Security and Access control management in Multi-domain collaborative environments

Amit R Mahale
Ebiquity Lab, Computer Science

Background

Objective: Developing an integrated framework to support assured information sharing.

Problem: Currently, Access control strategies focus only on factors like role, attribute or the group.

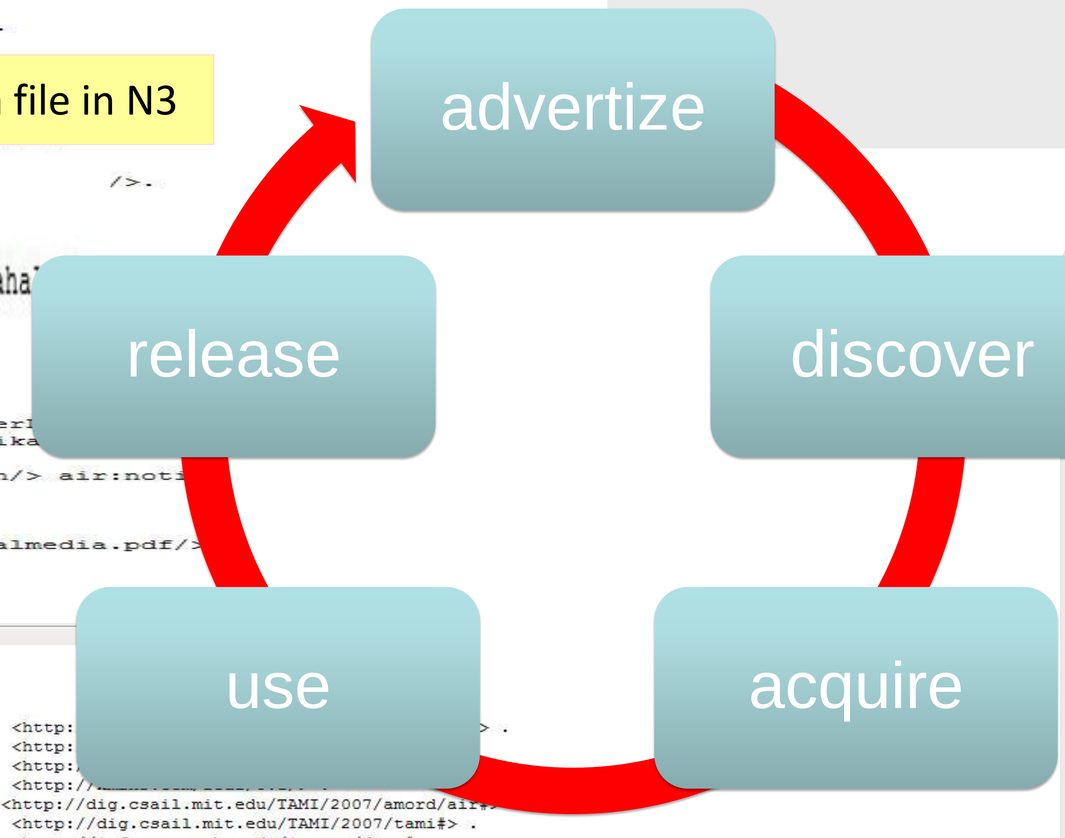
Goal: To develop an Access control strategy which utilizes the semantics of the environment, to promote seamless transfer of information between trusted parties.

