



Finnish
IT center for
science



Gridsec & Nordic NREN CERTS/ U. Kaila

TF-CSIRT, Jan 27-28, 2005

Grid security and NREN CERTS in the Nordic Countries

TF-CSIRT meeting
January 27-28, 2005
London

Urpo Kaila
FUNET CERT



Finnish
IT center for
science



Gridssec & Nordic NREN CERTS/ U. Kaila

TF-CSIRT, Jan 27-28, 2005

Agenda

- Grids as security threats
- NREN CERTS in the Nordic Countries
- Some Grids in the Nordic Countries
- Case: M-Grid in Finland
- CERTS and the Grid challenge



Grids as security threats

- Grids are one of the hottest ICT topics – a promise of cheap easy-to-manage and distributed computing power on demand
- GRID Security threats becomes and issues (examples in next slide)
- Presentations by Andrew Cormac/ UKERNA at the EUNIS conference in Bled, Slovenia in June-July 2004
- Thomas Stridh and Torbjorn Wictorin from Sunet CERT organised a nordic meeting on Grid Security for Nordic NREN CERTS in Linköping on October 2004
 - There we also met Nordic Grid people at the Linux Clusters For Super Computing (LCSC) workshop
 - A very good presentation by Olle Mulmo/ EGEE



The TeraGrid crack last year

Hackers Strike Advanced Computing Networks

By Brian Krebs/ washingtonpost.com / April 13, 2004:

- TeraGrid systems at NCSA at the University of Illinois at Urbana-Champaign and the San Diego Supercomputer Center (SDSC) at the University of San Diego, California attacked
- 20 institutions targeted
- Downtime up to five days
- Stanford (not part of TeraGrid) quarantined dozens of Linux and Solaris hosts



Some common Nordic denominators

- Definitions:
 - Nordic Countries:
Iceland, Norway, Denmark, Sweden & Finland (+ some special regions: Färö islands, Åland Island & Greenland)
 - Scandinavian Countries: Denmark, Norway and Sweden
- A long common history
- Similar mindsets
- (Almost) similar languages – icelandic and especially finnish differs
- Similar social and political structures
- Similar academic structures and NREN's
- Nordunet
- A long IT history, much bandwidth, CPU power and Ne[^] IT skilled people



NREN CERTS in the Nordic:

People who have been discussing grid security:

