Alban Gabillon

Patrick Capolsini

Nov. 2009

Modeling Security Policies for Geo Data
Politiques de sécurité pour données géographique

Patrick Capolsini

Université de la Polynésie Française (UPF)
BP 6570 Faa'a aéroport
TAHITI – Polynésie Français

Context of the study

- FLUOR project (ANR SESUR 2007)
  - ENST Bretagne
    - ✓ Designer or the Or-BAC Security Model (Organization Based Access Control)
  - GePaSud (Géosciences du Pacifique Sud) Laboratory University of French Polynesia
    - ✓ Geosciences – Geomatics Lab

Publications

- A. Gabillon and P. Capolsini. *Dynamic Security rules for Geo Data. in International workshop on Autonomous and Spontaneous Security (SETOP'09). Sept. 2009. St Malo, France: Springer-Verlag.*
- P. Capolsini and A. Gabillon. *Security Policies for the visualization of Geo Data. in proceedings of SIGSPATIAL ACM GIS 2009 International Workshop on Security and Privacy in GIS and LBS (SPRINGL'09). 2009. Seattle, WA: ACM Digital Library.*

Presentation overview

I. **Goals of the study**
II. Or-BAC model presentation
III. Spatial data model
IV. Taxonomy of spatial contexts
V. Example of a security policy
VI. Comparison with related works
VII. Conclusion and future works

Goals of the study (1/3)

- Growing needs of security policy for mobile subjects and objects
- Reminder: Dynamic Security Rules
  - Security rules (Permission, Prohibition) are activated according to a given context
- Goal: Model dynamic security rules based on spatial contexts

Identify and model various spatial contexts

Goals of the study (2/3)

3 possible solutions:

1. Use an existing security model for spatial applications
   - ✓ Geo-RBAC (Geographic Role Based Access Control)
   - ✓ GSAM (Geo-Spatial Authorization Model)
2. Use an existing generic authorization model
   - ✓ Or-BAC (Organization-based Access Control) which uses a first order logic language to model every type of context
3. Define our own new security model

Goals of the study (3/3)

Reformulated goals:

- Complete the Or-BAC language with spatial functions and predicates to represent spatial contexts
- Propose a taxonomy of spatial contexts
- Show how to model spatial contexts using Or-BAC
- Write security rules based on such spatial contexts

Presentation overview : where are we ?

