EMI Security model and the future in Clouds.

John White, Helsinki Institute of Physics for EMI Security Team.

ISGC 2013, Academica Sinica, Taipei
Contents

- Grid Security.
  - General principles.
- EMI project.
  - EMI common security efforts.
- Clouds.
  - Commercial.
- Grid middleware with Clouds.
  - Example.
“A collaboration & resource sharing infrastructure. A computing fabric spread over heterogeneous resources”

- Grid resources (compute/data storage/network) are owned by institutes/universities/centers.
  - Someone is responsible.
- Resources are contributed to a Grid.
  - Used by a Virtual Organization (VO).
  - Resource usage agreed with the VO.
  - VO membership administrated (VOMS).
  - Policies on resource usage drafted.
- A Grid user must be trusted before they can use Grid resources.
- A Grid site must be trusted to agree to a set of operational policies.
- The Grid software (middleware) must be trusted to run on a resource.
• **EMI project combines ARC, gLite and UNICORE stacks.**
  - Security models are similar but not identical.
    - gLite, ARC based on X.509 credentials for AuthN/AuthZ \(^1\).
    - UNICORE uses X.509 for AuthN, “SAML” attributes internally.

• **Opportunity to improve user experience, inter-operation.**
  - Simplified credential handling.
  - Common Authentication libraries.
  - Common XACML profile.
  - Common Authorization system.
  - Common SAML profile.
  - Common Delegation method.
  - Gateway to virtualized clusters - Argus-EES.

---

\(^1\) AuthN - Authentication (who you claim to be)
AuthZ - Authorization (what you may(not) do)
Security Token Service (STS) “authorizes and authorizes” users based on security tokens.  

- Aggregates the required information from external sources.
  - eg. The Identity Provider (IdP)
- Establishes a trust relationship between different security/application domains.
  - eg. Institute login → VO VOMS.
- The first STS version supports the ISSUE operation that transforms an incoming security token into another security token.
  - Incoming formats: Username/Password, SAML
  - Outgoing formats: X.509 – using external online CA, X.509 Proxy –exploiting VOMS

- UNICORE STS client.
- STS pilot service for WLCG.
  - Username/Password to VOMS proxy through CERN IdP.

2 Security token: a collection of statements (or claims) about a user or resource, in this case: X.509 certificate, SAML assertion, Kerberos ticket, Username/Password
● Noted EMI services used differing AuthN methods.

● **Strategy to provide and integrate Common AuthN libraries (CANI)**

● Provides a uniform layer for AuthN decisions.
  – C, C++ and Java libraries.
  – Testing follows standards\(^3\).
  – Provides a common library set to handle e.g.
    ▶ SHA2 signed certificates.
    ▶ RFC proxies.
    ▶ Longer default key lengths.
    ▶ OCSP, CRL renewal etc.
  – Delivered for EMI-2.

● Integrated to many EMI services.

---

\(^3\) [http://csrc.nist.gov/groups/ST/crypto_apps_infra/pki/pkitesting.html](http://csrc.nist.gov/groups/ST/crypto_apps_infra/pki/pkitesting.html)
For common AuthZ service there must exist a common set of attributes for authorization decisions.

- Allows writing standard AuthZ schemes for services.
- Includes obligations that enrich response beyond “yes/no”

Adoption:
- Argus PAP, PEP Server update to support Common XACML profile.
- UNICORE (USE) PDP callouts to Argus PAP.
- ARC HED Security Handler callouts to Argus PEP Server.
- Also ARC HED direct communication to Argus PDP.

More information: https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4XACML
A common AuthZ system. Argus. XACML policy engine.

4 Courtesy C. Witzig V. Tschopp, SWITCH
Currently integrating UNICORE security with VOMS-SAML and Argus.

UNICORE client fetches attributes from VOMS-SAML.
  – ➔ Latest VOMS-SAML implements the profile.

UNICORE integrates with Argus.
  – ➔ Support for extracting attributes from SAML assertion implemented in Argus.
  – ➔ Argus SPL extended to express equality checks among XACML attributes.

Agreement on common method to delegate X.509 proxies.

- Participation: ARC and gLite, (compute, data and security)
- gridsite delegation retained. No show-stoppers.
- Will proceed to form an OGF group.

