

**TERENA 3rd NREN-Grids Workshop
27 & 28 April 2006, Paris**

Meeting Report

John DYER & Cătălin MEIROȘU
9th May 2006

Introduction

The third TERENA NREN-Grids Workshop was hosted by Centre National de la Recherche Scientifique/Institut d'Astrophysique de Paris (CNRS/IAP). The workshop explored several aspects of security and incident handling in the context of Grid services. The workshop which ran over two half-days consisted of the following presentations followed by an open discussion. In summary the workshop concluded that:

- Grid Security and Incident Handling can best be handled by existing NREN-CERTs
- NREN-CERTs and Grid experts need to develop a close working relationship and good communication channels

Presentations

***GGF and the Security Area
Olle Mulmo, KTH, Sweden***

Olle Mulmo presented the activity of the Global Grid Forum (GGF), with a particular accent on the area related to security. GGF is leading the adoption of grid computing for research and industry by developing standards, building a community around these standards and ensuring support for and through this community. The activities in the security area develop in several directions, mainly represented by the Certification Authority Operations (CAOPS), the Grid Interoperation Now (GIN), the Firewalls Research Group, the Trusted Computing Research Group and the OGSA Authorisation Research Group (OGSA-AuthZ). A first draft of the GGF Security Roadmap has been made available through the efforts of many volunteers. However, the area to be addressed is extremely large. Help is therefore solicited, from all interested communities, including end users / consumers.

***First results in setting up a CERT Infrastructure in D-Grid
(or How Grids can use existing CERT Infrastructures)
Gerti Foest, DFN, Germany***

Gerti presented D-Grid, a project started by DFN with funding from the German Ministry of Education and Research. D-Grid aims at building an organisational basis that could integrate technical services and make them available to a wide range of Grid projects. One of the areas is related to security and plans to develop CERT services specifically for the Grid community. These services will be building on the

wide experience of the DFN-CERT. The project covers organisational and technical aspects. D-Grid cooperates with other international projects and initiatives, for example TF-CSIRT, EGEE and GGF. The first results of the technical activities will be published soon and will include a survey of national and international CERT activities, as well as an analysis of Grid systems and protocols with respect to potential security risks. A working group dedicated to Grids-related issues was assembled at D-Grid's initiative within TERENA's TF-CSIRT and an email list was setup at grid-cert@grid-security.net.

Grid Security Incident Handling
Carlos Fuentes, RedIRIS, Spain

Carlos presented the workflow of security incident handling at the IRIS CERT. They are using RTIR to keep track of incidents. A private whois database was assembled, containing verified points of contact for every connected institution. The first approach to Grid-related security incidents assumed that exactly the same workflow could be used as in the case of regular security incidents. However, this approach was not adequate because a Grid uses computing facilities that belong to many physical institutions. The solution was to define a virtual super-institution for each Grid, with its own security point of contact and inventory of infrastructure. Carlos thought better cooperation would be required between NREN CERTs and the Grid community in the future, for ensuring timelier response to security incidents. At the end of his talk, Carlos presented a progress report on the new functionality developed for RTIR under the auspices of the RTIR working group established within the TERENA TF-CSIRT.

GRID software from a security perspective
Klaus Moeller, DFN-CERT, Germany

Klaus reported on an ongoing DFN-CERT investigation on the security aspects of Grid use by the German academic community. The investigation examined several Grid software categories for vulnerabilities generated by design weaknesses, programming and configuration errors. The design weaknesses were exemplified by presenting several attack scenarios for UNICORE sites. By applying the average rate of programming errors observed in open source code to gLite, Klaus pointed out that the released code might contain more than 230 bugs. Given the fact that almost any software may contain vulnerabilities, Klaus identified a need for timely sharing, within the CSIRT community, of information that is complete, correct and includes exact recommendations on how to fix the vulnerability. He outlined several projects that aim at standardising the advisories in terms of reference numbers, description and rating of the seriousness level. Finally, Klaus called for improving the security of the patch and software distribution by employing signed RPMs and/or generating PGP signatures for the binary files.

A sustainable e-Infrastructure for Europe
Bob Jones, EGEE Project and CERN

Bob Jones gave an outlook on the present and future of Grid-related infrastructures in Europe. The EGEE project operates a production Grid infrastructure of 200 sites distributed over 39 countries. The networking infrastructure is assured by the GÉANT

network. EGEE developed gLite, Grid middleware that was made available under a business friendly open source licence. The EGEE project identified the need for a permanent Grid infrastructure that would ensure reliable and adaptive support for all sciences in a routine usage phase of multiple, parallel and interoperable Grids from 2008 onwards. Bob proposed to build on the experience of the EGEE and related projects to define a European Grid Infrastructure (EGI) that would be independent on short-term project funding and would federate National Grid Initiatives. The key added value of EGI would consist in coordinating the operations of the Infrastructure, middleware testing and certification, application support, dissemination, outreach and training. The EGEE project is working with the European Commission and the member states, national grid representatives and user communities to develop the details of such a structure and how it can be put in place.

