Incident Handling

e-IRG WorkShop. Open on e-Infrastructures

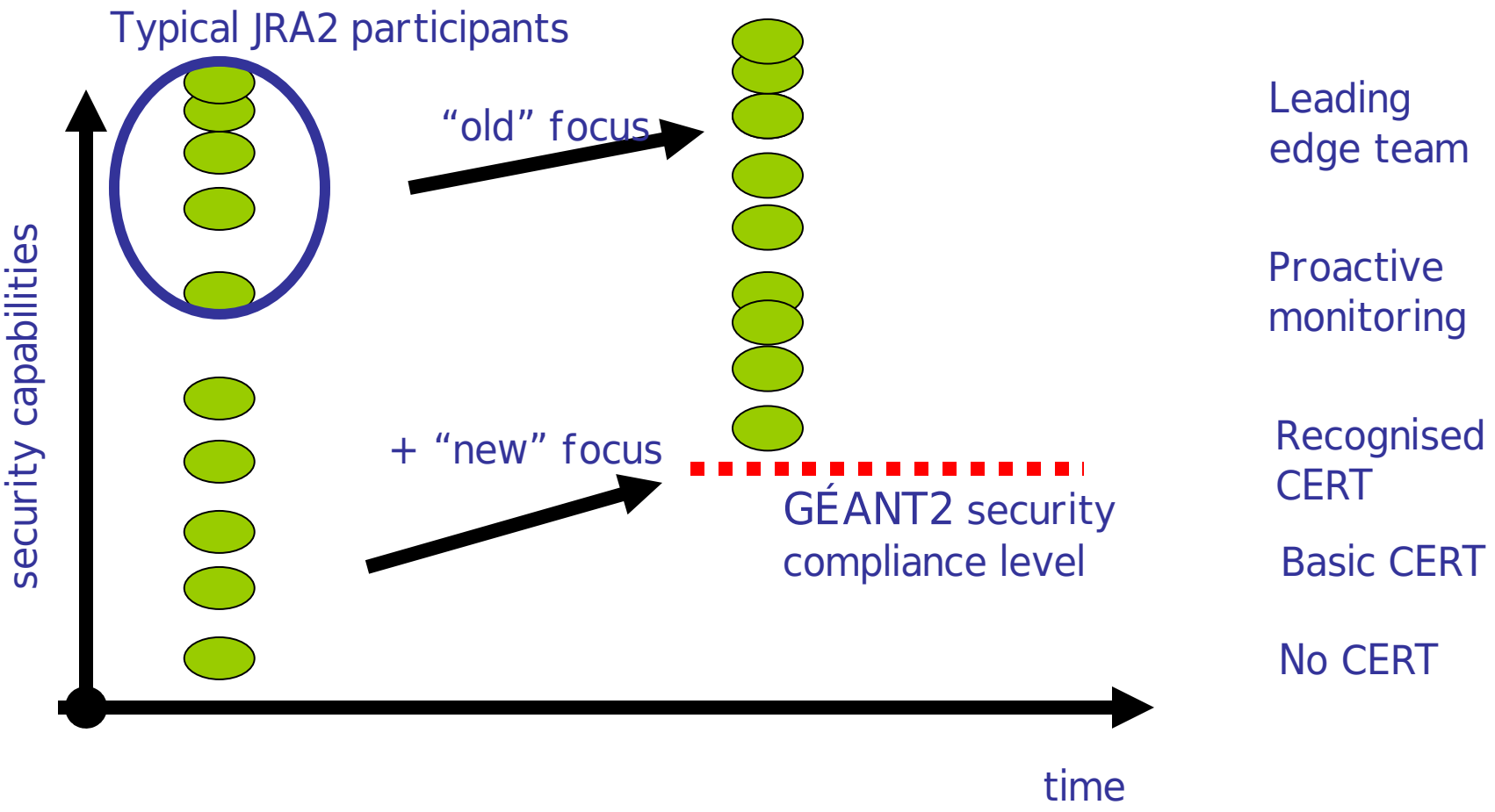
Helsinki, 5th October 2006

Carlos Fuentes <carlos.fuentes@rediris.es>

Current Status

- Most NRENs are running a CSIRT
- Excellent coordination in different levels
  - TF-CSIRT (TERENA Task Force). European Level http://www.terena.nl/activities/tf-csirt/
  - FIRST. Global level http://www.first.org/
    - All kind of CSIRT
      - NRENs
      - GovCERT
      - ISP
      - …
  - European Cooperation of Abuse fighting Teams (E-COAT) http://www.e-coat.org
  - TRANSITS
    - Training CSIRT staff
    - TERENA - http://www.ist-transits.org/
    - FIRST - http://www.first.org/transits/
- JRA2 (Activity of GEANT2 project)
  - Help to establish CSIRTs
  - Geant2 scope

What we are planning to do



GRID Incident Handling

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- New player in the game zone: **GRID**
  - Why?
    - A GRID is a super-institution running over several institutions
    - Require major coordination & a deeper analysis
      - A compromised machine affects more users & institutions
    - Ownership
      - Who owns the grid, or assumes ownership?
      - What are the assets and their criticality?
      - What level of security is needed?
      - To what risks are those assets exposed to?
      - To whom are responsibilities assigned to?

RedIRIS

GRID Incident Handling

- Responsibility
  - Who is responsible for the operation of the grid?
    - Includes knowing the customers and how to reach them
    - Includes assessing and reacting to incident notifications
  - Who is responsible for the software running on the grid?
    - Liaison with those responsible for package components
    - Responsible for packaging
    - Secure coding practices
    - Secure configurations
    - Includes assessing and reacting to vulnerability alerts

GRID Incident Handling

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- What should we do
  - This stuff should be clarified, define the infrastructure
    - It helps the CERTs in their work, if they know about it as well
  - What do all those cases have in common?
    - Flowerpot falls over and takes down a grid machine
    - DoS against a grid machine
    - Root compromise due to old versions of SSH or GridFTP
    - Strange stuff happening with a presumably stolen grid identity
    - Authentication bypass identified in grid software
  - Those cases should all be regarded as grid incidents by the responsible as per previous slide
  - They need be assessed by grid specialists
  - CERTs can help in the clean-up
  - CERTs should do that in a defined way
- EGEE-II-SA1 working on it

RedIRIS

Conclusions

- e-IRG to support a close relationship between CERT NRENs and GRID community
  - Explore the constitution of NGI incident response teams
  - Establish a direct liaison between EGEE-II and TF-CSIRT