I. Goals of the study

II. Or-BAC model presentation

III. Spatial data model

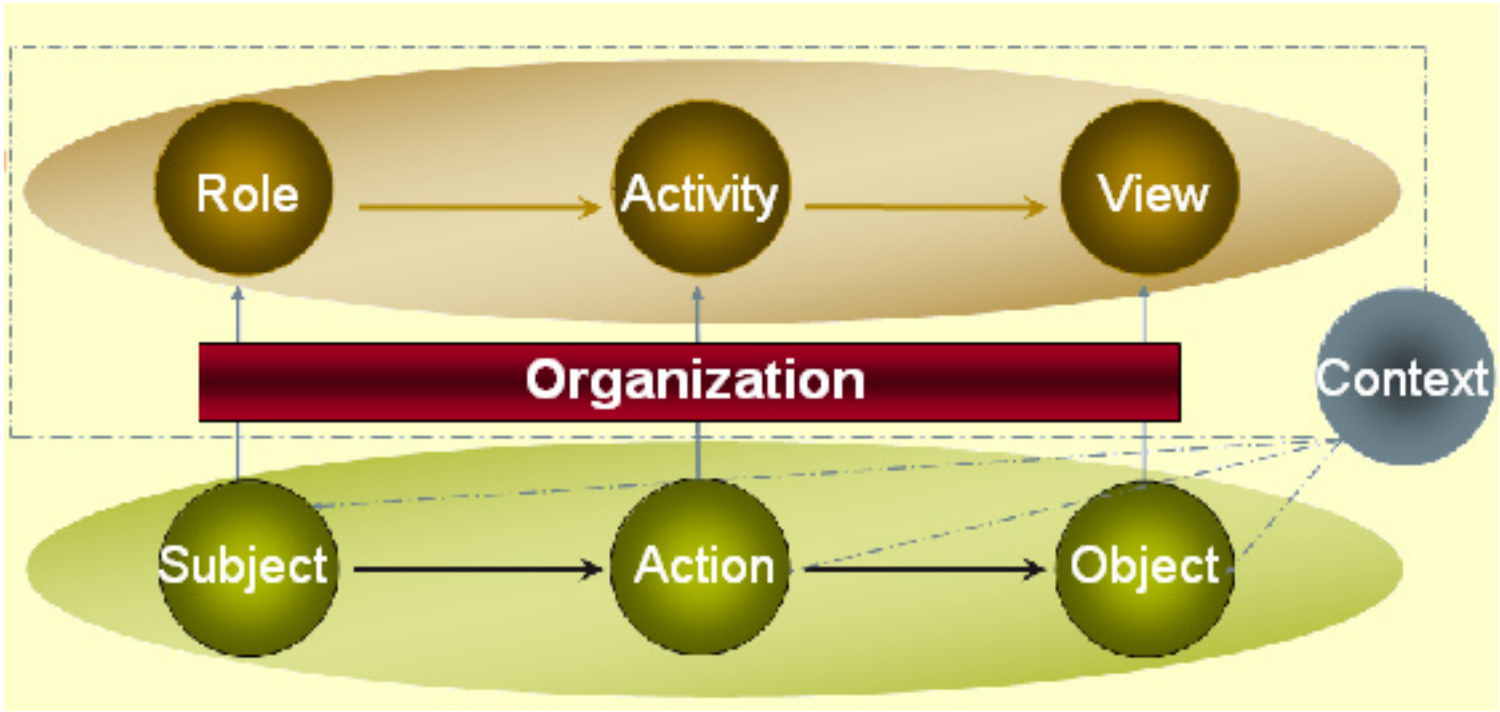
IV. Taxonomy of spatial contexts

V. Example of a security policy

VI. Comparison with related works

VII. Conclusion and future works

Or-BAC Model (2/8) : The Basis



Or-BAC Model (3/8) : Contexts

- Or-BAC context : any condition involving
  - a subject
  - an action
  - an object
- Defined using predicate *Hold*
  - *Hold(org,s,a,o,c)* : context *c* involving subject *s*, action *a* and object *o* is active
- Combine using AND, OR and NOT
- Example:

$$\forall s \in S, \forall a \in A, \forall o \in O, Hold(hospital, s, a, o, treating\_doctor)$$
$$\leftrightarrow name(o) \in patients(s)$$

Presentation overview : where are we ?

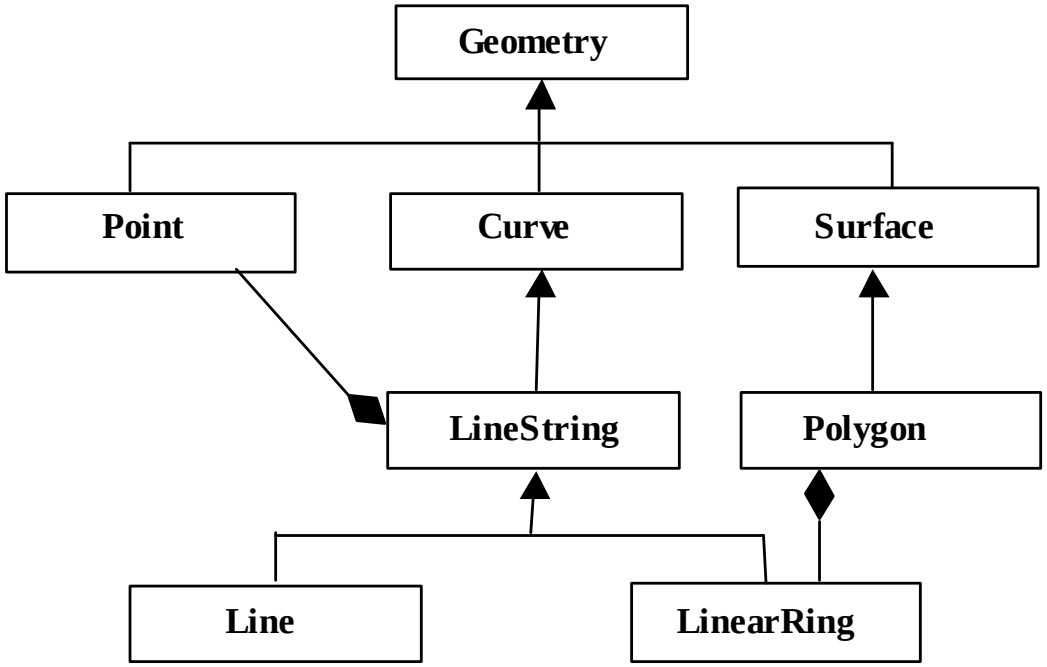
I. Goals of the study
II. Or-BAC model presentation
III. Spatial data model
IV. Taxonomy of spatial contexts
V. Example of a security policy
VI. Comparison with related works
VII. Conclusion and future works

