Declaration and Translation of Spatial Access Control Policy

Aijuan Zhang[a,b], Jingxiang Gao[b], Jiuyun Sun[b], Cheng Ji[a]
[a]School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China
Email: {zaj, jicheng}@cumt.edu.cn

[b]School of Environment Science and Spatial Informatics, China University of Mining and Technology, Xuzhou 221116, China
Email: jxgao@cumt.edu.cn, mapping2011@126.com

***Abstract*—Access control service is used to solve the controllability problem of data and service, access control system is finally deployed in the form of policy. The description forms of policy are different in the stage of configuration and deployment. Safety policy translation model is used to realize configuration policy and automatic translation of deployment policy. However, currently it lacks automatic translation model. What's more, automatic translation models are different according to different access control models. In this paper, a spatial access control model is proposed through the object-oriented idea. In addition, the spatial access control policy elements are declared, and they are translated through compiling principle. Finally, the configuration policy is translated to deployment policy which is described by XACML through the policy translation rules.**

***Index Terms*—access control policy, spatial, policy translation model, XACML**

I. Introduction

Access control which is one of the core services of security is used to solve the controllability problem of service and data. Control rules of access control system are finally deployed in the form of policy[1], so policy becomes the core of access control research. Considering the policy hierarchy, the leader of access control policy, Moffett and Sloman [2] have discussed the importance of the policy hierarchy, policy at different layers can meet the demand of different hierarchies of the security engineering. Security analysts use abstract policy to describe security requirement and the administrators use actual low-layer policy for policy configuration. This requires policy translation (which is also called policy refinement) to realize the translation from high-layer policy to low-layer policy.

For policy translation, there are few special prototype systems. Lamsweerd proposed object-oriented security requirement analysis and introduced KAOS (Knowledge Acquisition in Automated Specification) formalization method in 1999. This method extended the demand engineering analysis method and formalization reasoning technology, but it did not relate the goal and the behavior of the goal, nor consider confliction analysis. Bandara extended policy refinement based on KAOS method [3, 4]. He refined the object-oriented policy integrated with system behavior. Relevant system information came from UML modeling model or finite state machine of the system. This work made substantial outstanding contribution to the policy refinement. Later, based on Bandara's research, the literatures [5, 6, 7, 8] conducted formal verification for the service quality policy by using Liner Temporal Logic (LTL). This method solved a series of problems from the policy design to realization. However, whether this method was suitable for access control policy hasn't been verified.

For the access control policy refinement of the network system, the literatures [9, 10, 11] conducted a lot of research of policy refinement based on the model. Specific approach is: Use RBAC management method. Firstly, define a high-layer abstract policy, and then derive a low-layer specific policy. This Model-based Management method uses object-oriented method in the modeling system, so as to support policy-based management on the target objects and behaviors. The research of this aspect simply proves the validity of the refinement process.

Beigi [12] proposed policy translation model based on case reasoning. The method firstly establishes case database, inputs configuration parameters of management targets in the system, and then chooses specific cases in the case database, and gets the final refinement policy through data preprocessing and reasoning calculation. The defect of the technology is that it excessively rely on the case database, it also needs the participation of experts in this field, so it can only be applied to specific application fields where the configuration parameters can be quantified. If new services are introduced, it may cause translation failure. Dai[13] adopts compiling principle idea in the design and realization of policy translation compiler.

Corresponding author: Jingxiang Gao
School of Environment Science and Spatial Informatics, China University of Mining and Technology, Xuzhou 221116, China
Email: jxgao@cumt.edu.cn

doi:10.4304/jsw.8.5.1132-1139

Policy translation is the basic means to realize standardization policy deployment. However, at present, there is no valid translation model in the spatial access control management policy, so the translation can't be done automatically.

Firstly, a two-stage description method for the spatial access control policy is proposed in this paper, and then the translation rules between two policy languages are decided. Secondly, based on the morphology syntax and semantic analysis of the configuration policy, spatial access control policy translation model is proposed, so as to realize the spatial policy translation from the design policy to the standardized XACML deployment policy.

II. The Hierarchy of Security Policy

Sloman and Moffett proposed three-layer structure of the security policy [1]. In this structure, the policy can be divided into three description modes:

- Policy in natural language: In the security requirement analysis stage, the security analysts use this abstract policy to describe security requirement.
- Policy in declarative or semi-formalized language: It is the middle-layer policy, which will be used by the configuration manager for policy configuration. This is the implementation policy, usually the declarative language will be used, such as XACML [14] description.
- Policy in natural logic: It is used to analyze and verify the policy.

The relationship between three-mode policy and the software development is shown in the following figure.

