IRTF updated

Leif Nixon

NDGF security officer, EGI CSIRT

September 19, 2011

THE GOAL OF OUR ORGANIZATION IS TO MAKE YOUR SECURITY PROCEDURES SO INCONVENIENT THAT YOU GIVE UP HOPE AND DIE FROM BED SORES.

Security in the EGI era

- Approximately 8–12 incidents (depending on how you count)
- 15 vulnerability advisories issued
  - 3 critical
  - 7 high
  - 4 moderate
  - 1 low

Incident causes

EGI-20110809-01	NO	stolen ssh credentials
EGI-20110713-01	CA	stolen ssh credentials
EGI-20110418-01	IN	stolen ssh credentials
EGI-20110301-01	FR	bruteforce ssh
EGI-20110121	ES	web server misconfig
EGI-20111201-01	PK	bruteforce ssh
EGI-20101018-01	IT	bruteforce ssh
EGI-20100929-01	FI, DK	stolen ssh credentials
EGI-20100722	IT	bruteforce ssh
EGI-20100707-01	CERN, CA	stolen ssh credentials/ remote vulns in CMSes
EGEE-20091204	CH, DK, PL, DE, NL, BE…	stolen ssh credentials/ remote X keyboard sniffing
GRID-SEC-001	Most of known world	stolen ssh credentials

Incident causes

EGI-20110809-01	NO	stolen ssh credentials
EGI-20110713-01	CA	stolen ssh credentials
EGI-20110418-01	IN	stolen ssh credentials
EGI-20110301-01	FR	bruteforce ssh
EGI-20110121	ES	web server misconfig
EGI-20111201-01	PK	bruteforce ssh
EGI-20101018-01	IT	bruteforce ssh
EGI-20100929-01	FI, DK	stolen ssh credentials
EGI-20100722	IT	bruteforce ssh
EGI-20100707-01	CERN, CA	stolen ssh credentials/ remote vulns in CMSes
EGEE-20091204	CH, DK, PL, DE, NL, BE...	stolen ssh credentials/ remote X keyboard sniffing
GRID-SEC-001	Most of known world	stolen ssh credentials

0 incidents related to grid middleware!

11 of 12 incidents are due to defeating ssh authentication.

Identity crisis!

Passwords – stolen, reused by users across sites
SSH keys – stolen, can’t be revoked
One-time passwords – RSA hack
Certificates – Comodo and DigiNotar incidents

Technical Evolution Group

“To reassess the implementation of the grid infrastructures that we use in the light of the experience with LHC data, and technology evolution, but never forgetting the important successes and lessons, and ensuring that any evolution does not disrupt our successful operation.”

Technical Evolution Group

Security Technical Working Group

- Should review risk analysis – what are the real threats now? Where should we focus?
- Is the trust model still appropriate?
  - E.g. can we siplify the “glexec” issue?
- X509/VOMS/IGTF have been essential in having a world-wide use of resources
- But there are problems associated with proxies
- Can/should other federated ID management systems be integrated?

Technical Evolution Group

Security Technical Working Group

Probable outcome: more holistic perspective on site security.

Federated identities

- Lots of traction
- Can improve user experience wrt X.509
- Possible to revoked compromised credentials!

Federated identities

But what happens when an IdP gets compromised?

One thing is certain

We won’t be going out of business.