Spatial data model (1/8)

- Or-BAC language to specify contexts is based on first order logic
- We extend this language with functions and predicates defined by the OGC OpenGIS Geometry Model
- Hypothesis : all objects are geo-referenced according to the OpenGIS Geometry Model

Spatial data model (2/8) : Geometric objects

- Description : set of descriptive attributes
- Geometry : Location + Shape (simplified OpenGIS Geometry Model classification)



Spatial data model (4/8) : Spatial functions

- Arguments : one or two geographic objects
- Returns : a scalar or a new geographic object
- 11 spatial functions introduced in the Or-BAC language :

✓ *distance*
✓ *buffer*
✓ *convexHull*
✓ *intersection*
✓ *union*
✓ *difference*
✓ *symmetric difference*
✓ *interior*
✓ *boundary*
✓ *exterior*
✓ *dimension*

Spatial data model (6/8) : Spatial predicates

- Used to test for the existence of a specified topological relationship between two geometric objects
- 8 spatial predicates introduced in the Or-BAC language :

✓ *Equals*
✓ *Disjoint*
✓ *Intersects*
✓ *Touches*
✓ *Crosses*
✓ *Within*
✓ *Contains*
✓ *Overlaps*

Spatial data model (8/8) : Moving objects

- Velocity attributes
  - *speed*: a scalar >= o
  - *direction*: an angle with the geographic North, which value is between 0° and 360° (N/A if speed is 0)
- Example: If *p* is a moving object then *speed(p)* represents its speed and *direction(p)* its heading.

Presentation overview : where are we ?

I. Goals of the study
II. Or-BAC model presentation
III. Spatial data model
IV. Taxonomy of spatial contexts
V. Example of a security policy
VI. Comparison with related works
VII. Conclusion and future works

Taxonomy of spatial contexts (1/8)

Related to the position of the subject

- Based on the position of subjects enrolled in a given role
- Basis for Location Based Systems (LBS)

$$\forall s \in S, \forall a \in A, \forall o \in O, Hold(1^{st}\ Battalion, s, a, o, InFiringzone)$$
$$\leftrightarrow \quad Within(s, Firingzone)$$

Permission(1st Battalion, Recruit, Fire, Target, InFiringzone)

Recruits from the first battalion have the permission to fire on targets if and only if they are inside the firing zone.

Taxonomy of spatial contexts (2/8)

Related to the position of the object

$$\forall s \in S, \forall a \in A, \forall o \in O, Hold(1^{st}\ Battalion, s, a, o, Intrusion)$$
$$\leftrightarrow \quad Within(o, Securityzone)$$

Permission(1st Battalion, Sentry, Arrest, Civilian, Intrusion)

Sentries from the first battalion have permission to arrest any civilian located within the security zone.

Taxonomy of spatial contexts (3/8)

Related to the positions of both the subject and the object

$$\forall s \in S, \forall a \in A, \forall o \in O, \forall d \geq 0, Hold(1^{st}\ Battalion, s, a, o, Firingrange)$$
$$\leftrightarrow distance(s, o) \leq 0.5$$

Permission(1st Battalion, Artillery, Fire, Tanks, Firingrange)

Artillery from the first battalion have permission to fire on tanks which are within the range of 500 meters.