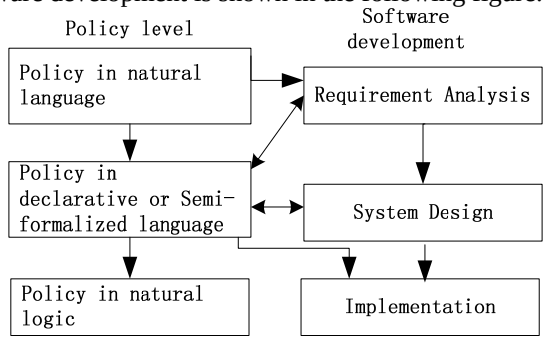

Figure 1. Integrated policy generation in software development

The highest-layer policy aims at the security analysts. It describes the abstract security goals, which is abstract policy. The second layer which aims at security designer and security configuration personnel is the specific strategies made. However, the policy of this layer is divided into logic-oriented policy and event-oriented policy. Currently, standardized description language XACML of the access control policy is the middle-layer policy, GeoXACML is the extension of XACML in geographic information, but they are not suitable for user-oriented policy editing. Therefore, in the modeling process, user-oriented senior declarative language is used to edit the policy rules, and then it will be translated into XACML for deployment. User-oriented senior statement language and semi-formalized XACML language are both middle-layer policy languages, these two languages indicate policy transformation, which is called intra-formational refinement.

III. Spatial Access Control Model Based on Attribute

Spatial data has geographical characteristics. It includes not only the semantic attribute, but also the spatial relationship attribute. Spatial access control requires that the spatial data access can constrain to many layers, division of granularities of spatial vector data from coarse to fine includes: map, a single layer, specific object (object set), some attributes of the object. Meanwhile, the model needs space-time correlation. In order to realize spatial access control requirement, a space-time access control model based on RBAC model is proposed by extending the attributes of the subject and object in this paper. The model is shown in the following figure.

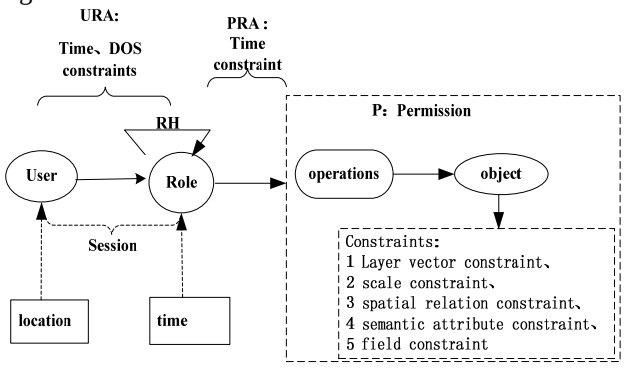

Figure 2. Spatial access control model based on attributes

Spatial data is packaged based on object-oriented idea. In view of four kinds of data control granularities requirements, attribute constraints of four granularity objects including map, layer, element object and object view is designed. Meanwhile, in order to realize time context and spatial relation correlation of the control, time and space regional constraint is added to the subject of the above model. For the above spatial access control model, the description formed by the attributes of users, roles and spatial data is regarded as the constraint conditions for authorization. Elements and relationship between the elements in the model is listed below.

- $User = (identifier, location, duty\ of\ separation : DOS, roles)$

  Identifier attribute is used to identify the user's identity. Location attribute indicates the area of subject. In order to realize spatial correlation of the object control granularity, spatial constraint needs an authorized geometry to confirm the spatial relationship. This authorization geometry comes from the attribute of the subject. In this paper, this attribute is put on the user-level subject and is described by Location. DOS means duty separation constraint. It is inherited from the RBAC model constraints. Role attribute is used to constrain permission set available for users.

- $Role = (name, time, pps)$: It is the intermediate connecting users and PPS (permission policy set). This model is time correlated. However, for time constraint, it is hoped that this model will be the context environment factor in the role activation or authorization judgment. Therefore, attribute of $time$ is set for the role.
- $opertions$: Spatial object operation interface.
- $UA \subseteq (User \times Time \times Role)_C$ $c \in \{time\ cons\ of\ UA\}$. It means that the role is given to the user in a specific time.
- $PA \subseteq (P \times time \times Role)_C$: It means m:m mapping from the permission set to the role set in a specific time.
- $RH \subseteq (R \times R)_C$: It means the partial order inheritance relationship between the roles.
- $Objects$: It means spatial objects of different granularities.

It is indicated from the spatial access control requirements: the above model should have the following spatial data constraints.

