Update on operational security

Romain Wartel, CERN IT

EGEE Operational Security Coordination Team

GDB Meeting, 07 November 2007

www.eu-egee.org

Information Society and Media

EGEE and gLite are registered trademarks

Recent incident

A low severity incident occurred on Oct 18. It is now resolved:

- **It illustrated again that cooperation between sites and grid projects is essential**

- **Collaboration between the OSG security team and the OSCT was really helpful**

- **During the incident, several concerns/weaknesses have been identified at different levels**
  - **See next slides**

Usage of KCA robots (1/8)

- **Whenever used in conjunction, KCAs and robots are posing new security risks.**

KCA robots require Kerberos keytabs (= unprotected long lived credentials) to be stored on the filesystem on the node where the robots are created. The keytabs are then used to automatically request short-lived X509 certificates from the KCA.
The use of KCA robots need a security review.

- **Action:** The FNAL KCA managers will discuss the issues related to KCA robots at the next TAGPMA meeting (6th-9th Nov). David Groep (SCG) will report back

- **Status:** Discussed in a JSPG meeting and has been referred to TAGPMA

Blocking proxies - AuthN (2/8)

- **No CRL for KCAs is available to the sites**

It is not possible to block valid proxy certificates issued by KCAs at the authentication level

- **Action:** The FNAL KCA should include a URL to its CRL in the next CA release

- **Status:** Irwin Gaines (FNAL KCA) agreed on 29/10/2007 (JSPG meeting), implementation in progress

Blocking proxies - AuthZ (3/8)

- **It is not possible to easily block valid proxy certificates at the authorization level**

It is not easily possible to block valid proxy certificates at the authorization level. Usually not a significant issue as the lifetime should be 24h (~ time needed to contact all the CSIRTs).

But various VOs are using a longer proxy lifetime (often 7 days):

  - Temporary workaround (required for some time)
  - Some VOs/infrastructure (eg: CDF, NorduGrid) use extended lifetime instead of using of MyProxy

A central AuthZ service in EGEE should be investigated.

- **Action:** MWSG has been notified and is discussing a CRL-like mechanism (central AuthZ service) for authZ
- **Status:** Raised in MWSG. Consensus that this is needed. Christoph Witzig will report back after the MWSG meeting early December

Incident response in Italy (4/8)

- **Incident reporting and follow-up both at the site and at the region was delayed and the incident response procedure has not been followed**

- **Action:** The ROC Security Contact has been asked to perform a review of the security incident handling in the region and to identify actions to ensure that an appropriate and timely response is given to security incidents, both at the sites and at the regional level

- **Status:** A report has been requested (31/10/2007) before the end of the year

OSCT-DC role (5/8)

- **There were delays in the follow-up of the incident in the OSCT**

The OSCT-DC (= Duty Contact) should “assume responsibility to coordinate [incidents] in an appropriate timeframe” (OSCT internal documentation)

- **Action:** Clarification of the role of the OSCT Duty Contact (OSCT-DC) in the team

- **Status:** Done during the OSCT phone meeting on 30/10/2007 (the role of the OSCT-DC was already explicitly documented)

CDF Framework (6/8)

- **Security issues have been identified in the CDF framework**

Its design and implementation should be reviewed.

- **Action:** CDF should state the corrective actions it intents to implement to prevent similar incidents from re-occurring

- **Status:** The CDF VO managers have been asked (on 01/11/2007) to produce a report before the end of the year

Framework audit (7/8)

- **The VO frameworks impact the security of the infrastructure**

The use of frameworks is increasing and requires appropriate mechanisms to ensure a reasonable level of security in the job submission process. It is also important to ensure that existing middleware security mechanisms match the needs of the VOs.

- **Action:** The frameworks need a security review

- **Status:** On hold

Granularity of controls (8/8)

- **Traceability and control are essential to grid operations**

The incident demonstrated the importance of sufficient granularity in the traceability of the originating user of a job and in the controls that can be applied to the users and the VOs.

(glexec can help, but only with the setuid bit mode)

- **Action:** JSPG is updating the traceability and logging policy (old "LCG Audit requirements")

- **Status:** A new draft is being prepared

Traceability and logging policy

"The minimum level of traceability for Grid usage is to be able to identify the source of all actions (executables, file transfers, pilot jobs, portal jobs, etc) that are part of an incident and the individual who initiated them.

In addition, sufficiently fine-grained controls, such as blocking the originating user and monitoring to detect abnormal behaviour, are necessary for keeping services operational.

It is essential to be able to understand the cause and to fix any problems before re-enabling access for the user."

https://edms.cern.ch/document/428037

Questions?

EGEE and gLite are registered trademarks