# Beyond Grid Security

**Bruno Hoeft, Ursula Epting, Tobias Koenig**

Forschungszentrum Karlsruhe, Institute for Scientific Computing,
Herman von Helmholtz Platz 1, 76344 Eggenstein-Leopoldshafen

Bruno.Hoeft@kit.edu, Ursula.Epting@kit.edu, Tobias.Koenig@kit.edu

**Abstract:** While many fields relevant to Grid security are already covered by existing working groups, their remit rarely goes beyond the scope of the Grid infrastructure itself. However, security issues pertaining to the internal set-up of compute centres have at least as much impact on Grid security. Thus, this talk will present briefly the EU ISSeG project (Integrated Site Security for Grids).

In contrast to groups such as OSCT (Operational Security Coordination Team) and JSPG (Joint Security Policy Group), the purpose of ISSeG is to provide a holistic approach to security for Grid computer centres, from strategic considerations to an implementation plan and its deployment. The generalised methodology of Integrated Site Security (ISS) is based on the knowledge gained during its implementation at several sites as well as through security audits, and this will be briefly discussed. Several examples of ISS implementation tasks at the Forschungszentrum Karlsruhe will be presented, including segregation of the network for administration and maintenance and the implementation of Application Gateways. Furthermore, the web-based ISSeG training material will be introduced. This aims to offer ISS implementation guidance to other Grid installations in order to help avoid common pitfalls.

## 1. Introduction

The Integrated Site Security for Grids (ISSeG) project, is partly funded by the EU and part of the EU Framework Program 6. ISSeG started at the beginning of February 2006 for a period of 26 months and will end in March 2008. Three scientific partners and one industry partner are collaborating in the project:

- CERN, Switzerland; the first initial implementation and the overall project management
- Forschungszentrum Karlsruhe GmbH (FZK), Germany; the adaptation of the initial implementation, development of methodologies for generalised recommendations
- Science and Technology Faculty Council (STFC) (former CCLRC and PParc), United Kingdom; developing training and dissemination material.
- CAPGEMINI, France; an international security company; risk assessment and site security audit of the three scientific project collaborators

Grid security is only as strong as the security of each federated site. The mission of this project is to enlarge the Grid security from a grid centricity towards an integrated site security. The improvements gained through two implementations at CERN and Forschungszentrum Karlsruhe as well as the experiences of the implementation are collected and taken as basis for the development of training material, for the compilation of the recommended methodology and for generalised recommendations. The material will guide other sites in deploying the integrated site security.

The ISSeG approach is designed for a deployment at worldwide LHC Computing Grid, but the compiled methodologies, the generalised recommendations and the developed training material are not restricted to WLHC only, but applicable at a large number of other sites and communities as well.

## 2. ISSeG concept and structure

The project is organised in the following project phases: Development of strategic directions [1],[2]; implementation plan; deployment; dissemination. During the development of the first project phase five strategic directions are defined:

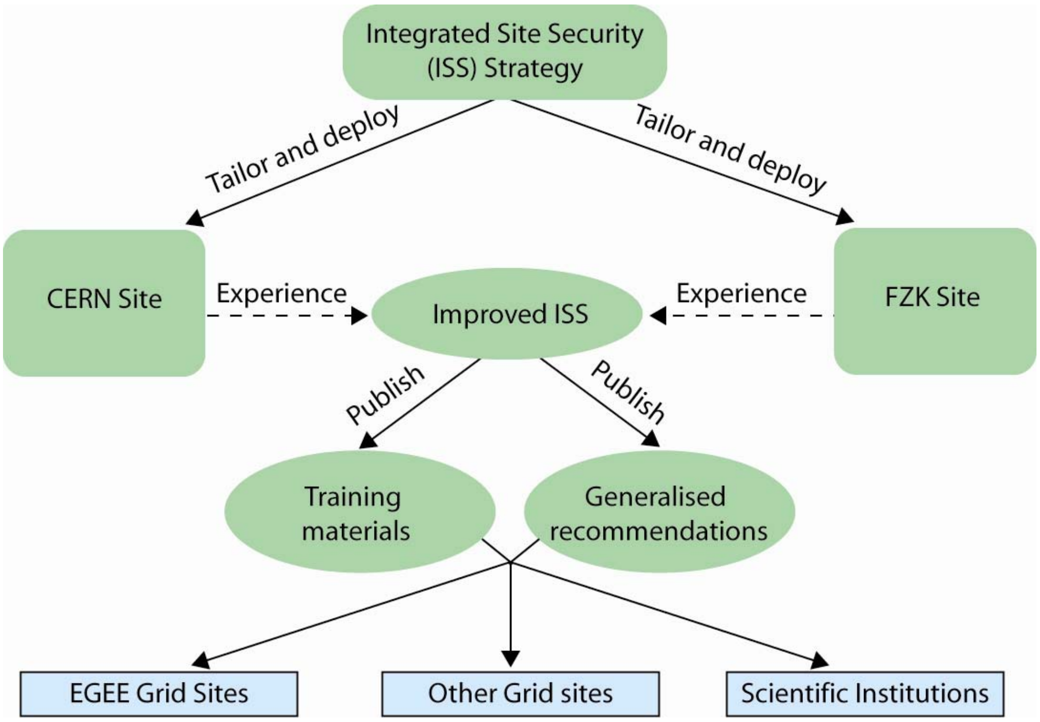
- Central management of resources
- Integrate identity and resource management
- Enhance network connectivity management
- Integrate and evolve security mechanisms and tools
- Integrate security training, best practice and administrative procedures

The further granulized strategies are the basis for the implementation plan. The implementation plan is already technically oriented towards the specific requirements of a participating site. For example the first strategic direction is covered by the implementation area: Resource management extensions. This area is further refined into the following subtopics:

- Extend the use of centrally managed accounts
- Extend the use of MS Patch-Management
- Evaluate mechanisms for central Linux-Patch-Management
- Revise configuration of active network devices to enhance security

The tasks defined in the implementation plan are deployed at the ISSeG Partners. All gained experiences as well as use of best practices are collected [3][4].

The following figure visualizes the concept of ISSeG from the first phase, the strategic direction, to the last phase, the dissemination of the generalised recommendations and the training material:



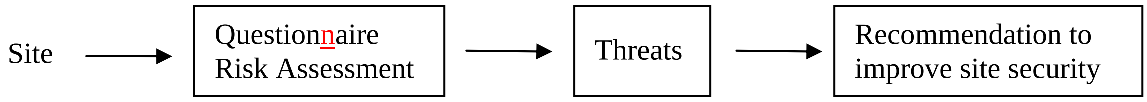
## 3. Security Audit

A site security assessment has been carried out at the three partners of the ISSeG project in terms of:

- Administrative and regulatory
- Training and awareness
- Technical security (network, servers, end-user systems)

The security audit is based on a questionnaire containing a subset of the ISO/IEC 1 7779:2005 standard [5]. With the results of the questionnaire the current security level as well as weaknesses against certain threats of each collaborator could be identified on a prior defined asset/threat matrix.

A questionnaire for a self audit of sites is developed, based on the comparison of the ISSeG collaborators security audit. The results of the questionnaire at a site will identify threats confronting the site. Based on the asset/threat matrix recommendations will be offered for the site. If the site is following the actions, specified in the recommendations, the site will close the vulnerability and raise their security level to a higher standard.



## 4. The aim of ISSeG

The aim of ISSeG is more than to fulfill the security goals for a single site. Goals for a single site could be:

- Retain the security of the site for an effective working environment, while enough openness for scientific research is assured;
- Ensure confidentiality, integrity and availability of research and personal data.

We conceive the security approach of integrated site security towards the concept of integrating the technical, administrative and educational aspects of information security at your site so that they work together to improve your overall site security. While this is not specific to Grid environments, it is extremely relevant to all Grid sites as we all work together.