- Map granularity constraint: Map-level class contains multiple layers composing the map. Different layers for different classes of users are the constraints of map level object (object). Therefore, when defining the map class, the attribute of vector FVec=[1|0*] is added. Whether specific map is visible or not will be indicated through setting 1 or 0 to corresponding layer.
- Layer granularity constraint: The granularity indicates the control to all objects of a certain class of surface features. It is the class-level control granularity. The common constraint attributes of the granularity are scale and production time.
- Object granularity constraint: The granularity indicates the control to objects (set) of a certain class. The object level constraints attributes include spatial attribute and non-spatial attribute, which are from the source spatial data, while non-spatial constraint attribute is decided by the specific system requirements.
- Object view granularity constraint: It is used to decide the information content of the object shown to users. Therefore, it can be confirmed through the list of attribute field name. In this paper, Field attribute is used to decide it.

IV. Spatial Access Policy Description

The model is eventually required to be managed and used in the form of policy. In the above spatial access control model, User, Role, Object and Operation have their own attributes. Attribute constraints of the model using BNF paradigm description are shown as below.

$User - AttrExpression$ ::=

$AttrExpression[\{and \mid or\ AttrExpression\}+]$

$Role - AttrExpression$ ::=

$AttrExpression[\{and \mid or\ AttrExpression\}+]$

$Operation - AttrExpression$ ::=

$AttrExpression[\{and|or\ AttrExpression\}+]$

$Object - AttrExpression$ ::=

$AttrExpression[\{and \mid or\ AttrExpression\}+]$

$AttExpression$ ::= $Attribute\ OP\ AttributeValue$

$Attribute$ ::=

$User.identifier \mid User.location \mid User.role \mid$

$Role.name \mid Role.time \mid\mid Operation.id \mid$

$Object.FVec \mid Object.scale \mid Object.location \mid$

$Object.semanticAttribute$

OP ::= " > " | " >= " | " < " | " <= " | " = " |

" ≠ " | " ∈ " | " ∉ " | $spatial\ Rel$

$spatial\ Rel$ ::=

$Equals \mid Disjoints \mid Touches \mid Crosses \mid Within s \mid$

$Overlaps \mid Intersects \mid IsWithinDistance$

$AttributeValue$ ::= {determined by the exact system}

Among them, $spatial\ Rel$ indicates the supportive spatial relation constraint. In this paper, seven spatial topological relations and a spatial metric relation constraint will be supported.

Description of Spatial Access Control Policy by VPL

The most obvious feature of VPL description policy is to describe the authority by using view, and then give the authority to role, but the original VPL cannot describe the constraint based on attribute, so this paper adds a keyword "where" and uses constraint description to describe the control of multi-granularity. The keywords are shown in bold, which include policy, roles, holds, on, in, view, control, allow, deny and where, etc. In the definition of role, their authorities will be described by using the keyword of "holds", which is shown below.

```
Policy G1{
 roles
   Reader holds Gmap1 on ChinaInfoModel
   Reader holds Getting on City in [8:00  23:00]
   Admin holds Gmap1 on ChinaInfoModel
   Admin holds Getting on City
   Admin holds Setting on City

 view Getting controls cInfo:ChinaInfoModel/gml:Feature/cInfo:City
 {
 allow getInfo
 }

 view Setting controls cInfo:ChinaInfoModel/gml:Feature/cInfo:City
  where (scale>5 and withins “jiangsu”； fFilter=(name,area))
 {
 allow modify
 }

 view Gmap1 controls cInfo:ChinaInfoModel
 where (FVec=001;null;null)
  {
  allow getInfo
        modify
  }
}
```

Figure 3. VPL policy

The above policy indicates that the role Reader and Admin can implement the operation getInfo, modify for the third layer City of the map-class. What's more, the access of Reader to the layer City must be made during 8:00 to 23:00 everyday. Admin can conduct getInfo operation to the layer City and compile the data of City whose scale is bigger than 5 within the location of Jiangsu.

Description of Spatianl Access Policy by GeoXACML

VPL gives user-oriented senior policy description method, but these policies are not structured, so when these policies are required to be deployed and analyzed by access control monitoring module, it is low efficiency and distributed interaction can not be realized. Therefore, the final deployment policy selects the standard and structured GeoXACML policy for deployment. Description of the above spatial access control policy by XACML is given in the following text.