DK-CERT

Preben Andersen
Mikael Stamm

UNINETT CERT

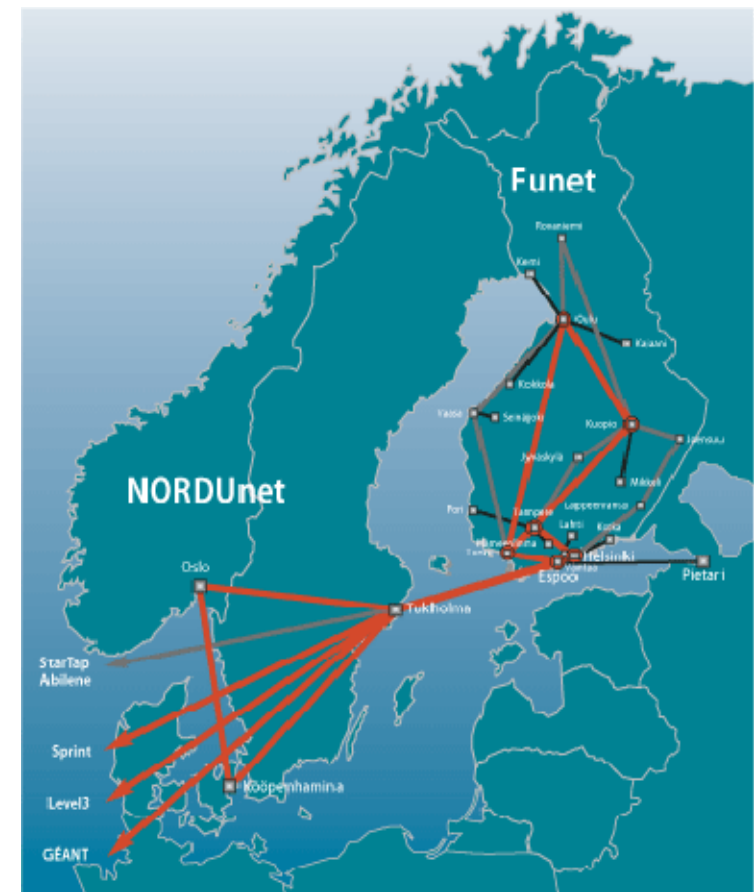
Per A Enstad

FUNET CERT

Urpo Kaila

SUNet CERT

Thomas Stridh
Torbjorn Wictorin





Finnish
IT center for
science



Gridssec & Nordic NREN CERTS/ U. Kaila

TF-CSIRT, Jan 27-28, 2005

Funet CERT

cert@cert.funet.fi

Tel: +358 9 457 2038

Fax: +358 9 457 2302

Funet CERT

- Established 1995, Finland's first official CERT-team
- Operated and staffed by CSC

Current team consists of 5 members: Leila Pohjolainen*, Pekka Kytölaakso, Tony Falenius, Urpo Kaila & Harri Sylvander

- All part time, total approximately 1.5-2 man/year's work
- Serves at office hours, NOT 24/7/365

* "Ms. Funet CERT "



CSC – The hosting organisation for Funet

Services:

- Supercomputing
- The Funet NREN
- Scientific consulting
- IT Services

Customers:

- All finnish universities and polytechnics
- Research institutions
- Some private research too

Organisation:

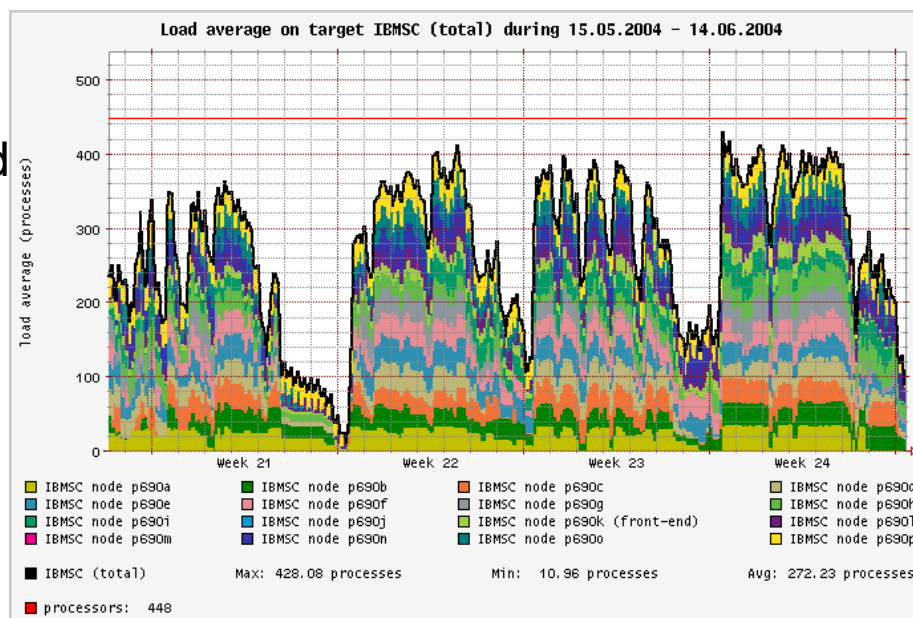
- Staff: 140
- Turnover: 13.3 MEUR / 2003





Some NRENS and grids in the Nordic Countries

- Nordugrid
 - <http://www.nordugrid.org>
 - Largest computational grid in continuous operation
- DEISA
 - Distributed European Infrastructure for Super-computing applications
 - <http://www.deisa.org>
 - sites running IBM p690.
 - global scheduling service.
 - standard set of software
 - Dedicated network
- Grids vs 'traditional' HPC





