Security Area

Christoph Witzig (SWITCH)

on behalf of John White (HIP)

Overview of Work

- Maintenance
  - of existing security components
- Harmonization
  - Common authN library
  - Common profiles (SAML, XACML)
  - Common authorization service
- New Stuff:
  - Easier credential management

Maintenance – gLite (1)

- Java Delegation service:
  - coordination with EMI-ES
- MyProxy, Proxy Renewal, GridSite, gSoap, ...
  - By CESNET
- Site access control:
  - gLExec → add support for PAM module (e.g. Argus)
  - LCAS/LCMAPS/EES: convergence of code
- Reduction of components:
  - Generally hard to drop entire components
    - Code reduction often more feasible
  - Trustmanager, java-util → common authN library

Maintenance – gLite (2)

- Confidentiality Services:
  - Hydra:
    - will be released in an EMI-1 update cycle
    - New tests, documentation, vulnerability assessment
  - Pseudonymity service:
    - Refactoring, certification, release Q4 2011
- VOMS:
  - VOM(R)S convergence
  - Third-party attribute queries

Maintenance – ARC and Unicore

- ARC:
  - Support according to user requests
  - Nordugridmap, arcproxy: adapt to possible changes in VOMS
  - Recover LCAS/LCMAPS support
- Unicore
  - Refactoring of security PT (done)
  - Optimization of security stack
  - Support for resource sharing

Harmonization (1)

- Common authentication library
  - APIs for C, C++, Java done
    - (almost) all internally reviewed
  - PT must be formed (TBC)
    1st release Feb 2012
    - Java: UNICORE security PT
    - C: NIKHEF, additional manpower needed
    - C++: ARC
  - Note:
    - Assumption: Most code taken from existing libraries
    - Reach-out to other PT needs to be done

Harmonization (2)

- Common SAML profile:
  - Defined
  - Implementation in VOMS, 1st use by UNICORE
- Common XACML profile:
  - Defined
  - Support by Argus
  - Use by CREAM, UNICORE, ARC

Harmonization (3)

- Common authorization service
  - Use of Argus
  - Today: gLExec, global banning
  - Support in CREAM and data management (DPM, LFC) added
  - Coming: Support in ARC and UNICORE (→ common XACML profile)
  - New feature: Argus EES

Support for AAIs

- EMI AAI WG:
  - Easier credential management for non X.509 users
  - Support for AAIs and Kerberos
  - Late start of activity due to other priorities

- Security Token Service (STS)
  - To translate tokens into another format
    - SAML / Kerberos → X.509
  - Brokers trust between different security domains
  - Generic for all kinds of tokens, standards-based interface (WS-Trust)
  - Current plan to base on Shibboleth IdP v3
  - Reach-out to other related efforts

Vulnerability Assessment

- Work done by E.Heymann, UAB, w/collab. UWM
- Components assessed:
  - VOMS Admin 2.0.18 → vulnerabilities fixed
  - gLExec 0.8 → vulnerabilities fixed in EMI-1
  - Argus 1.2 → no vulnerabilities found
- Components to be assessed:
  - VOMS core (2.0.2) started
  - To do: CREAM, WMS, Target System Interface, Gateway
- UAB cannot assess every component → security training for SW developers

Further Information

- EMI JRA1 security Wiki: https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4Security

- DJRA1.3.2: Security Work Plan

Thank you!

EMI is partially funded by the European Commission under Grant Agreement RI-261611