- **Role description**: XACML uses attribute match to identify the subject. Role can be defined as the attribute of Subject by using SubjectAttributeDesignator tag. As shown in the following figure, Subject has the role of manager.

```
<Subject>
  <SubjectMatch MatchId="&function;anyURI-equal">
    <AttributeValue DataType="&xml;anyURI">&roles;manager</AttributeValue>
    <SubjectAttributeDesignator AttributeId="&role;" DataType="&xml;anyURI"/>
  </SubjectMatch>
</Subject>
```

Figure 4. A role definition in GeoXACML

- **Operation description**: Operation which can be implemented for a resource is described by < Action> attribute match, as shown in the following figure, it describes the operation: getMap().

```
<Action>
  <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue DataType="http://www.w3.org/2001/
XMLSchema#string">getMap<AttributeValue>
    <ActionAttributeDesignator AttributeId="urn:oasis:names:Tc:xacml:1.0:action:action-id
DataType="http://www.w3.org/2001/XMLSchema#string"/>
  </ActionMatch>
</Action>
```

Figure 5. An operation definition in GeoXACML

- **Resource description based on the map**: The map is described by multiple layers. The layer set can be regarded as a class that references to multiple layers in an object-oriented data model. In order to realize interaction of heterogeneous services, interactive data can be coded with GML, and the class is described by Xpath form, which can also explain the hierarchical relationship between data classes. Layer set contains multiple layers. If you need to clarify the use status of each layer, you can use <Condition> tag to restrict the value of Fvec which is the attribute vector. It is shown in the following figure.

```
<Resource>
  <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
ChinaInfoModel
    </AttributeValue>
    <AttributeSelector RequestContextPath="name(//:cInfo:ChinaInfoModel)
" DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </ResourceMatch>
</Resource>
```

```
<Condition>
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of">
      <Function FunctionId="http://www.geoxacml.org/1.0/function#equals"/>
      <AttributeSelector RequestContextPath="//cInfo:ChinaInfoModel/cinfo:FVec"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
10010
      </AttributeValue>
    </Apply>
</Condition>
```

Figure 6. A layer set definition in GeoXACML

The map class is called ChinaInfoModel. In this rule, layer 10010 can be accessed to, i.e. the first and the fourth layer can be accessed to.

- **Resource description based on the layer**: The layer is also a class, which describes all objects of a class. Layer-class is described by <Resource>. Meanwhile, the layer can be constrained by using global attribute. Therefore, <Condition> attribute match can be used to describe the constraint of scale attribute, which is shown in the following figure.

```
<Resource>
  <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">City
    </AttributeValue>
    <AttributeSelector
RequestContextPath= "name(//cInfo:ChinaInfoModel/gml:FeatureMember/cInfo:City)”
DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </ResourceMatch>
</Resource>
```

```
<Condition>
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of">
    <Function FunctionId="http://www.geoxacml.org/1.0/function#Integer-less-than"/>
    <AttributeSelector
RequestContextPath="//cInfo:ChinaInfoModel/gml:FeatureMember/cInfo:City/cInfo:scale"
DataType="http://www.w3.org/2001/XMLSchema#integer"/>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"> 25
      </AttributeValue>
  </Apply>
</Condition>
```

Figure 7. A graphic layer definition in GeoXACML

The above figure indicates that the layer City whose scale is less than 25 can be shown.

- **Object-level resource description based on the semantic constraint**: element object and object view level constraints are actually based on the extension of class constraint, it uses object-level attribute to constrain element object, thus enabling the controlled object to satisfy the semantic constraint or spatial relation constraint. Resources definition based on object-level semantic attribute constraint is shown in the following figure.

```
<Resource>
  <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">City
    </AttributeValue>
    <AttributeSelector RequestContextPath="name(//cInfo:ChinaInfoModel/gml:FeatureMember/cInfo:City)"
" DataType="http://www.w3.org/2001/XMLSchema#string"/>
  </ResourceMatch>
</Resource>
```

```
<Condition>
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of">
      <Function FunctionId="http://www.geoxacml.org/1.0/function#Integer-less-than"/>
      <AttributeSelector
RequestContextPath="//cInfo:ChinaInfoModel/gml:FeatureMember/cInfo:City/cInfo:area"
DataType="http://www.w3.org/2001/XMLSchema#integer"/>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"> 500000
      </AttributeValue>
    </Apply>
</Condition>
```

Figure 8. Semantic attribute-based object description in GeoXACML

The above policy rules indicate: only the city with an area over 500km 2 can be shown for the object of City layer.

- **Object-level resource description based on spatial constraint**: Spatial constraint relations used in the above spatial access control model include topological relation and metric relation, which involve permission geometry description. There are two kinds of description for spatial area including physical description and logical description. In this paper, GeoXACML function is required to be extended, so as to realize the description of physical permission area and logical permission area in the policy.