More information: [https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4DelegationInEmi](https://twiki.cern.ch/twiki/bin/view/EMI/EmiJra1T4DelegationInEmi)
Argus EES

- “An obligation transformer used to ensure that an appropriate site-specific execution environment is procured based on the site-agnostic obligations and input attributes”.
- A service that may co-exist with Argus to start VMs or send jobs to a Cloud*.
  - Argus-EES ready for EMI-2.
  - Tested with Argus. (PEPd)
  - OpenNebula will come as update for EMI-2
- No show-stoppers.

http://www.eu-emi.eu/products/-/asset_publisher/z2MT/content/argus-ees
Grid Security

In summary... on Grids...

- **The resource owner:**
  - Knows users accessing their resource(s) (AuthN).
  - Allows/denies user actions on their resource (AuthZ).

- **The Virtual Organization:**
  - Knows who is acting in their VO.
  - Can suspend membership.
  - Can deny access to VO resources.

- **The Grid user:**
  - Knows their job/data is going to a “properly run site.”
  - Can avoid sites if necessary

---

\(^5\) Not strictly done in security software.
Cloud computing is for the information age what electrification is for industrial age.
“...in the end, the saving offered by utilities become too compelling to resist, even for the largest enterprises...”

Cloud computing will be “no less influential than ebusiness”
- Gartner 2008

Cost advantages of Cloud Computing will be 3 to 5 times for business applications and more than 5 times to consumer applications.
- Merrill Lynch 2008

Cloud computing is more attractive in the economic downtown
- IDC 2008

Cloud computing could become the fundamental approach towards Green IT*
- Who?
Commercial Cloud Computing

• **Definitions by analyst firms.**
  
  – A style of computing in which massively scalable IT-related capabilities are provided “as a service” using internet technologies to multiple external customers.
    - Gartner 2008
  
  – An emerging IT development, deployment and delivery model, enabling real-time delivery of products, services and solutions over the internet.
    - IDC 2008
  
  – “the idea of delivering personal and business productivity applications from centralized servers.
    - Merrill Lynch 2008

• **Academic world...**
  
  – Something we can’t afford.
    – So far CERN physicists in general.
  
  – Private Cloud... virtualization technology on a cluster?
    – Most academic computing sites.
• **What is Cloud Computing? What do you need?**
  – email address.
  – mobile telephone/laptop.
  – VISA/PayPal etc.

• **Companies build enough capacity to handle the peaks.**
  – Virtualization allows companies to optimize their data/compute.
  – Spare capacity can be sold or switched off.
  – Sell “X”aaS to anyone (for enough $).

• **Virtualization. Where does it come from?**
  – The basic idea to run a different O/S while not touching the underlying system.
  – e.g. Running Windows inside a Linux box... Wine.

• **Clusters may become flexible... saves costs... more profit.**

• **Where does “security” come into this?**
Cloud Security

- **On commercial providers... security:**
  - Terms of use etc. Heavily weighted to the provider.
  - Data... no guarantees of who can see.
  - Data... no guarantees of where... e.g. National data acts.
  - Provenance of who runs/owns the infrastructure unknown.

- **On Academic (virtualized) clusters:**
  - Limits of the cluster are known... no different than a Grid site.
  - Data... site staff may see data.
  - Data... should be stored on site.
  - Provenance of who runs/owns governed by policies.

- **General observations:**
  - If there are data security concerns, don’t use a “Cloud”.
  - Otherwise, encrypt, encrypt, encrypt, encrypt!
Data encryption on a Grid

General Standalone scheme.

- gLite/EMI solution.
- Key generation in client.
- (De)Encryption in memory.
- GFAL-enabled clients.
Secure InterCloud eXchange (SICX)

- Multi-cloud storage without vendor and data lock-in.
- Data striped in similar manner as encryption keys.
- Hydra clients re-written in Java.
- Simpler Hydra service created for evaluation.
- STS to hide X.509 credentials.
- Cloud benchmarking used.

Complete proof of concept system demonstrated to Finnish Technology Funding agency, June 2012 In preparation for pilot with Geneva canton, CH.
Clouds and Grid MW
Information in this talk is given in far greater detail in:

- **EMI Milestone document MJRA1.12**
  “EMI Security Architecture”
  https://twiki.cern.ch/twiki/bin/view/EMI/MilestoneMJRA112

- **EMI Deliverable document DJRA1.3.4**
  “Security Area Work Plan and Status Report”
  https://twiki.cern.ch/twiki/bin/view/EMI/DeliverableDJRA134

Documents in work but ready for EMI PM36 (April 2013).

Any other questions: John.White@cern.ch
Questions?

Thank you!

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