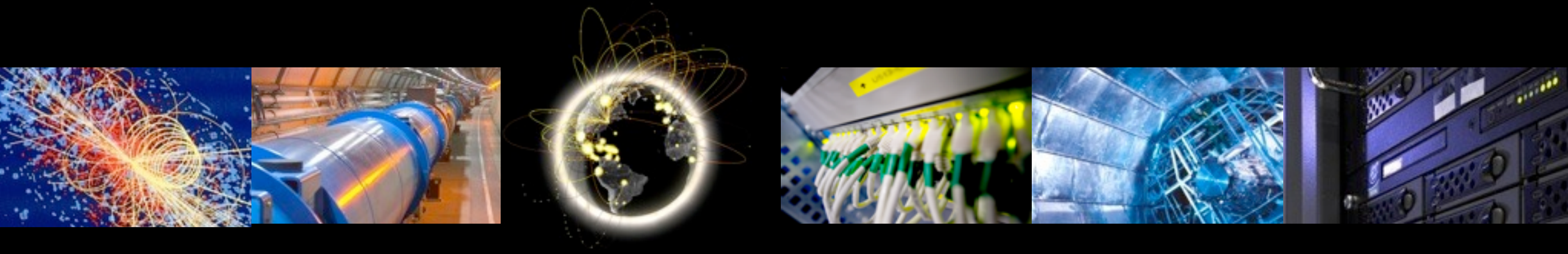
WLCG Group

Update on the security TEG

GDB, 14th December 2011



WLCG
Worldwide LHC Computing Grid

General update

- Representation from the 4 LHC VOs + several sites
  - 19 members in total
- 2 face-to-face meeting organised (7th Nov, 7 Dec)
- Weekly phone meetings

- 5 different subtasks
  - WLCG risk assessment (in progress)
  - AAI on the worker nodes (in progress)
  - AAi on the storage systems (not started)
  - Identity federation (in progress)
  - Usability vs Security (just started)
- All details at:
  - https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG

Risk assessment

- Work in progress!
- Aim at producing a document.
  - http://cern.ch/go/dt9S
- Objectives:
  - Identify our assets (what we want to protect)
  - Identify the main threats stemming from malicious intents
  - Score and highlight the most important risks
    - Based on likelihood of each threat
    - Based on the typical impact of the realisation of the threat
  - Discuss the risks and how they affect our assets
  - Propose recommendations for each of the risks

- An early draft version is available (no recommendations yet)
  - All feedback welcome!

Assets

Asset	Comments
Trust / collaboration	The trust established between WLCG participants, collaborating infrastructures, external partners and funding agencies, needs to be maintained
Reputation	Reflects the opinion of the general public, funding agencies and participants about WLCG
Intellectual property	It includes both copyrighted material and the result of scientific work conducted on WLCG resources
Data protection	The protection of the data collected by, stored at and handled by WLCG resources.
Digital identities	Includes both the credentials and the attributes enabling the authentication and authorization of users and services.
CPU resources	Physical or virtual entities that are consumed through Services to enable calculations to be conducted, for example worker nodes
Data resources	Physical or virtual entities that are consumed through Services to enable LHC data to be stored
Network resources	Network facilities enabling the different WLCG participants to cooperate and users to access WLCG resources
Services	A service is any computing or software system, which provides access to, information about, or controls tangible assets. This includes the services necessary to the usage, support, operation, monitoring of WLCG as well as the communication and dissemination within and outside the collaboration, such as websites, wikis, etc.
Data integrity	The accuracy, lack of alteration and consistency of stored data (for example scientific data) on WLCG resources

Risk scoring

- Likelihood: estimate of the number of expected events per year, mapped to a scale from 1 to 5.

Impact \ Likelihood	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	**15**
4	4	8	12	**16**	**20**
5	5	10	**15**	**20**	**25**

- Impact:
  - Minimal impact on WLCG's ability to deliver its services to users
  - Minor impact, operational or financial costs, or local service disruption for less than a week
  - Serious localised disruption of some WLCG services for some users, for a week or more, leading to a productivity loss, or significant financial or operational costs
  - Serious global disruption of some WLCG services to all users, for a week or more, leading to a productivity loss, or significant financial or operational costs
  - WLCG is unable to deliver services to any of its users, for a week or more, or suffers risk to its funding or other business continuity issue

Risks

Threat	Likelihood	Impact	Risk
Misused identities	5	5	**25**
Compromised identities	5	4	**20**
Attack propagation between WLCG sites	4	5	**20**
Exploitation of a serious OS vulnerability	4	4	**16**
Threats originating from trust services	3	4	**12**
Negative publicity on a non-event	2	4	**8**
Insecure configuration leading to undesirable access	3	2	**6**
Insufficient protection of information leading to sensitive data leakage	3	2	**6**
Incidents on resources not bound by WLCG policies	1	5	**5**
Exploitation of a serious VO/middleware software vulnerability	2	2	**4**
Data removal/corruption/alteration	1	3	**3**
DoS from an external organisation	1	1	**1**

WLCG Worldwide LHC Computing Grid

LCG

Publicity & Traceability

- Publicity
  - Aggravating factor for all previously mentioned risks
  - Media interest needs to be handled with care (and training!)
  - Negative impact is not necessarily linked with severity of incident
  - The accuracy of the information being reported often not relevant
- Traceability
  - 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
  - The AAI on the WN subtask will review different technical possibilities and implementations, in terms of security, performance impact, development and maintenance costs.
  - The result of this work will be presented during GDBs.