KoM WP3 Task3.2
Overview and Next steps

Yuri Demchenko
University of Amsterdam
Task 3.2 Development of Security and Access Control Mechanisms in a Multi-cloud Federated Environment [M2-M24]

Task leader: Yuri Demchenko (UvA)

- Mechanisms to be developed should allow users to access all federated resources using their home institution account
- Develop appropriate trust and identity management mechanisms
Task 3.2 Activity Details (from DoW)

- Design and implementation of federation mechanisms at the IaaS level that will allow cloud inter-provider federation
- Usage scenario: Independent private cloud providers (members of a federation) that share the same API can reserve/allocate part of their resources to be used in a communal pool of resources (aka distributed community cloud) that can be used any user belonging to the federation.
  - Actually re-use/re-factor Grid VO model
- The mechanisms to be developed should enable federated access control and resource management
  - Authentication, authorization and auditing
  - Resource allocation prioritization - Control & signaling?
  - Support lightweight decentralized business models
    - Evaluate brokered federation operation and management
- Leverage the experience with similar systems, such as the JiT Cloud and OurGrid middleware whose development are led by UFCG
Task 3.2 interaction with other tasks

- Task 3.1 Operation and Support of the Production Infrastructure [M1-M24]
- Task 3.2 Development of Security and Access Control Mechanisms in a Multi-cloud Federated Environment [M2-M24]
- Task 3.3 Adaptation and Deployment of Cloud Federation Mechanism [M1-M24]
- Task 3.4 Exploitation of Shared Resources in an Opportunistic Federated Cloud [M1-M24]
- Task 3.5 Adaptation of CSGrid middleware [M1-M24]

- Task 3.2 will contribute with the security analysis and taxonomy [M2-M?]
- Task 3.2 expect to receive from other tasks use cases and scenarios [M?-M?]
- Task 3.2 jointly with other tasks will specify requirements and define security/access control policy [M?-M?]
- Security interface definition, to be implemented by applications
- Security mechanisms developments
- Security mechanisms integration
Interaction with other WPs

- Should be done via general WP3 interaction
- WP3 <-> WP5 Use cases
How to enable effective collaboration?

- Knowing involved people
- Planning work
- Interaction
- Common development platform
Deliverables and Milestones: Security Issues need to be addressed

- MS3.1: Infrastructure configured to allow access to users and developers of EUBrazilCC (M3)
  - All application users and system developers with access to a minimal part of the infrastructure that allows them to use it for their needs
- MS3.2 Deployment of opportunistic private cloud (M12)
  - Prototype able to connect desktops within a LAN to a private cloud in an opportunistic way
- MS3.3 Deployment of federation mechanisms (M16)
  - Prototype able to connect IaaS providers that share the same API using the Network of Favours incentive mechanism

- D3.1 Adaptation Requirements for CSGrid Middleware (M6)
- D3.2 Infrastructure Assessment Report (M12)
- D3.3 Prototype of the CSGrid Adaptation Mechanisms (M12)
- D3.4 Implementation of the Mechanisms to Federate Clouds and Exploit Shared Resources Opportunistically (M16)
- D3.5 Final Infrastructure Assessment Report (M24)
Initial Steps in Security Development

- Define what to protect
  - IaaS infrastructure or separate Compute, Storage, Network
  - Cloud applications
  - Collaborating user community

- Identify/specify used protocols
  - Cloud management protocols: OCCI, CDMI, OVF
  - Grid resources access and management: SE, CE, VOMS, SLCP

- Legacy security solutions and migration strategy
  - Grid on clouds vs native cloud solutions
  - VO based vs Cloud Identity Federation model

- Access control models and policy platform/profile
  - RBAC/ABAC, Identity Federation/Delegation, Security Token Service, Trust establishment and delegation
Federated Identity and Delegation in Clouds

- Existing federated identity schemes can be used to create consistent authentication between distributed computing resources (specifically cloud infrastructures) and a user/client
  - VOMS and (X509 Proxy Certificate or SAML VOMS credentials)
  - Shibboleth (with SAML assertions)
  - ABFAB and Moonshot project (Federated IdM and Trust Management)
  - CILogon and InCommon Federation (in US)
  - OpenID and similar services

- Identity Federation in clouds
  - EGI Identity Federation
  - OpenStack KeyStone Identity Broker/gateway
  - AWS Identity and Access Management (IAM)

- Traditional approach in clouds requires the Cloud Service Provider (CSP) to be involved into federation establishment
  - Need to limit CSP role to an initial Trusted Introducer
  - Avoid CSP role as (identity) broker or (authorisation) gateway
Federation in Grid and Clouds: Grid VO vs Cloud Virtual Infrastructure

