EGI CSIRT Procedure for Compromised Certificates and Criteria for central emergency suspension

Dr Linda Cornwall STFC/RAL

EGI CF13 OMB 12th April 2013

Contents

- Why a procedure?
- Types of Certificate which may be compromised
- Severity of compromise
- Emergency suspension criteria
- Summary of procedures

Plenty of time for questions and discussion

Why a procedure?

- When a situation occurs, and a certificate is compromised, CSIRT needs to have a procedure in place
  - Act in an agreed manner
  - Saves time, know what to do
  - Protects sites

At present draft still in work

NOT asking for approval today, probably next OMB.

CSIRT will meet 24-25th April, Finalize this document

Types of Certificate which may be compromised

- User certificate
  - Most common case
  - DN may undergo central emergency suspension
- Host or service certificate
- Robot certificate
  - DN may undergo central emergency suspension
- CA compromise

Central emergency suspension

Central emergency suspension framework allows for central infrastructure wide blacklisting of a DN, which is suspected of malicious use or to prevent malicious use

- Sites are protected quickly, e.g. during an incident which occurs out of hours
- Sites may run an Argus server, or download a list of suspended DNs and deploy alternative mechanism they know and control
  - Sites must do one or the other

A DN can be re-instated quickly

Central emergency suspension (2)

The need for emergency suspension to be carried by EGI CSIRT out is to protect sites against malicious and other mis-use

Most likely reason is the certificate is linked to malicious jobs or a security incident

- Including if jobs have been submitted which are unlikely to have been submitted by the owner/user

If the certificate has been used to submit jobs which are causing problems to the infrastructure

- Central emergency suspension may be carried out for operational reasons – NOT by EGI CSIRT

Central emergency suspension (2)

Other examples where central emergency suspension may be carried by EGI CSIRT out due to certificate compromise

- System containing proxies or private keys compromised
  - This is a type of incident
- Normal User certificate shared with others
- Usable private key or proxy copied to location readable by others, e.g. web page
  - Private keys should always be password protected
- User e-mailed proxy to mailing list with world readable archive
- Device stolen containing unprotected private keys, or potentially usable private keys

Central emergency suspension (3)

- Emergency suspension does NOT imply fault on the certificate owner's part
  - A system may have been compromised containing the certificate
  - A proxy may have been exposed by a vulnerability and used by a malicious user

Emergency suspension must be at CSIRT discretion, cannot think of all possible criteria. Use common sense.

User Certificate compromise

- Most cases of compromise are likely to be a User certificate
- EGI CSIRT decides what action to take
  - No action
    - e.g. mis-configuration or vulnerability which exposes proxies in limited way to other authz users - certificates probably not treated as compromised
  - User should revoke and re-apply
  - Full procedure, including emergency suspension

User Certificate compromise – revoke and re-apply

- User should revoke certificate
- User should remove any proxies from long term storage
- User should ask to be suspended by the VO
- User requests a new certificate
- User may ask to re-join a VO

User Certificate compromise

- Carry out emergency suspension of the DN(s)
- Inform sites and NOC managers
  - DN(s) suspended and why
- Revoke certificate(s)
  - If you have access to private key(s) revoke certificate(s)
  - User may revoke certificates

User Certificate compromise (2)

- Request revocation if applicable
  - CA likely to revoke certificates in case of root compromise where private keys are stored
- EGI CSIRT carries out incident response or any other investigation

Remove central emergency suspension if appropriate -when

- User has been contacted and co-operated
- Certificate has been revoked
- User has confirmed they are suspended from VOs
- Investigations are complete
  - Or progressed sufficiently for user to be re-instated
- 24 hours have passed since any exposed proxy has expired
- User has removed any long term proxies from storage (e.g. MyProxy)
- In the case of mis-use, action either not carried out by user or user can be trusted to act appropriately in future

User applies for new certificate

- User applies for new certificate
- User re-joins VOs.

Service Certificate compromise

Service certificates cannot be used to submit jobs, therefore simple procedure is enough

- Service provider shuts down service
  - This includes putting the service in downtime, stating security operations
- If compromise – jointly with EGI CSIRT follow the incident handling procedure

Service Certificate compromise (2)

- If necessary, suspend the service
- If cannot contact service owner
  - If CSIRT has private key CSIRT will revoke the certificate
  - If necessary suspend site, e.g. if a security incident is suspected at site
- After any appropriate investigations
  - Service provider may apply for new certificate
  - Service provider may restore service

Robot certificate compromise

- Rare, we hope
- Similar to compromised user certificate
  - Including emergency suspension of the robot DN
  - Robot owner will need to inform users that the portal is not available
  - Robot owner will need to actively investigate, along with the CSIRT
  - Until resolved, all users dependent on that Robot will not be able to submit jobs

CA compromise

- We hope this will never happen, but we should define what happens if it does
- If a member of CSIRT suspects a CA has been compromised –
  - Alert the CA
  - Alert the IGTF
  - Alert the EUGridPMA or other appropriate regional authority

CA compromise (2)

- EGI CSIRT does NOT need to do anything
- The IGTF will handle this:
  - Including broadcasts to sites
  - Re-issuing of trust anchors
- All Users with Certificates from that CA will not be able to submit jobs until resolved
- Similarly sites authenticating with that CA will be out of action

Comments, questions, discussion

- ??

Notes.