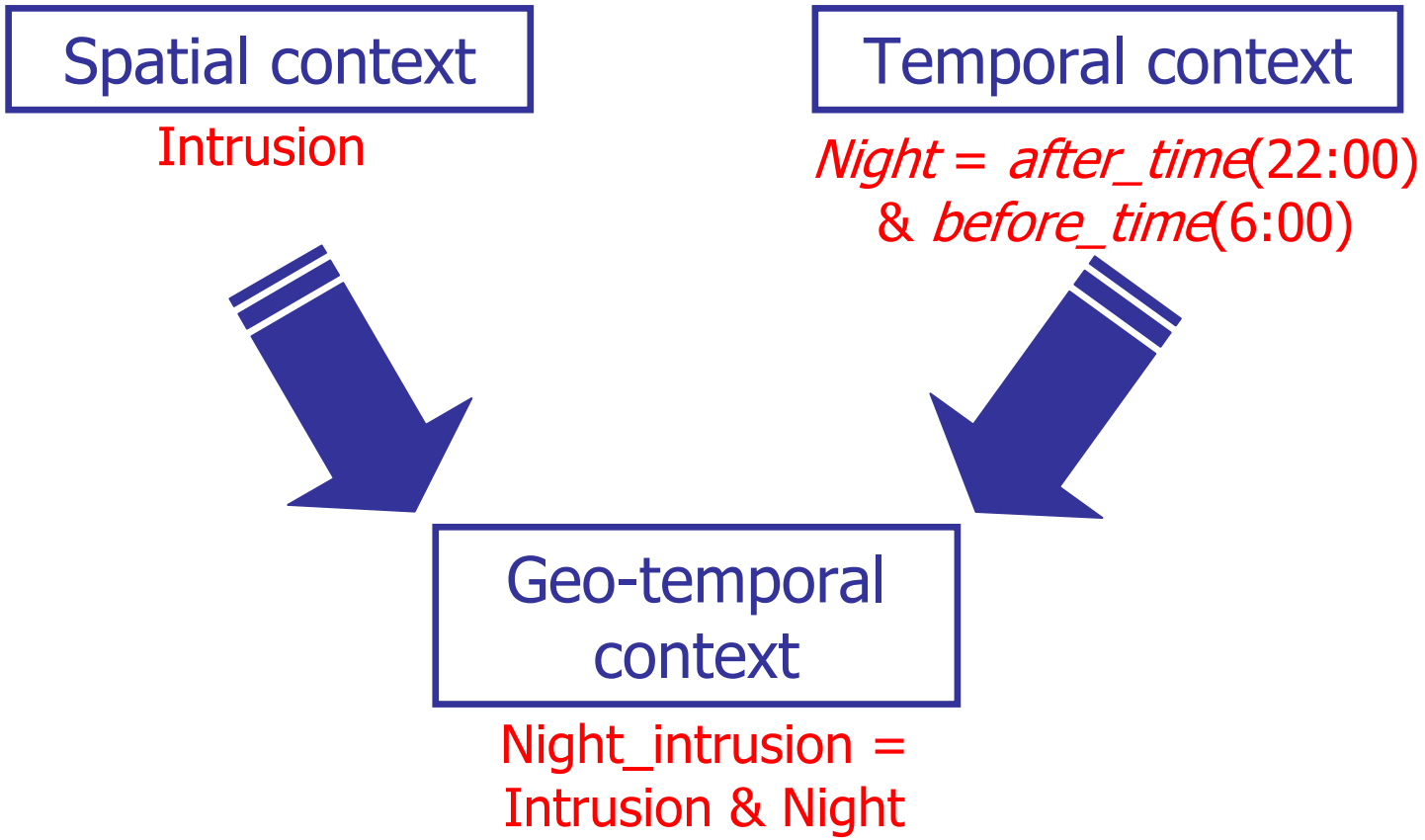
Taxonomy of spatial contexts (4/8)

Or-BAC built-in temporal contexts

- Or-BAC defines functions returning temporal contexts
  - *before_time*
  - *after_time*
  - *before_date*
  - *after_date*

Taxonomy of spatial contexts (5/8)

Geo-temporal contexts



Taxonomy of spatial contexts (6/8)

Related to the visualization of spatial data

- In some models, zoom-in is considered as a separate privilege (like *display* or *write*)
- We prefer to model the zoom-in operation as a context of another operation (*display* for instance)
- Context mzf (maximum zoom-in factor):

$$\forall org \in Org, \forall s \in S, \forall a \in A, \forall o \in O, \forall z \geq 1, Hold(org, s, a, o, mzf(z)) \leftrightarrow scale(a) \leq (z \times Defaultscale)$$

Permission(1st Battalion, Soldiers, Display, Barrack_Map, mzf(2))

Soldiers from the first battalion have the permission to display maps of barracks with a maximum zoom-in factor of 2.

Taxonomy of spatial contexts (7/8)

Related to movement

$$\forall org \in Org, \forall s \in S, \forall a \in A, \forall o \in O, Hold(org, s, a, o, SameVelDir)$$
$$\leftrightarrow speed(s) \leq (1.1 * speed(o)) \wedge (0.9 * speed(o)) \leq speed(s)$$
$$\wedge direction(s) \leq (5 + direction(o)) \wedge (direction(o) - 5) \leq direction(s)$$

Permission(1st Battalion, Tank, Communicate, Tank, SameVelDir)

Tanks at first battalion are allowed to communicate with each other provided they are moving in the same direction and at the same speed.

Taxonomy of spatial contexts (8/8)

Summarized taxonomy of contexts

- Related to subject position
- Related to object position
- Related to both subject and object positions
- Geo-temporal
- Related to visualization of spatial data
- Related to movement

Presentation overview : where are we ?

