Grid Security Monitoring

Daniel Kouřil, CESNET

EGEE07, October 2nd

www.eu-egee.org

Information Society and Media

The Goal

- **security monitoring should:**
  - prevent from security problems
  - detect known issues that can lead to a security problem
  - detect suspicious patterns
    - issues not know in advance
  - help stop spreading ongoing attacks, ...
  - possibly detect a breach, etc.
    - do we really want to perform intrusion detection?

The 1st Grid Attack

- **how is it going to look like?**
  - i.e. what we should be able to detect?
- **attack on the grid infrastructure**
  - preventing a (sub)grid from working
  - making them not work correctly
- **attack using the grid infrastructure**
  - far more dangerous
  - requires grid-aware attackers
    - but gives them an attractive tool!

What to monitor

- **grid specific infrastructure**
  - project-wide (BDII, GOC DB, web, ...)
  - VO infrastructure components (VOMS, WMS, UI, MyProxy...)
  - resources
    - i.e. sites (CE, SE)
- **Common networking components**
  - DNS,
  - can rely on sites, ISPs, etc, but should be able to incorporate results (when authorized)

How to monitor

- **Identify potential weaknesses**
  - improper credential management, ...
- **and how they can be measured**
  - weak passphrase, wrong filename permissions, ...
  - vulnerabilities identified by the GSVG
- **and how they can be monitored**
  - sensors, monitor jobs, ...
- **and how the reports are collected and processed**
  - including notifications and proper access control
  - aggregation of reports from multiple sources
  - dependencies across sites, etc. (denyHosts, ...)
  - binding monitoring to policies/procedures?
    - how to process detected problems
    - don‘t be annoying for the site admins

Monitoring tools

- **many available and used**
  - infrastructure (SAM, Nagios), jobs (L&B), ...
  - work independently
  - no high-level view (?)
- **no YAMT (yet another monitoring tool)**
  - try to make them collaborate instead
  - automated sharing, correlation, ...
- **scalable!**
  - a lot of machines to monitor in the Grid
- **Honeypots**
  - can we afford running these tools?
  - interesting to examine grid attack(er)s
  - what areas to monitor inside honeypots?

How to proceed?

- **Plan by the end of the project**
  - possibly to continue in EGEE III
- **Identify primary areas of concern**
- **Identify proper monitoring tool(s)**
- **Write sensors, tests**
- **Design how the results are processed**
  - aggregation, access control, responsible people (VO, site admins, ...)