  1) Spatial constraints described by Geometry

  In the constraint, when the authorized area can not correspond to an exact logic area, it can be directly described by physical area. In the policy rules show in the following figure, spatial resource description is the same as < Resource > in Figure8. The content of < Condition > tag is basically described in this part. It is shown in the following figure:

```
<Condition >
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of">
    <Function
FunctionId="urn:ogc:def:function:geoxacml:1.0:geometry-contains"/>
    <AttributeValue
DataType="urn:ogc:def:dataType:geoxacml:1.0:geometry">
      <gml:Polygon id="Europe"
srsName="urn:ogc:def:crs:EPSG:6.6:4326"
xmlns:gml="http://www.opengis.net/gml">
        <gml:exterior>
          <gml:LinearRing>
            <gml:posList dimension="2">
              -11 55 -10 35 -5.5 36 -1 36 1 38 5 38 11 38 14 36
              26 33 29 36 26 39 29 46 39 47 40 49 27 56 27 60
              25 60 20 58 21 56 19 55 11 55 10 57 7 57 8 54 3
              53 -2 60 -8 58 -11 55 -11 55
            </gml:posList>
          </gml:LinearRing>
        </gml:exterior>
      </gml:Polygon>
    </AttributeValue>
  <AttributeSelector
DataType=urn:ogc:def:dataType:geoxacml:1.0:geometry
RequestContextPath
="//wms:myMap/*/cInfo:ChinaInfoModel/gml:FeatureMember/cInfo:
provinceBound/cInfo:shape/>
</Condition>
```

Figure 9. Spatial constraints described by geometry in GeoXACML

The above rule indicates that only the City object within designated coordinate boundary range in the provincial boundary layer provinceBound is shown.

2) Spatial constraints described by logic area

If logical spatial location is used to describe spatial constraint, then it is required to extend GeoXACML function. In this paper, string type is used to describe logical spatial location, and the translation function logToRealMap is also defined, which is used to automatically translate the location from logic location to physical location in the policy matching process. The definition is shown as follows:

logToRealMap(loc:logicLocation):geometryBag

It is used to calculate corresponding physical spatial location set with logic location as the input parameters. It is required to extend the spatial function set of GeoXACML. When this function is called by the access control implementation module analytic XACML policy, the function will make the spatial query request, and return it to the corresponding physical location set. The following policy rule omits the definition of <Resource>, which indicates: showing the city object within the logic area “JiangSu".

```
<Condition >
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of">
    <Function FunctionId="urn:ogc:def:function:geoxacml:1.0:geometry-contains"/>
    <AttributeSelector DataType=urn:ogc:def:dataType:geoxacml:1.0:geometry
RequestContextPath="//
cInfo:ChinaInfoModel/gml:FeatureMember/cInfo:provinceBound/cInfo:shape/>
    <Function FunctionId=” http://stmac:logToRealMap” />
      <Attributevalue DataType=urn:ogc:def:dataType:String>JiangSu
      </Attributevalue>
    </Condition>
```

Figure 10. Spatial constraints described by logic location

- **Description based on object view**: If you want to control the field information which can be displayed by the object, then you should set up the

control attribute fFilter of the field for the object. Therefore, in < Function > tag, fFilter and other attributes constraints of the object can be put together to implement "and" operation. The policy description is shown in the following figure.

```
<Condition>
  <Apply Funcion ID="and">
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of">
      <Function FunctionId="http://www.geoxacml.org/1.0/function#Integer-less-than"/>
      <AttributeSelector
RequestContextPath="//cInfo:ChinaInfoModel/gml:FeatureMember/cInfo:City/cInfo:scale"
DataType="http://www.w3.org/2001/XMLSchema#integer"/>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"> 25
      </AttributeValue>
    </Apply>
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of-any">
      <Function FunctionId="http://www.geoxacml.org/1.0/function#equals"/>
      <AttributeSelector
RequestContextPath="//cInfo:ChinaInfoModel/gml:FeatureMember/cInfo:City/cInfo:fFilter"
DataType="http://www.w3.org/2001/XMLSchema#String"/>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string"> name
      </AttributeValue>
    </Apply>
</Condition>
```

Figure 11. Object-view constraint description in GeoXACML

The above rule indicates that: only the "name" attribute is shown for the layer "City" whose scale is less than 25.

- **Time context attribute constraint:** in the above spatial access control model, time is the attribute of role, and it plays a constraint role in the implementation process of URA and PRA. In RBAC model which is described by GeoXACML, we describe it by < Function >in RPS, which is shown in the rule below, the effective time of rule is between [9h, 17h].

```
<Condition>
  <Apply FunctionId="&function;and">
    <Apply FunctionId="&function;time-greater-than-or-equal">
      <Apply FunctionId="&function;time-one-and-only">
        <EnvironmentAttributeDesignator AttributeId="&environment;current-time"
          DataType="&xml;time"/>
      </Apply>
      <AttributeValue DataType="&xml;time">9h</AttributeValue>
    </Apply>
    <Apply FunctionId="&function;time-less-than-or-equal">
      <Apply FunctionId="&function;time-one-and-only">
        <EnvironmentAttributeDesignator AttributeId="&environment;current-time"
          DataType="&xml;time"/>
        </Apply>
      <AttributeValue DataType="&xml;time">17h</AttributeValue>
    </Apply>
  </Apply>
</Condition>
```

Figure 12. Time constraint description in GeoXACML

V. POLICY TRANSLATION MODEL

Although the structure of GeoXACML is clear, it is not suitable user-oriented policy compiling. Therefore, VPL should be used for policy compiling, and the policy which is described by GeoXACML should be used for deployment. In order to realize policy translation, policy translation model which is based on semantic analysis is proposed in this paper.