I. Goals of the study
II. Or-BAC model presentation
III. Spatial data model
IV. Taxonomy of spatial contexts
V. Example of a security policy
VI. Comparison with related works
VII. Conclusion and future works

Application : entities

roles

activities

views

Driver

AmbulanceDriver

TaxiDriver

Display

Query

UpDate

SpatialObject

Road

MainRoad

SecondaryRoad

Hospital

MilitaryHospital

GasStation

organizations

Abstract entities

Concrete entities

Empower

TransFast

Use

Consider

some Amb drivers

some Taxi drivers

ShowGeometry
parameter : *scale*

ShowDescription

Delete

UnDelete

some Main Roads

some Sec. Roads

some Hospitals

some Mil. Hospi

some Gas Stations

subjects

actions

objects

Application : contexts

mzf ➔

$$\forall s \in S, \forall a \in A, \forall o \in O, \forall z \geq 1, Hold(TF, s, a, o, mzf(z)) \leftrightarrow scale(a) \leq (z \times Defaultscale)$$

radius ➔

$$\forall s \in S, \forall a \in A, \forall o \in O, \forall d \geq 0, Hold(TF, s, a, o, radius(d)) \leftrightarrow distance(s, o) \leq d$$

On_theway ➔

$$\forall s \in S, \forall a \in A, \forall o \in O, Hold(TF, s, a, o, On\_theway) \leftrightarrow \exists r, (Use(r, Road) \wedge Within(s, r) \wedge Touches(o, r))$$

Application : contexts

$$Rush\_hours = (after\_time(7:00)\ \&\ (before\_time(9:00))$$

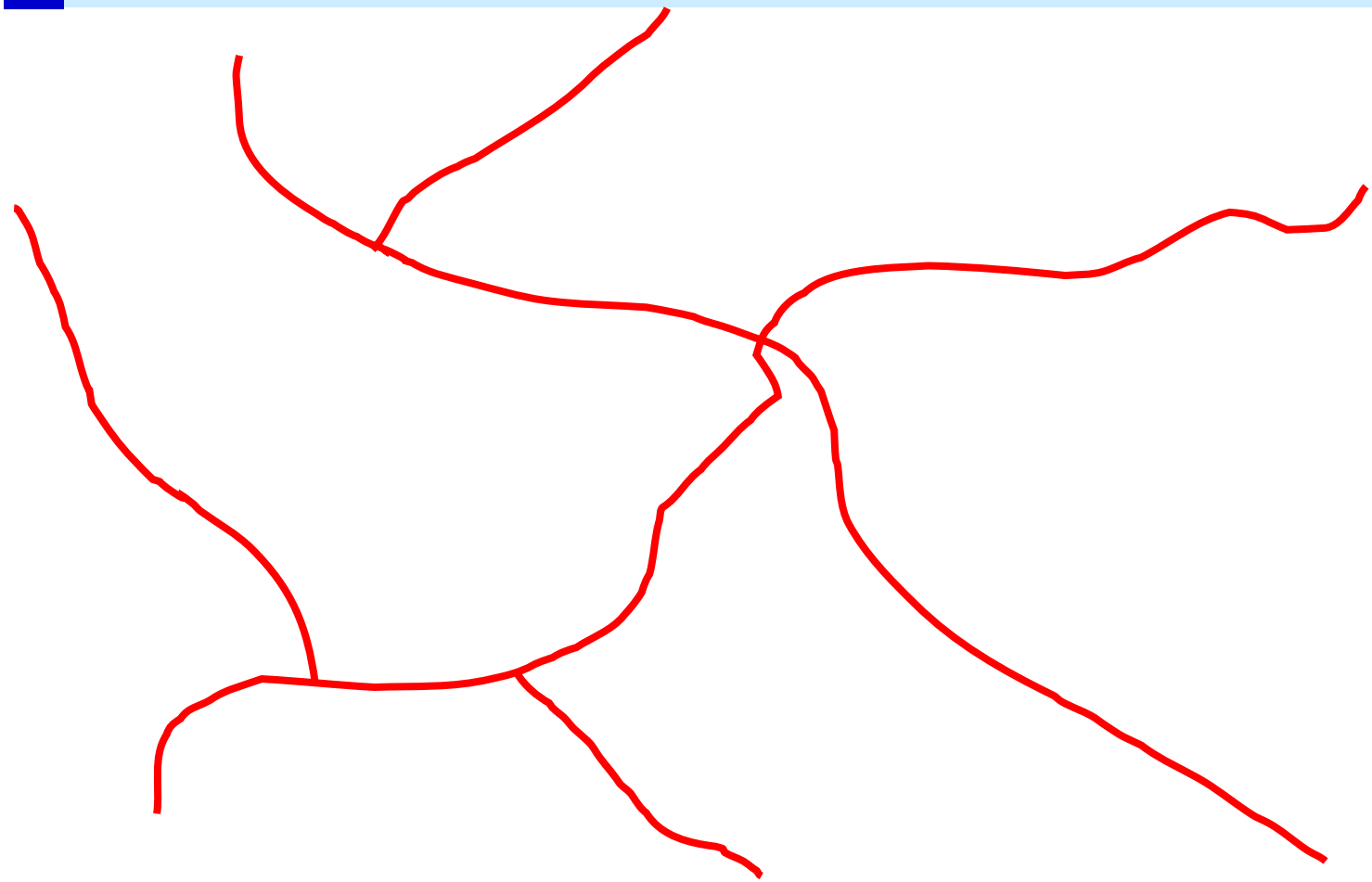
Rush_hours ➔ $\oplus(after\_time(17:00)\ \&\ (before\_time(19:00))$

