Security Monitoring

Daniel Kouřil (CESNET), kouril@ics.muni.cz

OSCT meeting, 22.3.2010

Security Monitoring in OSCT

- **Started in cca Jan 2009**
- **Integration with project monitoring**
  - SAM existed, Nagios emerging
  - Collaboration with OAT, membership overlaps
  - Agreement on main principles
    - https://twiki.cern.ch/twiki/pub/LCG/OSCT-EGEEIII-tasks/security-monitoring-v0.12.pdf
- **Patch monitoring**
  - Many attacks abuse unpatched vulnerabilities
  - Continuation in development of Pakiti
- **Tracing users‘ activities**
  - Identifying information sources
  - Development of basic tools

Goals of security monitoring

- **Detecting operational problems or even incidents**
  - Focus on grid specics or issues being exploiting
  - Not a replacement of sites‘ responsibilities
- **Help sites to keep their resources secure**
  - Warning sites exposing vulnerabilities
- **Main focus on higher levels (ROC, project)**
  - Provide the project and ROC (OSCT) with information about site status
  - not concerned with site level and its internals
- **No special privileges required from sites**
  - Only public interfaces used
- **Utlization/extenstion of existing monitoring framework(s)**

Current Status

- **A few SAM tests used**
  - CRL, file permission checks, Pakiti in production
  - Results encrypted and only available to ROC security contacts
  - Manual evaluation
- **Focus on Nagios-based framework**
  - Project and ROC view
    - SAM probes to be ported
    - Tests to be launched from ROC-level Nagios
  - Results collected in a standard way via message bus
    - Encryption applied
  - Access allowed to ROC security contacts and site admins
    - Synchronized with GOC DB (TBC)

Pakiti

- **Open source tool to check patching status**
  - https://www.sf.net/projects/pakiti
  - Any site can run its own Pakiti server to monitor internal machines
  - Many problems can be prevented by proper patch mgmt!
- **Server evaluates packages installed on clients**
  - Detects security patches not applied
  - Allows for searching for particular vulnerabilities (CVE)
    - Proved very useful recently (e.g. CVE-2009-2692, CVE-2009-2698)
- **Currently maintained by OSCT**
  - A lot of improvements applied
  - New release published recently
- **OSCT operates Pakiti server for EGEE**
  - Information collected with SAM/Nagios probes (WNs)
  - Only OSCT members allowed to access

Pakiti Results

- **Significant adaptations applied in 2009**
  - Scalability and performance
  - New functions specified and designed
- **First widely used in Aug/Sep 2009 to track severe kernel vulnerability**
  - A lot sites (WNs) found to be vulnerable
  - Gradually escalated, discussed at PMB
  - OSCT endorsed by the management
  - Site suspensions made possible
- **Other similar exercises since then**
  - Better procedures
  - Site often reacted more promptly
- **Pakiti utilized outside EGEE, too**

Tracing users‘ activities

- **Aimed to help in resolutions of incident**
- **Processing of monitoring data to trace particular users**
  - Only users granted access to the data can use the tools
- **Site and Grid (VO) level**
  - (Sys)log handling, L&B utilization
  - Different roles/privileges needed
- **Two tools developed so far for**
  - lcgCE for site admins
    - Parsing log files produced by lcgCE
  - L&B for VO managers
    - Obtaining job data from LB server(s)

lcg-CE tracer: usage example

- Digging for information related to a suspected user DN
  - Site CSIRTs notified about malicious job submitted by a given DN

```
# dig-lcgce -s 20090901 -e 20090916 userDN eq '/C=IT/O=INFN/OU=Personal
Certificate/L=CNAF/CN=giuseppe misurelli'

{
'localUser': '18700',
'ceID': 'gridit-ce-001.cnaf.infn.it:2119/jobmanager-lcgpbs-cert',
'timestamp': '2009-09-07 14:00:21',
'userFQAN': ['/dteam/Role=NULL/Capability=NULL',
'/dteam/italy/Role=NULL/Capability=NULL', '/dteam/italy/INFN-CNAF/Role=NULL
/Capability=NULL'],
'userDN': '/C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=giuseppe misurelli',
'jobID': 'https://lb009.cnaf.infn.it:9000/ZTHAJucuJpw4mgwKysV_2A',
'lrmsID': '118258.gridit-ce-001.cnaf.infn.it`
}
```

gLite-LB tracer: usage example

- Looking for information about jobs recorded by a given LB
  - Security officer needs forensics on a specific job

```
#lbtrace -k host -H octopus.grid.kiae.ru list owner eq
'/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=samoper/CN=582979/CN=Judit Novak'
and status eq done and destination eq snowpatch-
hep.westgrid.ca:2119/jobmanager-lcgpbs-ops

--- Job 1:
JobId: https://octopus.grid.kiae.ru:9000/B1uLHolwYwpTYh1uwudmjQ
Owner: /DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=samoper/CN=582979/CN=Judit
Novak
Source: sam111.cern.ch
JobState: Done
StatusReason: Job terminated successfully
Destination: snowpatch-hep.westgrid.ca:2119/jobmanager-lcgpbs-ops CondorID: 664
GlobusID: [none]
PBSOwner: [none]
PBSNode: [none]
```

Transition of security monitoring

- **Project-wide Pakiti installation maintained by the OSCT**
  - Several sites operate their local instances
    - CESNET, SEE-Grid sites, NIKHEF
  - Checks maintained by SAM, but nothing meanigful reported at the SAM portal
  - The CERN instance is easy to move to EGI one
- **SAM probes**
  - Part of standard test suite
  - Results available from the SAM portal only to OSCT members
    - In the past allowed to detect sites vulnerable to a certain issue
  - Similar model followed with Nagios
- **Traceability tools**
  - On-demand tools provided as commands
  - Whoever can use them on data they own

Security Monitoring in EGI

- **Development**
  - Continuation in current aims
  - Maintanence of the tools developed
- **Operations**
  - Maintanence of project-wide Pakiti server
  - Results checking/evaluation, automation of the process
- **Support of NGIs/sites and their „internal“ monitoring**
- **Effort needed cca 1FTE**
  - Hopefully part of TSA1.2 (A Secure Infrastructure)
  - Any contribution of NGIs is highly welcome