In order to establish corresponding relationship between these two policies, there is a need to define a set of reasonable policy elements translation rule, where the spatial access control policy described by VPL will be mapped into policy element described by GeoXACML mapping rule is shown below.

TABLE II.
MAPPING RULES OF RBAC

Spatial Access control model	XACML	VPL
user	subject	Subject
role	Subject attribute	role
object	resource	The "controlled" in view
operation	action	The "operation" in view
permission	Role<PolicySet> and Permission<PolicySet>	Role.. holds.. in policy
Inheriented relation	<PolicySetIdRefenence> in PPS	extends

TABLE I.
MAPPING RULES OF ATTRIBUTE CONSTRAINTS

Spatial Access Control model	XACML	VPL
Exclusion constraints	Separation of Duty <PolicySet> or Policy Assignment <PolicySet>	role exclude
location	Subject attribute	Subject attribute
time	<Condition>in RPS	Role attribute
Scale FVec	<Condition> in PPS	Class-oriented attribute
>,<,>=,<=,=, $\in$, $\notin$ Spatial function	<Function> in Condition	operatiors

TABLE I gives the corresponding rules of RBAC model elements, while TABLE II gives the corresponding rules of corresponding attribute constraints in these two languages.

Relization of Vpl-GeoXACML Translation

VPL-GeoXACML translation work process is basically the same as that of the compiler of other languages (such as C, Java, etc.). However, in the intermediate code generation stage, GeoXACML code is generated, the overall structure of the policy translation module is shown in the following figure.

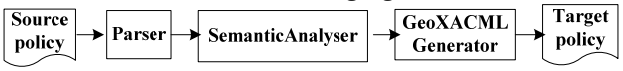

Figure 13. The policy translation module

- Morphology and syntax analysis will be realized by class Parse, and the language elements of VPL will be filled in the symbol table. After the processing, symbol table filled in VPL elements is formed.
- SemanticAnalyser is used to improve symbol table, which is filled in completely according to the relationship between VPL elements, especially the inheritance relationship between roles and the hierarchical relationship between resources, so that each element has its own attribute. SemanticAnalyser is mainly used to detect conflicts among rules.
- According to the VPL - XACML mapping rule, VPL element in the symbol table will be translated into corresponding GeoXACML elements by Generator, so as to produce objective policy file.

In order to make semantic detection and realize the translation between VPL and GeoXACML, support from symbol table and its sub-class is needed. Data structure which is used in the translation process will be introduced below.

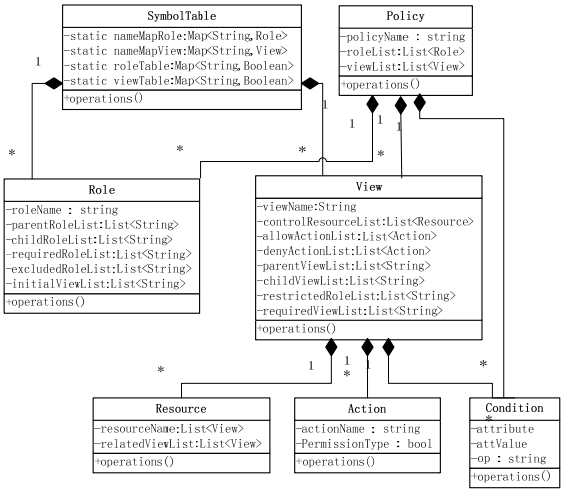

Figure 14. The data structures of the compiler

- SymbolTable contains Map structure of roles and views
- Role encapsulates hierarchy relationship attribute caused by inheritance
- Class View polymerizes classes of Resource, Action and Condition.
- Resource encapsulates resource object by using XPath name and contains view for the resources
- Action encapsulates the operation name and permission class
- Condition encapsulates key-value pairs of the attributes.

VI. EXAMPLES OF POLICY TRANSLATION

Mapping relationship between languages and action code of syntax declaration is defined by using Javacc. Mapping between two languages is realized by using XACML processing package provided by SUNXACML. Experimental examples are as follows.