Architectural issues of Grid Security
Dirk Schroetter, Cisco Systems

Dirk approached issues related to Grid Security from a network equipment vendor perspective. He introduced the security architecture of the Globus Toolkit version 4.0 and cited sources indicating that due to the poor performance of the message-level security implementation, the transport-level security is the solution actually used in practical deployments. Taking GridFTP as an example, Dirk described the problems that might be encountered on the control channel and on the data channel when performing high-speed data transfers over network infrastructure built on standard commercially available equipment. He introduced Service Control, a solution that would employ a stateful analysis engine in the network equipment to allow for scaling the throughput to about 10 Gbps while performing deep packet inspection. Dirk also presented the experimental Network Based On-demand/Grid System (NBGS). NBGS works with the Globus Toolkit v4 and offers on-demand, dynamic, automated and quick provisioning of network resources (by automating Cisco CLI or SNMP commands) that may be requested by Grid clients before these clients can schedule application jobs to run on available Grid compute resources.

An NREN-CERT view on ownership and responsibility
Christoph Graf, SWITCH, Switzerland

Christoph Graf asked the questions: "who owns the Grid?"; "who is responsible for the Grid?" and "what are the risks?" It is vital for CERTs to understand these issues when pursuing their role of addressing users' security issues, a task equally applicable in the Grid world as it is for more traditional applications. In order to carry out this role, the CERT teams will need to develop good communications channels with the Grid specialists, in order to help them assess what went wrong. Since large projects like EGEE rely on software from 3rd parties they themselves may not be in a position to help CERTs with information of software implementations.

Whilst it may be easy to answer the question of who owns and is responsible for a cluster of machines dedicated to a grid project, when isolated machines located on a campus LAN are running Grid software, the answer to this question becomes less clear and indeed may be very difficult to determine. This can be problematic if the machine is part of a VO and the VO security is compromised. Whilst it is possible that a local site contact will have information about the Grid services being run, this will

not always be the case. As a result CERTs can only be reactive to incidents and not proactive is reducing them or preventing them.

To-date, there has not been a good track record of the Grid community using the traditional NREN CERTs. Indeed to the knowledge of those present at the workshop, there is no instance of a Grid project registering the local NREN-CERT as the security contact for their machines. Similarly, NRENs have often ignored the existence and development of Grids.

Discussion Session

In terms of providing of trust, the existing Grid projects are relatively small and form well bounded communities and is not an intractable problem, however this will not scale. Identity management needs to be handled at the local institutional level. However, having hundreds or thousands of identity providers exposed at the international level is unmanageable, it is therefore important that these identity providers are aggregated. For the academic and research community, NRENs are the most natural aggregators of identity information. This however raises the issue of how to equate what might be differing levels of trust in different trust communities. Work in this area is being discussed in the REFEDs group (www.terena.nl/refeds) and is tracking the progress made between the Interent2 community and the US federal government. It was noted that whilst it will be appropriate for NRENs to manage the aggregation of identity information and authentication, the authorization to access and use resources will be managed within the institutions or VOs.

It was also noted that the situation with regards standardization is still far from settled. IBM and Microsoft are both strongly backing web-based services which is not commonly accepted across the industry. Microsoft has recently declared that it will not be implementing SAML v2.

In terms of dealing with incidents, it was agreed that the best route will be to use existing NREN CERTs, with the proviso that issue of ownership and responsibility has to be resolved and clearly understood. Maybe Virtual Organisation managers will take overall responsibility. It is however vital that the Grid community experts and NREN CERT teams develop collaborative links and formal communications links.

Klaus Ullmann of DFN explained that both NRENs and Grid communities operate infrastructure comprising of resources that have to be funded. We all need to work together to put in place mechanisms to solve problems that arise. He did not think that the NREN-PC was the body that should ultimately take responsibility, nor was it currently clear that the new body being discussed to oversee a sustainable Grid infrastructure would be the right place. It is clear that all groups need to work together over the coming years to identify the best solution.

There was some discussion about the possibility of segregating Grid use of the network from general-use; however it was agreed that since there is no technical reason why this should be done, indeed since around 50% of European NRENs do not have an optical platform, then this would be impossible without building a parallel infrastructure. Other issues that were touched on included the potential need for Grid operators to keep usage logs to comply with European directives.

TERENA 3rd NREN-Grids Workshop
27 & 28 April 2006, Paris

Attendee List

Yuri Demchenko	University of Amsterdam
Francois Ducrot	Renater
Stephane Dudzinski	DIAS
John Dyer	TERENA
Szalai Ferenc	NIIF/HUNGARNET
Lars Fischer	NORDUnet
Gerti Foest	DFN
Carlos Fuentes	IRIS-CERT/RedIRIS
Jean-Paul Gautier	CNRS/UREC
Brian Gilmore	The University of Edinburgh
Mathieu Goutelle	CNRS UREC (EGEE)
Christoph Graf	SWITCH
David Groep	NIKHEF
Marc Hemberger	EMBL Heidelberg
David Jackson	CCLRC
Bob Jones	CERN
Christos Kanellopoulos	GRNET/AUTH
David Kelsey	CCLRC/Rutherford Appleton Laboratory
Catalin Meirosu	TERENA
Klaus Möller	DFN-CERT
Olle Mulmo	KTH
Michael Naumann	ESO
Ian Neilson	CERN
Alex Reid	AARNet
Geneviève Romier	CNRS - UREC
Dirk Schroetter	Cisco Systems
Milan Sova	CESNET
Louis Twomey	HEAnet Limited
Klaus Ullmann	DFN-Verein
Rosette Vandenbroucke	BELNET
Dany Vandromme	RENATER
John Walsh	Trinity College, Dublin
Asli Zengin	TUBITAK-ULAKBIM