Grid federates resources and users by creating Virtual Organisations (VO)

- VO membership is maintained by assigning VO membership attributes to VO resources and members
- Resources remain under control of the Grid Resource Centers
- Users remain members of their Home Organisations (HO)
  - AuthN happens at HO or Grid portal
  - To access VO resources, VO members need to obtain VOMS certificate
  - X.509 Proxy Certificate is used to AuthZ users/jobs at Grid resources

In clouds, both resources and user accounts are created/provisioned on-demand as virtualised components/entities

- User accounts/identities can be provisioned together with access rights to virtual resources
Cloud Federation – Scaling up and down

- Scalability is one of the main cloud feature
  - To be considered in the context of hybrid cloud service model
    - Cloud burst and outsourcing enterprise services to cloud
    - Cloud services migration and replication between CSP

- Scaling up
  - Identities provisioning
  - Populating sessions context

- Scaling down
  - Identity de-provisioning: Credentials revocation?
  - Sessions invalidation vs restarting

- Initiated by provider and by user/customer
Discussion how to proceed

- Who is involved?
- Design and development team cooperation
Supporting material

- Federated Identity and delegation
  - Approach and tools
- Multi-tenant Access Control for Cloud Infrastructure Services
- GAAA-TK (Generic AAA Toolkit)
  - Security context and session management, delegation
  - Policy and attribute profiles
  - Policy management and evaluation
- Federation in clouds and Intercloud Federation Framework (ICFF)
  - Operational models and components
- Intercloud Architecture Framework (ICAF)
  - Multilayer Cloud Services Model (CSM)
  - ICCMP, ICFF, ICOMF, ICSF (Intercloud Security Framework)
Basic Cloud Federation model – Combined User side federation

Simple/basic scenario 2: Federating Home Organisation (HO) and Cloud Service Provider (CSP) domains

Cloud based services created for external users (e.g. website) and managed by Customer 1

Involved major actors and roles

- CSP – Customer – User
- IDP/Broker

Cloud accounts A1.1-3 are provisioned for each user 1-3 from HO with 2 options

- Individual accounts with new ID::pswd
- Mapped/federated accounts that allows SSO/login with user HO ID::pswd

Federated accounts may use Cloud IDP/Broker (e.g. KeyStone) or those IDP-Xa created for Service Xa

User side Federation

IDP-Xa can be implemented as instantiated service of the CSP IDP
Basic Cloud Federation model – Federating CSP’s/multi-provider cloud resources

- Cloud provider side federation for resources sharing
- Federation and Trust relations are established between CSP’s via Identity management services, e.g. Identity Providers (IDP)
  - May be bilateral or via 3rd party/broker service
- Includes translation or brokering
  - Trust relations
  - Namespaces
  - Attributes semantics
  - Policies
- Inter-provider federation is transparent to customers/users

Provider side Federation
Authorisation in a Federated Cloud Environment

- PEP (Policy Enforcement Point)
- PDP (Policy Decision Point)
- PAP (Policy Authority Point)
- CVS (Credentials Validation Service)
GAAA Authorisation Framework and GAAA Toolkit (GAAA-TK)
GEYSERS project Network+IT IaaS infrastructure provisioning Security Infrastructure

• Logical Infrastructure Composition Layer (LICL)
  – FUSE ESB env, OSGi bundles
  – Packages: AuthN/AuhZ and Dynamic Access Control Infra (DACI)
• Network Control Plane (NCP+)
  – AuthnSvc&AuthzSvc Web services
  – SecurityGateway library
• GAAA Toolkit Java Library provides core functionality
  – GAAA-ISOD profile (Infrastructure Services On Demand )

AAI Components

Integration (via SecurityGateway)
Dynamic Access Control Infrastructure (DACI)

- DACI: Dynamic Access Control Infrastructure
- DACS: Dynamic Access Control Services

**Common Security Service Interface (CSSI)**

- **SecurityGateway**

**DACS instance[i]**

- Authentication Authority
- Attribute Authority
- Attr DB
- Identity Management Service

**Identity Management Service**

- SAML-XACML Layer
  - PIP (Authz Ctx Hdlr)
  - Obligation Handler
  - PDP
  - PAP

**Authorization Service**

- Authz-token Svc
  - Authz-token Authority
  - Authz Token Service

**DACI Management**

- DACI Configuration
- DACI Monitoring
- DACI Policy Management
- DACI Context Management
- DACI Trust Management

**DACS Trust Manager**

- Provisioned on demand security services (DACS)

