EGI Incident Response Task Force

Leif Nixon

Coordinator, Incident Response Task Force

April 6, 2011

What has happened so far?

- Approximately 6–9 incidents (depending on how you count)
- 12 advisories issued
  - 3 critical
  - 6 high
  - 3 moderate

Incident sources

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

Incident sources

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

0 incidents related to grid middleware!

8 of 9 incidents are due to defeating ssh authentication.

Should we all quit our jobs?

I’ve said this before:

- *There ain’t no such thing as grid security.* A rooted system is a rooted system, no matter the entry vector.
- We’re not protecting the grid software – we’re protecting the infrastructure.

Unfortunately, breaking a single site can break the infrastructure.

Layered site defense

Root escalation

User level intrusion

Intrusion at neighbouring site

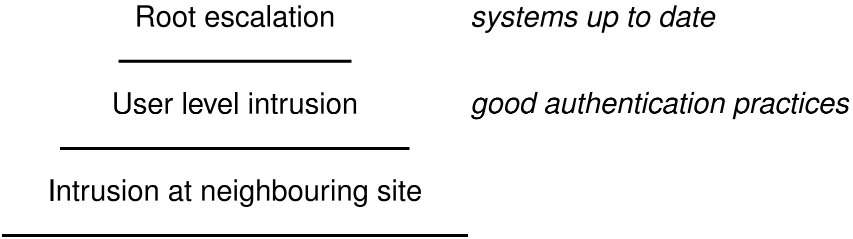
Layered site defense

Root escalation *systems up to date*

User level intrusion

Intrusion at neighbouring site

Layered site defense



Root escalation *systems up to date*

User level intrusion *good authentication practices*

Intrusion at neighbouring site

Layered site defense

Root escalation	*systems up to date*
User level intrusion	*good authentication practices*
Intrusion at neighbouring site	*good cooperation with other certs*

Layered site defense

Root escalation	*systems up to date*
User level intrusion	*good authentication practices*
Intrusion at neighbouring site	*good cooperation with other certs*

Good admin practices always help.

Good cooperation with other certs

- Take part in CERT networks; FIRST, TF-CSIRT, regional/national networks
- Share information as freely as possible (while respecting policies and legislation)

Good authentication practices

Currently, we mainly see two different authentication problems:

- *Bruteforce ssh attacks*
    - Random, non-targetted attacks
    - Usually single-site, single-machine incidents
    - Usually, the compromised account is a system account that was accidentally left exposed - not really a technical problem

Good authentication practices

Currently, we mainly see two different authentication problems:

- *Bruteforce ssh attacks*
  - Random, non-targetted attacks
  - Usually single-site, single-machine incidents
  - Usually, the compromised account is a system account that was accidentally left exposed - not really a technical problem
- *Stolen ssh credentials*
  - More or less targetted
  - Uses cleartext keys picked up from users' home directories, or passwords and encrypted keys stolen by trojan ssh clients
  - Usually multi-site. Can spread quickly through a community.

What can be done?

Scan file systems for unprotected ssh keys

- `# grep -L ENCRYPTED /home/*/.ssh/id_?sa`
- Mainly protects *other* sites, but does identify users with potentially troublesome habits

What can be done?

Scan file systems for unprotected ssh keys

- `# grep -L ENCRYPTED /home/*/.ssh/id_?sa`
- Mainly protects *other* sites, but does identify users with potentially troublesome habits

- **Cred theft** Offers some mitigation. Trojans are still a problem, but cred theft through trojans takes more time.
- **Bruteforce –**

What can be done?

Scan for weak passwords

- E.g. John the Ripper

What can be done?

Scan for weak passwords

- E.g. John the Ripper

- **Cred theft** –
- **Bruteforce** Some mitigation (but most common vector is admin mistakes that may not show up in a scan)

What can be done?

Move to soft certs

- Deploy e.g. gsissh

What can be done?

Move to soft certs

- Deploy e.g. gsissh
- **Cred theft** Some mitigation; but you may wind up with proxies lying around everywhere…
- **Bruteforce** Some mitigation (but most common vector is admin mistakes)

What can be done?

Hardware tokens

- Deploy e.g. Yubikey or SecureID

What can be done?

Hardware tokens

- Deploy e.g. Yubikey or SecureID
- **Cred theft** Much better (but beware of compromised auth servers)
- **Bruteforce** Some mitigation (but most common vector is admin mistakes)

What can be done?

Better admin practices

- **Cred theft** Some mitigation (discover trojans faster, avoid privesc)
- **Bruteforce** Better (avoid those admin mistakes)

What can *we* do about this?

The EGI CSIRT has little formal power when it comes to ssh auth problems. Hopefully these issues can at least be covered in training sessions.

Keeping sites patched

Patches are the last defense line against intruders.

- We are making good impact on re-apperance of *critical* vulnerabilities, at least.
- Still want to encourage better patching procedures. Why should any vulnerability remain unpatched after, say, 30 days?
- Metrics, metrics, metrics. Even if we can't get them into the metrics portal yet. What should we measure?
  - Average time to patch?
  - Number of unpatched vulnerabilities? Sum of their CVSS scores?

Better admin practices

- Facilities for rolling upgrades.
- Central log server.
- Readable log summaries that somebody actually reads.
- IDS
- Configuration management tools (Puppet/Quattor/Cfengine). Avoid node configuration drift.
- Configuration change procedures.

Again, we have little formal power, but can offer training. Perhaps encourage admins to go to HEPiX?

Random stuff

Encryption and signing

- X.509 vs. PGP
  - We have a nice PKI
  - But nobody else uses it
- Individual signatures or team key?
  - Public list of members?
  - No choice for X.509…

Random stuff

CSIRT chatroom

A CSIRT chatroom has been created on the EGI Jabber server.

See `https://www.egi.eu/about/intranet/jabber-howto.html` for instructions.

Name of chatroom: `csirt`
Password: same as IRTF weekly meeting

Keep the window open in a corner of your screen.

Random stuff

AOB

Comments? Questions? What are we doing wrong?