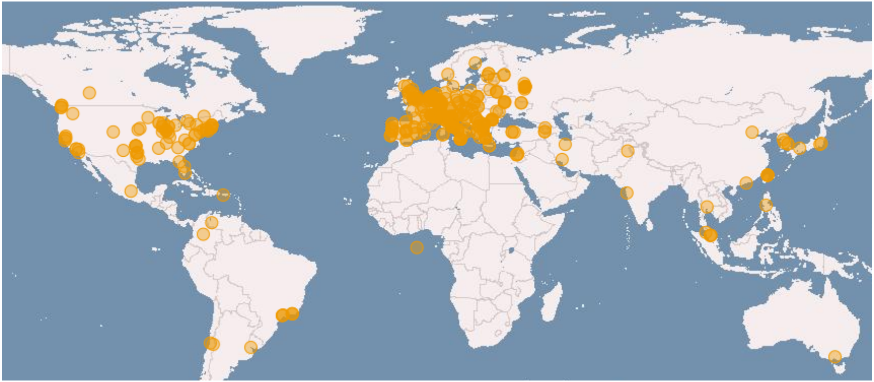
# Operational Security in EGI

Leif Nixon

Nationellt Superdatorcentrum

2012-12-17

# EGI[1] sites



[1] For some definition of “EGI”

# Operational Security in EGI

Impossible task:

- 58 different jurisdictions
- Sites are independent – very little centralized power
- Sites range from big national facilities to small underfunded departmental systems.
- Sites are usually already in the constituency of some other CSIRT.

# Operational Security in EGI

Basically, EGI is a federation of National Grid Infrastructures (NGIs) – typically one per country – that each encompass something between 1 and 40 physical sites.

# Operational Security in EGI

- High level policies give a framework to operate in.
- Weapon of last resort – suspension. Follow the rules, or you can’t be in our club.

# Operational Security in EGI

- Each NGI has an appointed NGI security officer.
- A core subset (about a half dozen) of the NGI security officers form the EGI Incident Response Task Force (IRTF).

# Operational Security in EGI

IRTF members serve as EGI Security Officer on duty, on a weekly rota.

- Handle incident reports
- Keep an eye on monitoring
- Keep things falling between chairs

# Operational Security in EGI

How to monitor the security status of the distributed sites?

Realization: we have an infrastructure to run computation jobs! Use that also for monitoring.

# Operational Security in EGI

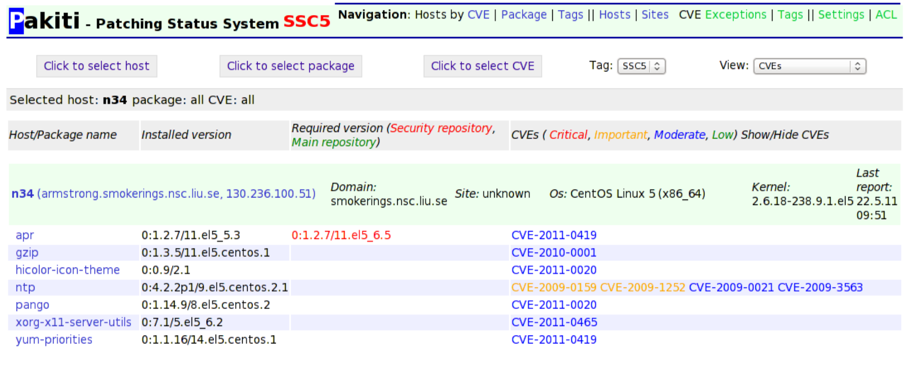
**Nagios**

- Monitoring jobs submit passive probe data into Nagios.
- Checks e.g. bad file permissions, vulnerable kernel modules.
- Used to quickly run custom tests across sites, e.g. to monitor CVE-2009-4033 which caused /var/log/acpid to be created with random permissions.

# Operational Security in EGI

## Pakiti

- Daily jobs dump the RPM data base and cross-checks against OVAL data.
- Web interface for monitoring, e-mail alerts for critical vulns.
- *Very* useful, but only gives results for a sample of the compute nodes at a site.



Pakiti - Patching Status System SSC5
Navigation: Hosts by CVE | Package | Tags || Hosts | Sites CVE Exceptions | Tags || Settings | ACL
Click to select host
Click to select package
Click to select CVE
Tag: SSC5
View: CVEs

