WLCG Security TEG Scope and Status

Romain Wartel <Romain.Wartel@cern.ch>

Version	Date	Author	Comment
0.1	02 April 2012	Romain Wartel	Initial version
0.2	20 May 2012	Romain Wartel	Adding FedId + Usability report

Security TEG Scope and Status

The Security TEG has highlighted several areas of work and divided its efforts in five different subtasks. Each subtask has a coordinator and several contributors.

More details are available at https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG

All the security TEG reports are available at http://cern.ch/go/Jdk7

1. WLCG Risk Assessment / Analysis

Status: complete, report available

The WLCG Risk Assessment exposes and proposes a score for the different risks that have been identified.
This is a status report, and recommendations/mitigations will be worked on at a later stage.

This is also a "live" document, which is expected to be updated regularly based on the feedback from the security operations and incidents faced by the security teams in our community.

2. AAI on the worker nodes

Status: work in progress, report available

One of the subtasks of the Security TEG focused on the "Authentication and Authorization Infrastructure (AAI) of the Worker Node".

The initial conclusions of the working group have already been presented during the December GDBs and TEG reports session in February, in particular:

- Fine-grained traceability is necessary and an essential component of WLCG security;

- It is only possible to achieve a reasonable level of traceability by implementing a form of Unix identity switching (gLexec, sudo, VM-per-job, Linux Containers, etc.).

Concerns were raised about the traceability of the ATLAS computing model, but were settled as ATLAS announced recently its intention to adopt glideinWMS.

The TEG then prepared a status report for this subtask. It is available at:

https://twiki.cern.ch/twiki/pub/LCG/AAIOnTheWorkerNodes/WLCG_WN_Security-05.pdf

The report remains work in progress and does not yet fulfill all the expectations of the TEG.

The goal of the document is to review the AAI situation on the WN, including the job submissions components of each experiment, with a particular focus on their traceability abilities.

Several areas would need further discussions or are yet to be addressed, including:

- The needs and requirements linked to the use and transport of credentials on the WN, including delegation, propagation, revocation and traceability.

- The implementation of security controls (e.g. blocking/banning end users, credential revocation) and who should operate them.

- The ownership of the traceability information. For example, is it acceptable to split the traceability information among different participants (VOs and sites)?

- The security implications and benefits of the introduction of virtualization on the WN
- The security implications of submitting jobs to external/private clouds
- The network connectivity requirements of the experiments
- The longer term future of the security model of the WN

3. AAI on the storage systems

Status: work in progress, report available

One of the subtasks of the Security TEG focused on the "Authentication and Authorization Infrastructure (AAI) of the storage systems".

The group has prepared a status report of the current situation on storage systems.

4. Identity Federation

Status: work in progress, report available

The "Federated Identity Management for Research Collaborations " document proposes a vision for the adoption of identity federation among different communities - including HEP.

The Security TEG has reviewed the document and given positive feedback.

The document is available at https://cdsweb.cern.ch/record/1442597

5. Usability vs Security

Status: complete, report available

The Security TEG reviewed a number of usability aspects of the current security systems. Usability is a key aspect to enable adoption and optimal use of WLCG security controls.

The group has prepared a status report and included a set of recommendations in this area.