

Security challenges for Experimental Facilities

Pedro Soria-Rodriguez
pedro.soria@atosorigin.com

Atos Research & Innovation (Atos Origin)

2008-04-02 - Bled

Security in Experimental Facilities

- Why Security?: Protection of assets
- Procedure:
 - 1) Identify assets
 - 2) Study threats to assets
 - 3) Identify vulnerabilities
 - 4) Decide on security measures to protect assets

10-minute risk assessment of Exp. Networks

ASSETS

Infrastructure + Content

- **Infrastructure:**
 - The physical+logical infrastructure to provide the slices to users (experimenters)
- **Content:**
 - The applications, software, networking, content, etc... which researchers will run on the experimental infrastructure

10-minute risk assessment of Exp. Networks

Threats, Vulnerabilities on INFRASTRUCTURE

- Vulnerabilities:
 - Confidentiality likely not an issue (not a production net.)
 - Resources: access needs to be controlled.
- Threats:
 - Stealing of unassigned resources for slices
 - Time duration of experiments: longer than assigned

10-minute risk assessment of Exp. Networks

Threats, Vulnerabilities on CONTENT

- Vulnerabilities:
 - Experimental content: may not be mature (vulnerable)
 - Confidentiality of experimental content (soft, methods, etc).
 - No confidentiality of information in experimental content
- Threats:
 - Unauthorized access to content other than the user's own.

Security / Trust in Exp. networks

Summary:

- Main security issues:
 - Confidentiality of content
 - Access control of infrastructure and content