CREAM and proxy renewal

Paolo Andreetto, INFN
JRA1-SA3 AH, Prague

Previous situation

- **BLAHP moves the proxy from the CE to the WN using a secure channel**
- **One BPR server is running on the WN for each submitted job (predefined port range)**
- **Drawbacks:**
  - Problems with firewall and IDS
  - Deployment of the BPR server on the WN

Requirements

- **Basic requirements:**
  - Proxies must be downloaded from the CE, or other services of the site, into the WN
  - A stolen proxy must not be renewed
- **A new security mechanism must be used whenever the proxy is stolen (two factor AuthN/AuthZ)**
  - Shared secret (security token) between the CREAM service and the jobwrapper

Temporary solution

- Proxies are copied into a gridFTP area of the CE
- The jobwrapper downloads the new proxy using a secure channel before the expiration
- A cracker with a stolen proxy can access the gridFTP area on the CE (proxies cannot be hidden)

Long term solutions (1)

- **Installation of a myproxy server on the CE**
- **Drawbacks:**
  - Duplication of the repository (myproxy and delegation back-end)
  - New dependency on Globus and changes in the CE metapackage
- **It has to be investigated how to prevent the renewal of a stolen proxy**

Long term solutions (2)

- A CREAM servlet accesses the delegation back-end
- The jobwrapper sends a HTTP GET request to the CREAM service using htcp for downloading the new proxy
- The servlet uses the CE AuthN/AuthZ layers (trustmanager, gJAF)
- One of the parameters of the request is a security token created by CREAM and hard-coded setup in the jobwrapper
- It can be implemented in a short time
- The tool htcp must be installed in the WN

Long term solutions (3)

- **The reverse delegation service is an extension of the current delegation service (same back-end)**
- **It provides a pullProxy operation**
- **The jobwrapper contacts the WS on the CE sending a proxy certificate request and receiving a proxy certificate chain**
- **No private key is moved from the CE to the WN**
- **A special client must be installed in the WN**
- **A shared secret can be:**
  - Exchanged in the soap message (WSS header)
  - Embedded into the proxy itself

Links

- **http://grid.pd.infn.it/cream/field.php?n=Main.ProxyRenewalWithServlet**
- **Reverse delegation ASAP**