$$\forall s \in S, \forall a \in A, \forall o \in O, Hold(TF, s, a, o, Not\_moving)$$

Not_moving ➔ $\leftrightarrow speed(s) = 0$

All drivers have the permission to display
main roads at the default scale

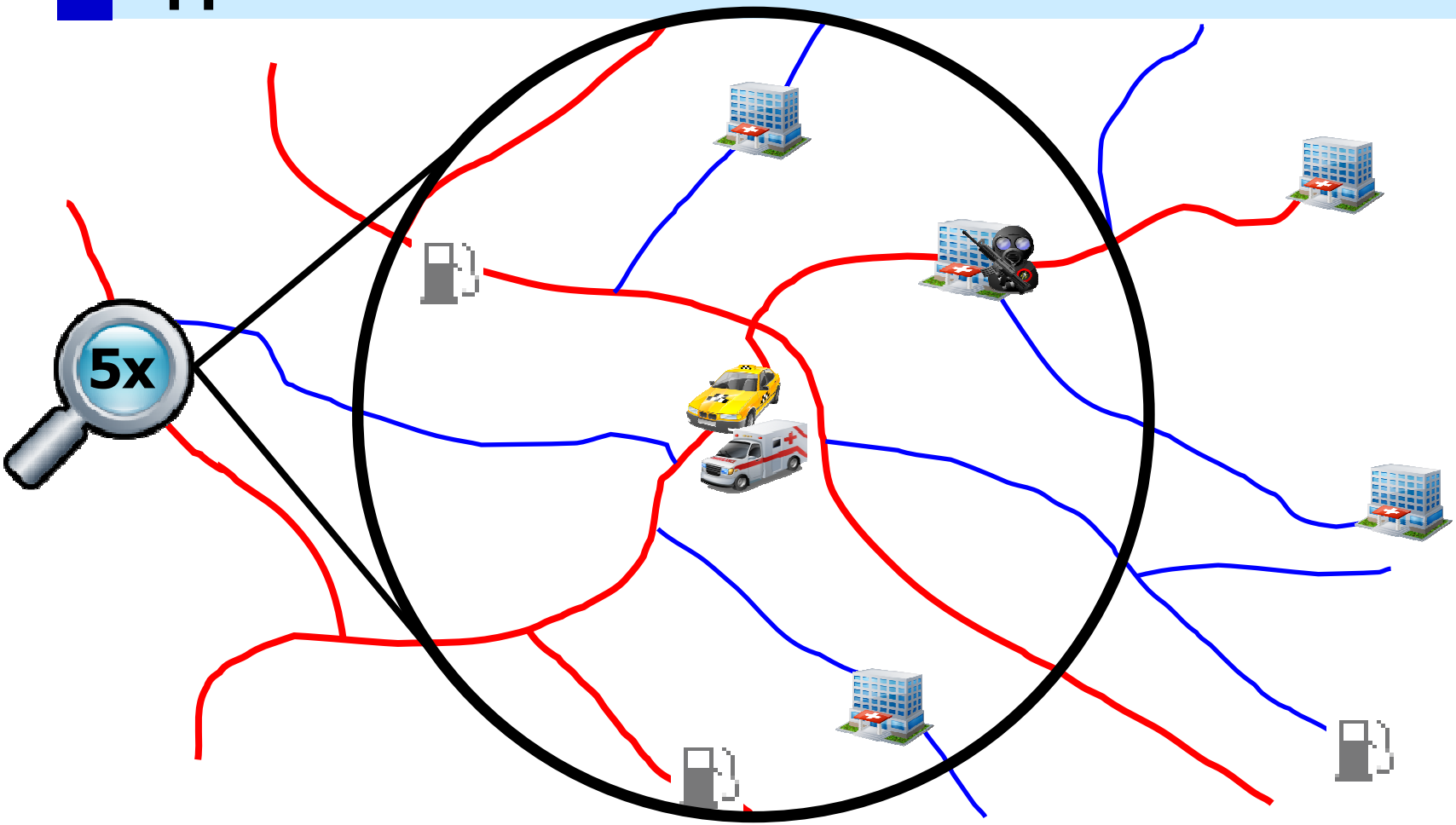
Application : Rule 1



$$Permission(TF, Driver, Display, MainRoads, mzf\ (1))$$

All drivers have the permission to display **any spatial object** within a radius of 40 km with a mzf of 5

