Toward a Dynamic Trust Establishment Approach for Multi-provider Intercloud Environment

Canh Ngo, Yuri Demchenko
{t.c.ngo, y.demchenko}@uva.nl

System and Network Engineering Group
University of Amsterdam
Agenda

• Motivation

• Trust Management Challenges

• Trust Model
  – Attribute-based Trust approach

• Application
  – Dynamic Trust Establishment for Intercloud
  – Trust Evaluation Engine

• Conclusion and Future work
Intercloud use-cases

- Enterprise IT infrastructure migration
- Large project-oriented scientific infrastructures
- IT infrastructure disaster recovery
Motivation

Intercloud Properties

• Communication between Cloud providers/applications
  – Vertical integration: different service layers
  – Heterogeneous: cross-domains, composite services
• Distributed, public data access environment
• Data/resources are off-premise
• RORA*: cloud resource ownerships
  – Physical ownership
  – Management/brokering ownership
  – Subscription/consumption ownership

*RORA: Resource, Ownership, Role, Action (GEYSERS project)
Challenges

• Distributed multiple security domains
  – Authorizations based on identities are not applicable
  – Attributed-based access control (ABAC): different attributes profiles at domains

• Clouds composed from multiple providers
  – Authorization for “unknown” entities ("know implicitly")?
  – Relations between Cloud providers: dynamic, established on Cloud provisioning lifecycles

• Approach: Trust Management for distributed, public environment
  – Attribute-based, attribute semantics can be transformed between domains
  – Multiple levels of delegations
  – Dynamic trust-chain establishment
  – Efficient attribute-based trust evaluation implementation
Trust Model

- **Entities**
  - Cloud Providers
    - Physical Cloud Providers: PIP
    - Intermediate Cloud Providers: VIP, Cloud Broker
  - Cloud Clients
  - End-users/applications

- **Trust**
  “the belief of trustor in trustee to behave reliably, securely in a specific context”

- **Trust relationships**
  - **Properties:**
    - Asymmetric
    - Contextual
    - Time-constraint
  - **Types:**
    - Direct trust relationships
    - Indirect trust relationships
Trust Model

Trust Mechanisms(1)

• **Trust decisions**
  – Simple: binary (trust, distrust)
  – Complex: trust predicates

• **Attribute-based trust policies**
  – Attributes to describe trust context
  – Policy actor, policy target, policy context
  – Formal logic formula:

\[
X = (x_1, x_2, ... x_n); x_i \in P_i
\]

\[
f(X) = \bigwedge_i \left[ \bigvee_j \left( \bigwedge_k m_k \right) \right]
\]
Trust Mechanisms (2)

- **Direct trust relationships**

  - Attributes:
    \[ X = (x_1, x_2, \ldots, x_n); x_i \in P_i \]

  - Attribute-based trust policy:
    \[ f_{actor}(target, X) \rightarrow pred \]

  - Actor, target: entities
  - \( X \): attribute-based context
  - pred: predicates (e.g. trust, distrust, etc)
Trust Mechanisms(3): Delegation

- Indirect trust relationship?
- Delegation
  “Transferring part of the ownership (i.e., right to control as defined by the policy/administrative context) from the trustor to the trustee”
- Trust credential issuer policy
  \[ f_{\text{trustor}_B}(\text{trustee}_A, X) \rightarrow tc^X_B \]

  tc: trust credential: 
  \{trustor, trustee, context\}

- Delegation policy
  \[ f^{d}_{\text{trustor}}(X) \rightarrow \{\text{targets}\} \]

  X – trust context
  d – abbrev. for delegation targets – Id/trust_anchors of recommenders (e.g. B)
Trust Mechanisms(4): Delegation

- Example:
  "B delegates A to access (r,w, etc) cloud resource X at C"

- At A: access context description X

- At B: $f_B (A, X) \rightarrow t_{C_B}^{XA}$

- At C:
  - Delegation policy at C for context X
    $$f_{C_d} (X) \rightarrow \text{targets} := \{B\}$$
  - Trust policy for unknown entities
    $$f_C (? , X) := [X. t_{C_B}^A : B \in f_{C_d} (X)] \rightarrow \text{trust|pred}$$
Trust Management: Challenges & Directions