**Update authz-policies upon reconfiguring Virtual Infrastructure**

**Dynamic Trust Establishment: DSA, Bootstrapping**

**Consolidate a common interface to access security services**

**KoM EU Brazil CC 12-14 Feb 2014**

WP3 Task 3.2 Federated Access Control
Security Services Reference Model

- Common Security Service Interface (CSSI)
- Dynamic Access Control Infrastructure (DACI)
- Trust establishment protocol for VI, Dynamic Security Associations (DSA), bootstrapping protocol

Common Security Service Layer
- Authentication & Identity Man.
- Authorization & Policy Man.
- Security Context Management
- Trust Management (Dynamic trust establishment, Bootstrapping)
- SLA Management

Note: Integration with SLA management/negotiation is needed to ensure consistency
Multi-tenant Access Control for Cloud Infrastructure Services

- Apply MT-AC in hierarchy
  - A high-level provider is a tenant of the low-level provider
  - Grant permissions -> Delegate granted permissions
  - Security context management using tokens as session credentials

Exchanging tokens in Intercloud

MT-AC in hierarchy

- User
  - (1) authz request
  - (2) grant token
  - (3) grant token
  - (4) access token
  - (5) request | access token
  - (6) response

- P_a domain
  - P_a Authz Service
    - C_a

- P_i domain
  - P_i Authz Service
    - C_i

- P_i Resource Service

- P_a
  - P_b1
  - P_b2
  - P_bk

- P_c1
- P_c2
GAAA-TK Implementation for complex infrastructure provisioning (GEYSERS project)
InterCloud Architecture Framework (ICAF)

◎ Multi-layer Cloud Services Model (CSM)
  ◎ Combines IaaS, PaaS, SaaS into multi-layer model with inter-layer interfaces
  ◎ Including interfaces definition between cloud service layers and virtualisation platform

◎ InterCloud Control and Management Plane (ICCMP)
  ◎ Allows signaling, monitoring, dynamic configuration and synchronisation of the distributed heterogeneous clouds
  ◎ Including management interface from applications to network infrastructure and virtualisation platform

◎ InterCloud Federation Framework (ICFF)
  ◎ Defines set of protocols and mechanisms to ensure heterogeneous clouds integration at service and business level
  ◎ Addresses Identity Federation, federated network access, etc.

◎ InterCloud Operations Framework (ICOF)
  ◎ RORA model: Resource, Ownership, Role, Action
    ◎ RORA model provides basis for business processes definition, SLA and access control
  ◎ Broker and federation operation

◎ Intercloud Security Framework (ICSF)
  ◎ Dynamic Security Infrastructure provisioning and protocols
Multilayer Cloud Services Model (CSM)

http://www.ietf.org/id/draft-khasnabish-cloud-reference-framework-06.txt

CSM layers

(C6) User/Customer side Functions
(C5) Intercloud Access and Delivery Infrastructure
(C4) Cloud Services (Infrastructure, Platform, Applications)
(C3) Virtual Resources Composition and Orchestration
(C2) Virtualisation Layer
(C1) Hardware platform and dedicated network infrastructure
General use case for infrastructure provisioning:
Workflow => Logical (Cloud) Infrastructure

Enterprise/Scientific workflow
Is mapped to heterogeneous cloud infrastructure containing IaaS, PaaS components
General use case for infrastructure provisioning: Logical Infrastructure => Network Infrastructure (1)

Distributed heterogeneous cloud infrastructure requires separately provisioned network infrastructure that can be outsourced to Cloud Carrier
General use case for infrastructure provisioning: Logical Infrastructure => Network Infrastructure (2)

Provisioning network infrastructure may involve multiple providers
Introducing OCX (Open Cloud eXchange)
Intercloud Federation Infrastructure and Open Cloud eXchange (OCX)

OCX Services

Trust Broker
Broker
(Federated Cloud Instance Customer A (University A))
Broker
(Federated Cloud Instance Customer B (University B))

Cert Repo (TACAR)
TTP Trusted Introducer
FedIDP

Cloud Service Broker
Discovery Directory (RepoSLA)

Directory (RepoSLA)

OCX and federated network infrastructure

Gateway AAA
(I/P/S)aaS Provider
IDP

Gateway AAA
(I/P/S)aaS Provider
IDP

Gateway AAA
(I/P/S)aaS Provider
IDP

Gateway AAA
(I/P/S)aaS Provider
IDP

Federated Cloud Instance Customer A (University A)
Federated Cloud Instance Customer B (University B)
OCX Hierarchical Topology Model

CSP

GEANT

NREN

University

DFlow

IP/L3

L2

L1

L0

VR3

VR4

VR5

VR6

VR7

OCX

VR3

VR4

VR5

VR6

VR7

OCX

Visualisation

User

CE

VR3

VR4

VR5

VR6

VR7

OCX

Visualisation

User

CE