Scenario

- Information Sharing between two security agencies only during highly critical or emergency situation.
- Agency A has an intelligence report about an attack at location X. The kind of weapon to be used in the attack is supposed to be chemical weapon.
- Agency A does not have the expertise to tackle this issue.
- The System makes a decision to share this information seamlessly with Agency B which has expertise dealing with chemical attacks.

```
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .
@prefix air: <http://dig.csail.mit.edu/TAMI/2007/amord/air#> .

@prefix : <http://infrasec.umbc.edu/images/data#> .

:UMBC a foaf:Organization;

<http://ebiquity.umbc.edu/person/foaf/Anand/Karandika
foaf:Person;                                          />.
      foaf:openid <http://auth.umbc.edu/anandk1>;
      foaf:knows <http://ebiquity.umbc.edu/person/html/Amit/Maha
      foaf:openid <http://auth.umbc.edu/amahale1>.
       foaf:openid <http://auth.umbc.edu/david>.

<http://www.umbc.edu/~finin/foaf.rdf> air:in :Member
<http://ebiquity.umbc.edu/person/foaf/Anand/Karandika
air:in :MemberList.
<http://ebiquity.umbc.edu/person/html/David/Chapman/> air:not
:MemberList.
:Req1 a air:Request;
   foaf:openid <http://auth.umbc.edu/amahale1>;
   air:resource <http://ebiquity.umbc.edu/pdf/socialmedia.pdf/>
#ends
For Help, press F1
```

Data file in N3



Implementation

Contextual Data to model the environment is scripted in Notation 3 Format.

- Policies consisting of multiple rules are defined using the AIR Policy language developed at MIT.
- AIR Reasoner built over CWM & Pychinko accepts data and policy file and provides with compliance decisions along with justifications.

Workflow

Two stage process

- Reason the contextual data against the policy to make a decision about the current state of environment.
- If the situation demands sharing of Information, identify the entity depending on its characteristics and usability.

```
@prefix rdf:  <http:                                        > .
@prefix rdfs: <http:
@prefix owl:  <http:
@prefix foaf: <http://
@prefix air: <http://dig.csail.mit.edu/TAMI/2007/amord/air#>
@prefix tami: <http://dig.csail.mit.edu/TAMI/2007/tami#> .
@prefix data: <http://infrasec.umbc.edu/images/data#> .
@prefix : <http://infrasec.umbc.edu/images/data#> .

@forAll :REQ, :REQUESTER, :RESOURCE, :MEMBER, :MEMBERLIST .

:AccessPolicy
   rdfs:label
   air:variabl                                    E, :MEMBER, :MEMBERLIST;
   air:rule :Access_1.

:Access_1 a air:BeliefRule;
       rdfs:label "Access Rule #1";
       air:pattern {
          :REQ a air:Request;
           foaf:openid :REQUESTER;
           air:resource :RESOURCE.
        :UMBC data:owns :RESOURCE.
       };
       air:description (:REQ " is a request made by a requester xyx
with openid, " :REQUESTER ", for UMBC resource " :RESOURCE);
       air:rule :Access_2.

:Access_2 a air:BeliefRule;
       rdfs:label "Access Rule #2";
       air:pattern {
        :UMBC foaf:member :MEMBERLIST.
        :MEMBER air:in :MEMBERLIST.
          :MEMBER a foaf:Person;
           foaf:openid :REQUESTER.
           };
       air:description ("The requester xyz with openid, " :REQUESTER ",
is a UMBC member");
       air:assert { :REQ air:compliant-with :AccessPolicy }.

#ends
```

Policy in AIR

```
:Req1     air:compliant-with :AccessPolicy .
{
    :Req1     air:compliant-with :AccessPolicy .
}     tms:description  (
"The requester xyz with openid, "
<http://auth.umbc.edu/amahale1>
", is a UMBC member" );
 tms:justification  [
     tms:antecedent-expr  [
```

Output

Conclusions & Future Work

- New Dimension in Access control involving real time contextual information.
- Future work will be on making the system scalable, developing user friendly tools for policy administration.

Technical Highlights

- Developed using semantic web technologies.
- RDF Based model which has wide acceptance.
- Ontology to define the high level semantics of the environment.
- Semantically-enhanced browsing of scenario data

References
[1] A Semantic Context-Aware Access Control Framework for Secure Collaborations in Pervasive Computing Environments, Alessandra Toninelli, Rebecca Montanari, Lalana Kagal, and Ora Lassila.
[2] Utilizing Semantic Knowledge for Access Control in Pervasive and Ubiquitous Systems, Anand Dersingh, Ramiro Liscano, Allan Jost.

This work is supported by MURI contract FA9550-08-1-0265

Assured Information Sharing Lifecycle