meetings

Formal work item output (within first 18 months of GN2)

– Month 12, Deliverable: Report on ad-hoc advisory groups creation and activities
– Month 18, Deliverable: Updated report

Who

– Lead (co-funded): SWITCH
– Participation (co-funded): SURFnet
– Implementation (unfunded): Volunteering TF-CSIRT members
WI4: Relationship with TF-CSIRT (2)

Communication channels
- All JRA2 members are expected to join TF-CSIRT; No problems expected
- Use the TF-CSIRT list for JRA2 activities, like any other TF-CSIRT activity
- Separate JRA2 mailing list for things under non-disclosure (if needed at all), or if TF-CSIRT is getting annoyed or monopolised

JRA2 progress reports at TF-CSIRT
- Looking rather unproblematic

Ad-hoc groups of TF-CSIRT experts
- Fine, if TF-CSIRT finds volunteers
- Tough luck for JRA2, if TF-CSIRT fails :-(

Side-by-side or joint meetings
- Strong feeling for joint meetings
- Separate sessions for stuff under non-disclosure or pure GN2/JRA2 internas
- Separate sessions, if TF-CSIRT feels monopolised or bored

>>> The ToR of TF-CSIRT should
- Mention collaboration with GN2/JRA2
- Acknowledge the areas of overlap
- Specifically mention the ad-hoc groups of experts
Motivation
– The broader view of TF-CSIRT could be useful to GN2/JRA2

Tasks of advisory panel
– Comments on the work carried out by JRA2
– Overview of trends and evolution of network security and incident handling
– Recommendations for work in subsequent years of JRA2

Some specified details
– Advisory panel recruited from TF-CSIRT (10 members)
– Panel meetings adjacent to TF-CSIRT

Formal work item output
– Month 12, Deliverable: Report on activities and recommendations of advisory panel (updated yearly)

Who
– Lead: SWITCH
– Participation (co-funded): JRA2 activity leader
– Implementation (unfunded): volunteers from within TF-CSIRT
Role of TF-CSIRT

- Help in finding panel members
- Fine, if TF-CSIRT finds volunteers
- Tough luck for JRA2, if TF-CSIRT fails :-(

>>> The ToR of TF-CSIRT should

- Additionally mention that it helps to provide a panel to GN2/JRA2