PASSTORE: safe certs & password management for Grid hosts

Stefano Dal Pra
INFN
stefano.dalpra@pd.infn.it

www.eu-egee.org

Information Society and Media

The problem

- **A comfortable practice to manage Grid certificates for hosts would be to keep them all in a local host and scp them as needed**
  - In case of security incident at site level, all certs may become compromised at once.
  - CA explicitly requires to keep two separete copies for each cert/key pair in a place not reachable via network
- **A secure practice would be to keep them on two pendrives or similar devices**
  - Difficult to maintain them syncronized
  - Extreme care needed for safe management (stoling content may be quite easy)

The passtore solution

- **Keep certs/keys and passwords on a single host with:**
  - Two HD in RAID1 (two separate copies for each file)
  - Mysql DB using AES (simmetric) encryption
  - Private IP, Network interface down
    - only direct console access or through Avocent or alike (video stream directly from graphic card)
  - Iptables, no rules, policy DROP (no traffic allowed)
  - direct Network connection with another host who masquerades him
- **When passtore needs to scp a file it:**
  - Activates proper iptables rule (passtore,ssh --> target)
  - Activates network
  - Performs actual scp
  - Deactivates iptables rule and network

The passtore solution (2)

- **Use a python Command Line tool to:**
  - add/show/update passwords for user@<host[s]>:<service>
  - Produces cert requests (and stores the private key in encrypted form)
  - Query for status of stored certificates
    - Validity dates
    - Verify that Private key matches its certificate
    - Prevents insertion of nonmatching certs
  - copy the cert request file to the operator's host, who will mail it to the CA
  - Gets the new released certificate from operator's host and stores it in the DB
  - copy a couple key/cert to the target host (only)

Further details...

- **See https://forge.cnaf.infn.it/projects/passtore/**
  - Svn source repository
  - Reserved access
  - Write to stefano.dalpra@pd.infn.it if interested

Thanks for attention

Key points

- **Passtore is NEVER network reachable**
  - Network gets activated for the strictly needed time only
  - Connection started ONLY from passtore to target host
- **User cannot (directly) take a copy of a private key**
  - When copying to Grid host passtore knows remote password
- **Examples (next slide)**