Input: VPL source policy Conference.vpl
Output: XACML policy
RPS_Author_role.xml:
Role<PolicySet> of role Author
PS_Author_role.xml:Permission < PolicySet >of role Author
RAPS_Author_role.xml: Permission Role Assignment <PolicySet> of role Author
Processing module: vpl-GeoXACML compiler

Among them, the definition of source policy file Conference.vpl of VPL is shown in the following figure:

```
Policy p1{
 roles
       Author holds Registering in [8h: 23h]
view  Registering controls SubmissionPhase
     {
      allow   registerFeature
     }
}
```

Figure 15. Policy expressed by VPL

After the translation, GeoXACML policy is described as RPS, PPS and RAPS, which is shown in the following figure.

- RPS_Author_role.xml: Role <PolicySet> of role Author.

```
<PolicySet PolicySetId="RPS:Author:role"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-
algorithm:ordered-deny-overrides">
 <Target>
  <Subjects>
   <Subject>
    <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
     <AttributeValue DataType="http://www.w3.org/2001/
XMLSchema#string">Author</AttributeValue>
     <SubjectAttributeDesignator AttributeId="urn:oasis:names:Iterpreter:subject:role"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </SubjectMatch>
   </Subject>
  </Subjects>
  <Resources>
   <AnyResource/>
  </Resources>
  <Actions>
   <AnyAction/>
  </Actions>
 </Target>
 <PolicyIdReference>PPS:Author:role</PolicyIdReference>
</PolicySet>
```

Figure 16. RPS for Author

- PS_Author_role.xml: Permission <PolicySet> of role Author is shown in the following figure.

```
<PolicySet PolicySetId="PPS:Author:role" PolicyCombiningAlgId
="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:
ordered-permit-overrides">
  <Target>
    <Subjects>
      <AnySubject/>
    </Subjects>
    <Resources>
      <AnyResource/>
    </Resources>
    <Actions>
      <AnyAction/>
    </Actions>
  </Target>
  <Policy PolicyId="PPS:Permissions:for:Author:role"
          RuleCombiningAlgId=
          "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm
          :ordered-permit-overrides">
    <Target>
      <Subjects>
        <AnySubject/>
      </Subjects>
      <Resources>
        <AnyResource/>
      </Resources>
      <Actions>
        <AnyAction/>
      </Actions>
    </Target>
    <Rule RuleId="Permission:to::registerFeature:for:Author:role" Effect="Permit">
      <Target>
        <Subjects>
          <AnySubject/>
        </Subjects>
        <Resources>
          <Resource>
            <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                    SubmissionPhase</AttributeValue>
              <ResourceAttributeDesignator
                    AttributeId="urn:oasis:names:myIterpreter:resource:resource-id"
                    DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </ResourceMatch>
          </Resource>
        </Resources>
        <Actions>
          <Action>
            <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                    registerFeature</AttributeValue>
              <ActionAttributeDesignator
                    AttributeId="urn:oasis:names:myIterpreter:acion:aciton-id"
                    DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </ActionMatch>
          </Action>
        </Actions>
      </Target>
    </Rule>
  </Policy>
</PolicySet>
```

Figure 17. PPS for role Author

- RAPS_Author_role.xml: Permission Role Assignment <PolicySet> of role Author is shown

in the following figure. The activation time of application role Author is constrained by the file.

```
<PolicySet PolicySetId="RAPS:prerequire:constraints:Author:role"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:ordered-permit-overrides">
  <Policy PolicyId="RAPS:for:role:Author" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
combining-algorithm:ordered-permit-overrides">
    <Rule RuleId="Permissin:to:hold:Author:role" Effect="Effect">
   <Target>
    <Subjects>
     <Subject>
      <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Chair</AttributeValue>
       <SubjectAttributeDesignator AttributeId="urn:oasis:names:myIterpreter:subject:role"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
      </SubjectMatch>
     </Subject>
    </Subjects>
    <Resources>
    <AnyResource/>
    </Resources>
    <Actions>
     <Action>
      <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">enable</AttributeValue>
       <ActionAttributeDesignator AttributeId="urn:oasis:names:myIterpreter:attibute:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
      </ActionMatch>
     </Action>
    </Actions>
   </Target>
   <Condition>
      <Apply FunctionId="&function;and">
        <Apply FunctionId="&function;time-greater-than-or-equal">
          <Apply FunctionId="&function;time-one-and-only">
            <EnvironmentAttributeDesignator AttributeId="&environment;current-time"
                DataType="&xml;time"/>
          </Apply>
          <AttributeValue DataType="&xml;time">8h</AttributeValue>
        </Apply>
          <Apply FunctionId="&function;time-less-than-or-equal">
            <Apply FunctionId="&function;time-one-and-only">
              <EnvironmentAttributeDesignator AttributeId="&environment;current-time"
                  DataType="&xml;time"/>
            </Apply>
          <AttributeValue DataType="&xml;time">23h</AttributeValue>
      </Apply>
    </Apply>
    </Condition>
  </Rule>
 </Policy>
</PolicySet>
```

Figure 18 Role-based time constraints

Through the separation of role definition, authority definition and role authority constraint definition, it is easy to realize the mapping relationship from role to authority. Meanwhile, it can also ensure the description of constraints in the authorization process.