It affects not only the appliance of technical safeguards, for example to install anti-virus software on all PCs over a campus, automate their virus definition updates and to keep the virus protecting engine up to date. An administrative safeguard needs to be implemented as well, for example a security policy, stating that every PC must run a valid anti-virus software product and including arrangements for enforcement of the security policy. Never the less this must be complemented by education of the users so that they understand the necessity of the security measures. For example a normal user has to know that running anti-virus-software is mandatory and shields the PC from malicious software and that the PC can get infected as soon as this protection is switched off. Besides the user education, the management needs additional information for example of security procedures, law requirements and the implied costs of a security incident. The training shall encourage them to support the security team that even if there is the need to implement unpopular security actions they would support the enforcement through the organisation and with this backing up the necessary actions of the security team. A good solid education could achieve a much better understanding of security, and could change from a “viewing security as some odd add on” towards a culture including security in their standard way of behaving.

## 5. ISSeG partner projects

The security approach of ISSeG is to build recommendations based on a generalised methodology, which supports sites to improve their security. The grid infrastructure of the tier-0 and tier-1 sites within LHC collaboration has quite a high standard and could be considered as save.

For achieving this security level several groups in the EGEE framework are supporting the LHC installation. We are including the efforts of those projects if possible in our recommendations, or at least point to their contributions:

- OSCT → Operational Security Coordination Team: distributing information in LHC collaboration about security risks and exploits in Grid Middleware, finding/developing workarounds and initiation of patches to fix security risks and exploits; distributing information of penetrated sites
- JSPG → Joint Security Policy Group: including security aspects in MOU each site has to sign and caring for the enforcement
- GSVG → Grid Security Vulnerability Group: announcing patches and/or workarounds for scientific linux exploits and security risks, working closely together with CERT
- CERT → Computer Emergency Response Team: announcing patches and/or workarounds for operating system and cross platform application exploits and security risks

But still this is not sufficient to provide a secure shielded network within the LHC-OPN. Most in LHC collaborating sites consist of a multi disciplinary research environment. This implicates that the grid computing infrastructure of one site is only a fraction of the centre. There are several possible doors for security attacks of intruders to a site. One site is facing at several angles security threats. In case the site is hacked it is only a question of time till the grid installation at this site is penetrated as well and if one grid site is penetrated all other grid sites within the collaboration are not protected anymore.

For the support of other sites a questionnaire has been developed. With the questionnaire it is possible to execute a self audit and risk assessment on the site. The result of the questionnaire is highlighting on a thread/risk matrix certain issues pointing towards the appropriate recommendation. It is now up to the site to deploy the according at the "how to" section of the recommendation specified action(s). The questionnaire for the self audit as well as the recommendations can be found at the ISSeG web site [6]

Besides the questionnaire and the recommendations ISSeG is offering training material on its web site. It is organized to fit for the different roles of people. There is training material for user, administrator, developer and manager. The user training material encourages the user to comply with the security policy regulations, whereas the training material for the administrators includes much more technical components. All training material provides, besides a frame, with the basic information and includes spaces for individual adaptation for site requirements at which the training is held.

All material provided by the ISSeG project including the questionnaire, the recommendations and the training material will be kept up to date for the duration of the project and will be available at the web site[6].

**References**

[1] DESCRIPTION OF CERN ISS STRATEGY https://edms.cern.ch/file/741402/LAST_RELEASED/ISSeG-Del-D1.1.1-703955-v3.0.pdf

[2] DESCRIPTION OF FORSCHUNGSZENTRUM KARLSRUHE (FZK) ISS STRATEGY https://edms.cern.ch/file/748813/LAST_RELEASED/ISSeG-Del-D1.2.1-710066-v3.0.pdf

[3] INTERMEDIATE REPORT ON DEPLOYMENT AT CERN AND INPUT ON LESSONS LEARNT TO WP3 AND WP4 https://edms.cern.ch/file/807869/1/ISSeG-Del-D1.1.3-Report-710055-v3.0.pdf.

[4] .INTERMEDIATE REPORT ON DEPLOYMENT AT FORSCHUNGSZENTRUM KARLSRUHE AND INPUT ON LESSONS LEARNT TO WP3 AND WP4 https://edms.cern.ch/file/819336/1/ISSeG-Del-D1.2.3-Report-710075-v4.0.pdf

[5] ISO/IEC FDIS 17799:2005(E) – Information technology – Security Techniques – Code of practice for information security management.

[6] ISSeG taining WEB http://www.isseg.eu