• **Trust policy evaluation**: attribute-based policy evaluation
  – XACML with extensions
  – Using **Multi-data types Interval Decision Diagrams** (MIDD): neutralized with policy languages.
  – Efficient in evaluation complexity.
  – Authentic of attributes, trust credentials: SAML assertion to carry trust credentials

• **Distributed policy evaluation**: using Push model in AAA

• **Trust context description**:
  – Attribute profiles: using resource description languages
  – Semantics inference between attribute namespace ontologies

• **Dynamic trust relationships**
  – On-demand cloud resources
  – Provision trust policies
Dynamic Trust Establishment for Intercloud

• **Use-case:**
  – Consuming cloud resources from sub-contractor Cloud Service Providers

• **Adopt cloud resources/services lifecycles**
  – Request – Reservation – Deployment – Operation - Decommissioning
  – **Reservation & Deployment phases**
    • Establish direct trust relations between entities and/by linking/chaining trust anchors
    • Generate trust policies & delegation policies for provisioned cloud resources
    • Local attribute name spaces resolution
  – **Operation phase**
    • Establish (indirecldynamic) trust relationships for instantly provisioned infrastructures using trust policies & delegation policies
Indirect/Dynamic Trust Establishment Protocol

Operation phase:
Establish indirect trust relationships using trust policies & delegation policies

E: End-user
C: Cloud customer
P: Cloud provider

\[ f_C(E, X_1) \rightarrow t^X_1_C \]

Recommendation eval:
\[ (C \in f_P^D(X_1)) \land valid(t^X_1_C, X_1) \rightarrow trust \]
Indirect Trust Establishment Protocol Flow

Operation phase:
Establish indirect trust relationships for delegation chain of K providers (trust-chain)

C: client
P_i: Cloud Providers i
Dynamic Trust Establishment for Intercloud

Implementation

- **Dynamic trust establishment protocol**: experiment in Geysers (https://geysers.eu)

- **Trust evaluation engine**: SNEXACML
  - XACML extensions:
    - Policy issuer
    - Issuing trust credential: obligations
  - SAML assertion extension
  - Evaluation performance
    - Using Multi-type Interval Decision Diagrams (MIDD)

VM/storage at PIP
Trust evaluation engine: performance analysis

<table>
<thead>
<tr>
<th>Datasets</th>
<th>Policy level</th>
<th># Policy-sets</th>
<th>#Policies</th>
<th>#Rules</th>
<th>Attr</th>
<th>Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>GEYSERS</td>
<td>3</td>
<td>6</td>
<td>7</td>
<td>33</td>
<td>3</td>
<td>=</td>
</tr>
<tr>
<td>Continue-a</td>
<td>6</td>
<td>111</td>
<td>266</td>
<td>298</td>
<td>14</td>
<td>=</td>
</tr>
<tr>
<td>Synthetic-360</td>
<td>4</td>
<td>31</td>
<td>72</td>
<td>360</td>
<td>10</td>
<td>=(80%), complex(20%)</td>
</tr>
</tbody>
</table>

Average request evaluation time

Micro-benchmark evaluation response times
Conclusion

• An attribute-based approach for dynamic trust establishments for multiple Cloud providers
  – Attribute trust policies: flexible, manageable
  – Open for attribute namespaces resolutions
  – Dynamic provisioning trust relationships
  – High performance evaluation
Discussion and Future work

• On-going work
  – Resolutions of attribute namespaces ontologies
  – Attribute validation
  – Apply dynamic trust establishment protocol to Intercloud
  – Trust Policy Engine

• P2302 Group
  – Section 6.6-6.8, Intercloud Security
    • Trust Management Framework
      – Trust topology, protocols, evaluation mechanisms.
      – Auxiliary functions: collect and validate trust values, attributes, trust credentials
Thank you!

Contact Information

Canh Ngo, Yuri Demchenko
{t.c.ngo, y.demchenko}@uva.nl
System and Network Engineering research group (SNE)
University of Amsterdam