Finnish
IT center for
science



Gridssec & Nordic NREN CERTS/ U. Kaila

TF-CSIRT, Jan 27-28, 2005

Case: M-Grid in Finland

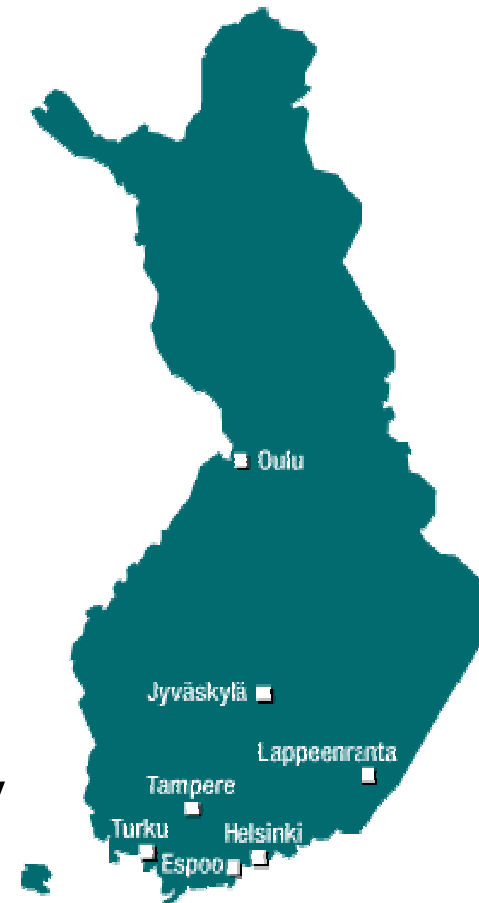
Material Science grid

Consortium by the physics departments
of seven universities, Helsinki
Institute of Physics and CSC

Financed by Academy of Finland
(75%) and the universities

President: Professor Kai Nordlund,
University of Helsinki, Acceleration laboratory
(thank you for the pictures!)

Project Managers; Arto Teräs and Ville Savolainen , CSC





Case: M-Grid in Finland

Hardware:

- HP Proliant DL145 & DL585
- 64-bit Opteron 1.8 – 2.2 GHz
- 2 x 1 Gbit network

Software:

- NPACI Rocks Linux
- NorduGrid ARC middleware

443 processors now

- 1.6 Teraflops
- CSC IBM SC 2.2 Teraflops

sequential and easy-to-parallel jobs





Issues and experiences with M-Grid

- New mode of operation: CSC and local admins
- Remote administration
- Coordination challenges
- Risks for conflicts
- Decisionmaking
- Communication with local IT departments
- New technology
- Risk for bandwidth-hijacking
- User management
- Discussions on the roundtable for IT managers at Finnish universities



Issues and experiences with M-Grid

- Trust in CA
- Responsibilities!
- user management
- Firewalling
- Classification of information
- root/ su(do) cross-site management
- Testing and patching

- Agreed to create a risk analysis, security policy and security guidelines based on the EGEE documents



NREN CERTS and the Grid challenge

- GRIDS can be like the Personal Computer revolution
- New people, organisations, technology, protocols and culture
- The mutual need for cooperation – we will all need each other
- The need for clear and explicit procedures and responsibilities in incident management
- Reviewing of the security procedures and responsibilities



NREN CERTS and the Grid challenge

- The EGEE Security Documents for LCG Sites could be a very good model:
 - Security Policy
 - Usage Rules
 - Incident Response
 - User Registration
 - Certification Authorities
 - Audit
 - Risk Analysis

 - Please quote properly if used



NREN CERTS and the Grid challenge

- The need for communication between Grid management, IT departments and NREN CERTS
- The need for international cooperation
 - On Nordic level
 - On European level
- Grids produce on of the core functions of NREN's – perhaps NREN CERTS could focus more on these and leave consumer related security, generic warnings of vulnerabilities and attacks to government and ISP CERTS?