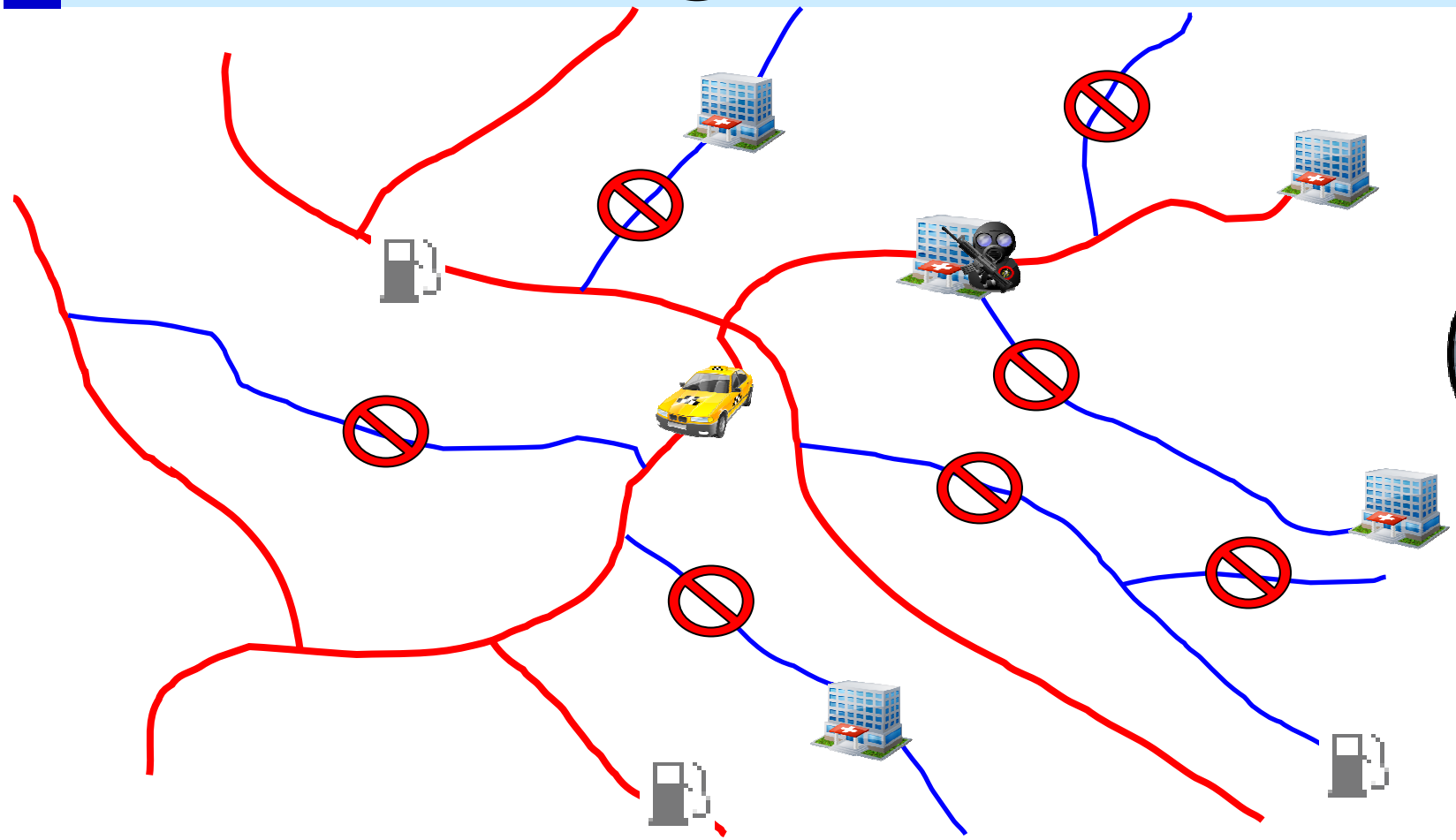
Application : Rule 2



$$Permission(TF, Driver, Display, SpatialObjects, mzf\ (5)\ \&\ radius(40))$$

Taxi drivers are prohibited to display **secondary roads** outside rush hours