Selected host: **n34** package: all CVE: all

| *Host/Package name* | *Installed version* | *Required version (Security repository, Main repository)* | *CVEs ( Critical, Important, Moderate, Low) Show/Hide CVEs* |
|---|---|---|---|
| **n34** (armstrong.smokerings.nsc.liu.se, 130.236.100.51) | *Domain:* smokerings.nsc.liu.se *Site:* unknown | *Os:* CentOS Linux 5 (x86_64) | *Kernel:* 2.6.18-238.9.1.el5 *Last report:* 22.5.11 09:51 |
| apr | 0:1.2.7/11.el5_5.3 | 0:1.2.7/11.el5_6.5 | CVE-2011-0419 |
| gzip | 0:1.3.5/11.el5.centos.1 | | CVE-2010-0001 |
| hicolor-icon-theme | 0:0.9/2.1 | | CVE-2011-0020 |
| ntp | 0:4.2.2p1/9.el5.centos.2.1 | | CVE-2009-0159 CVE-2009-1252 CVE-2009-0021 CVE-2009-3563 |
| pango | 0:1.14.9/8.el5.centos.2 | | CVE-2011-0020 |
| xorg-x11-server-utils | 0:7.1/5.el5_6.2 | | CVE-2011-0465 |
| yum-priorities | 0:1.1.16/14.el5.centos.1 | | CVE-2011-0419 |

# Operational Security in EGI

- What happens when we get an incident?
- What *is* an incident?

# Operational Security in EGI

- What happens when we get an incident?
- What *is* an incident?

*An [grid] incident is any real or suspected event that poses a real or potential threat to the integrity of [grid] services, resources, infrastructure, or identities.*

Anything can be labeled a grid security incident if you feel like it!

# Operational Security in EGI

The EGI incident response procedure is brief, but establishes a flat structure with maximum info sharing.

(It turns out professionally run CSIRTs have all sorts of privacy and disclosure policies that can hinder the information flow. You need to be adept at social engineering to be able to bypass that in clever ways[2].)

[2] Preferably without making lots of enemies

# Operational Security in EGI

Each incident is assigned an IRTF member as incident coordinator, who

- issues a heads-up warning to all sites
- works with the victim site to investigate the incident, possibly issuing additional all-sites broadcasts as new information is discovered
- coordinates the incident with other players (VOs, CAs, other CSIRTs, law enforcement, partner infrastructures. . . )
- makes sure a closure report is sent to all sites

# Operational Security in EGI

Total number of incidents involving grid technology:

# Operational Security in EGI

Total number of incidents involving grid technology: 0

# Operational Security in EGI

| | |
|---|---|
| EGI-20110418-01 | stolen ssh credentials |
| EGI-20110301-01 | bruteforce ssh |
| EGI-20110121 | web server misconfig |
| EGI-20111201-01 | bruteforce ssh |
| EGI-20101018-01 | bruteforce ssh |
| EGI-20100929-01 | stolen ssh credentials |
| EGI-20100722 | bruteforce ssh |
| EGI-20100707-01 | stolen ssh credentials/remote vulns in CMSes |
| EGEE-20091204 | stolen ssh credentials/X keyboard sniffing |
| GRID-SEC-001 | stolen ssh credentials |

# Operational Security in EGI

- Large majority of incidents due to stolen or weak ssh credentials
- We have no power to force sites to deploy e.g. two factor auth
- We do try to motivate sites to install important security patches, partly to offset the potential damage from user level intrusions

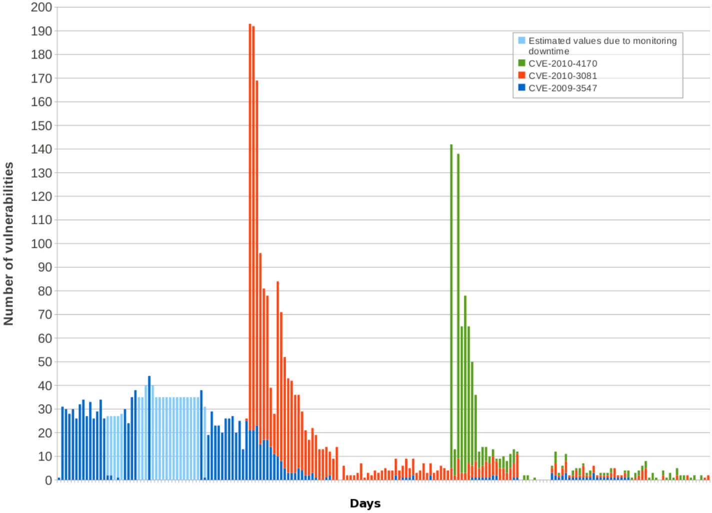
# Operational Security in EGI

- Security Intelligence Group (SIG) monitors public and non-public sources for new vulns
- The SVG Risk Assessment Team determines how serious new vulns are
- The EGI CSIRT and SVG produce detailed advisories that are broadcast to sites

# Operational Security in EGI

- When new serious vulns appeared we used to issue an advisory, watch Pakiti for a while to make sure sites applied patches, and then forget about it.
- This didn’t work; new vulnerable nodes keep appearing – bad config management, nodes that were under maintenance when patches were applied…
- We now continuously monitor for vulnerable nodes and slap them down as they appear.

# Operational Security in EGI



# Operational Security in EGI

Finally, we try to be good community members and maintain good relations with neighbouring CSIRTs at all levels.

Any questions, comments, feel free to contact me:

`nixon@nsc.liu.se`