VII. CONCLUSION

This paper provides description method of each element of spatial access control policy by using user-oriented author language VPL and deployment-oriented language GeoXACML, especially the policy description of time environment and multi-granularity spatial resource. And then, this paper gives the translation rule between two languages and realizes VPL - GeoXACML access control policy translation module based on the compiling principle. For the future work, it is required to provide automation standard policy translation tool for the enterprise development personnel, so as to realize automatic translation from policy described by UML to policy described by GeoXACML.

ACKNOWLEDGMENT

This work is partially supported by National Natural Science Foundation of China (No.41074010, No.41171343), A Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD), Graduate Student Research and Innovation Plan Fund of JiangSu Province (No.CX09B_116Z, No.C-X10B_156Z), and the Special Fund from the Central Colleges basic Scientific Research Bursary (No.2010QNB21), thanks for their support.

REFERENCES

[1] Li Bin, Zhao Lingjun. A Policy-based adaptive web services security framework. Journal of Software. 2011: 2456-2463.

[2] Moffett J D, Sloman M S. Policy hierarchies for distributed systems management [J]. IEEE Journal on Selected Areas in Communications 11(9), 1993:1404-1414.

[3] Bandara, A. K., Lupu, E. C., Russo, A. Using event calculus to formalize policy specification and analysis[C]. In Proc. of the 4th IEEE Workshop on Policies for Distributed Systems and Networks (Policy 2003), 2003:1-14.

[4] Bandara A. K, Lupu E. C, Moffett J, et. al. A goal based approach to policy refinement [C]. Fifth IEEE International Workshop on Policies for Distributed Systems and Networks, IBM T J Watson Res. Lab., Yorktown Heights, NY, USA: ACM Press, 2004:3-7.

[5] Rubio-Loyola J, Serrat J, Charalambides, M., et al. Using Linear Temporal Model Checking for Goal-oriented Policy Refinement Frameworks[C].In Proc. of the Sixth IEEE International Workshop on Policies for Distributed Systems and Networks.2005:181-190.

[6] Rubio-Loyola, J., Serrat, J., Charalambides, M., et al. A functional solution for goal oriented policy refinement [C]. In Proc. of the Seventh IEEE International Workshop on Policies for Distributed Systems and Networks.2006:133-144.

[7] Rubio-Loyola, J., Serrat, J., Charalambides, M., et al. A methodological approach towards the refinement problem in policy-based management systems [J]. IEEE Communications Magazine, 2006.44(10):60-68.

[8] Lin Li, Huai Jin-Peng, Li Xian-Xian. Attribute-based access control policies composition algebra. Journal of Software. 2009, 20(2): 403-414.

[9] Albuquerque J. P. D., Krumm H. Policy modeling and refinement for network securitySystems[C]. In: B.Firozabadi, W.Winsborough, A. Sahai (eds.).Proceedings of the 6th IEEE International Workshop on Policies for Distributed Systems and Networks. Washington, DC,USA: IEEE ComputerSociety,2005.24-33.

[10] Albuquerque J. P. D. Scalable model-based policy refinement and validation for network security systems [R], Tech.Rep.IC-06-005, Institute of Computing,University of Campinas. March 2006.

[11] Albuquerque J. P. D, Krumm H. On scalability and modularization in the modelling of network security systems[J]. 10th European Symposium on Research in Computer Security, Milan,Italy, 2005.9, Berlin Heidelberg, Germany. Springer-Verlag. Lecture Notes in Computer Science 2005, 3679:287–304.

[12] Beigi, M, Calo, S., Verma D. Policy Transformation Techniques in Policy-based Systems Management [C].IEEE International Workshop on Policies for Distributed Systems and Networks, Yorktown, NY, 2004.6:13-22.

[13] DAI Xiang-dong. Research on extensible policy transformation mechanism based on two-phase transformation. Computer Engineering and Design, 2008, 29(21):5569-5571.

[14] Extensible Access Control Markup Language (XACML) Version 2. Standard, OASIS, February 2005[EB/OL].

Aijuan Zhang received her B.S. degree in computer science from CUMT in June 2002 and her M.S. degree in computer science from CUMT in June 2005. She is currently working towards her Ph.D. degree in Spatial Informatics. Her current research interest includes distributed GIS security and services.