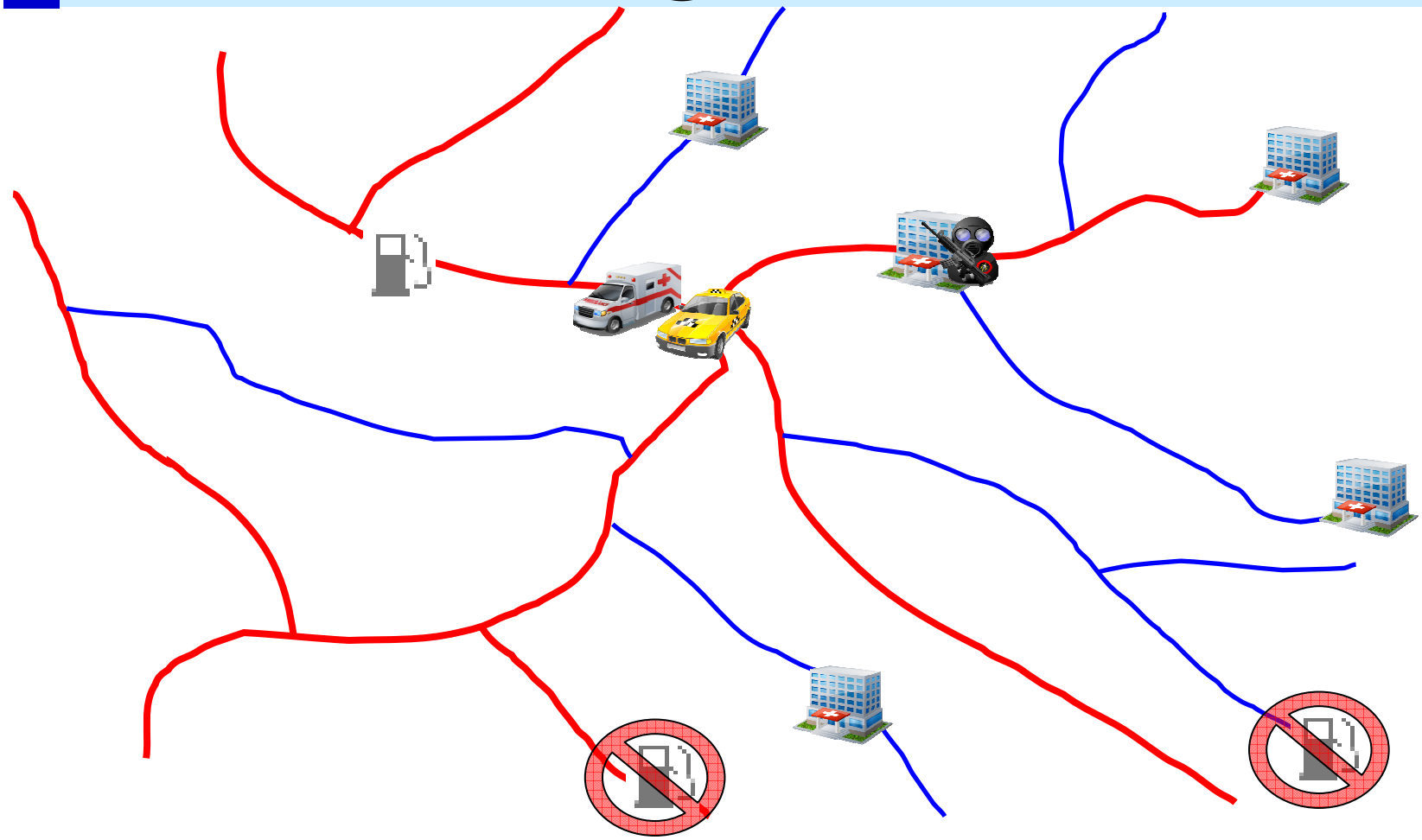
Application : Rule 3



Prohibition(TF,TaxiDriver,Display,SecondaryRoads,Rush_hours)

All drivers are <u>prohibited</u> to display **gas stations** which are not on their way

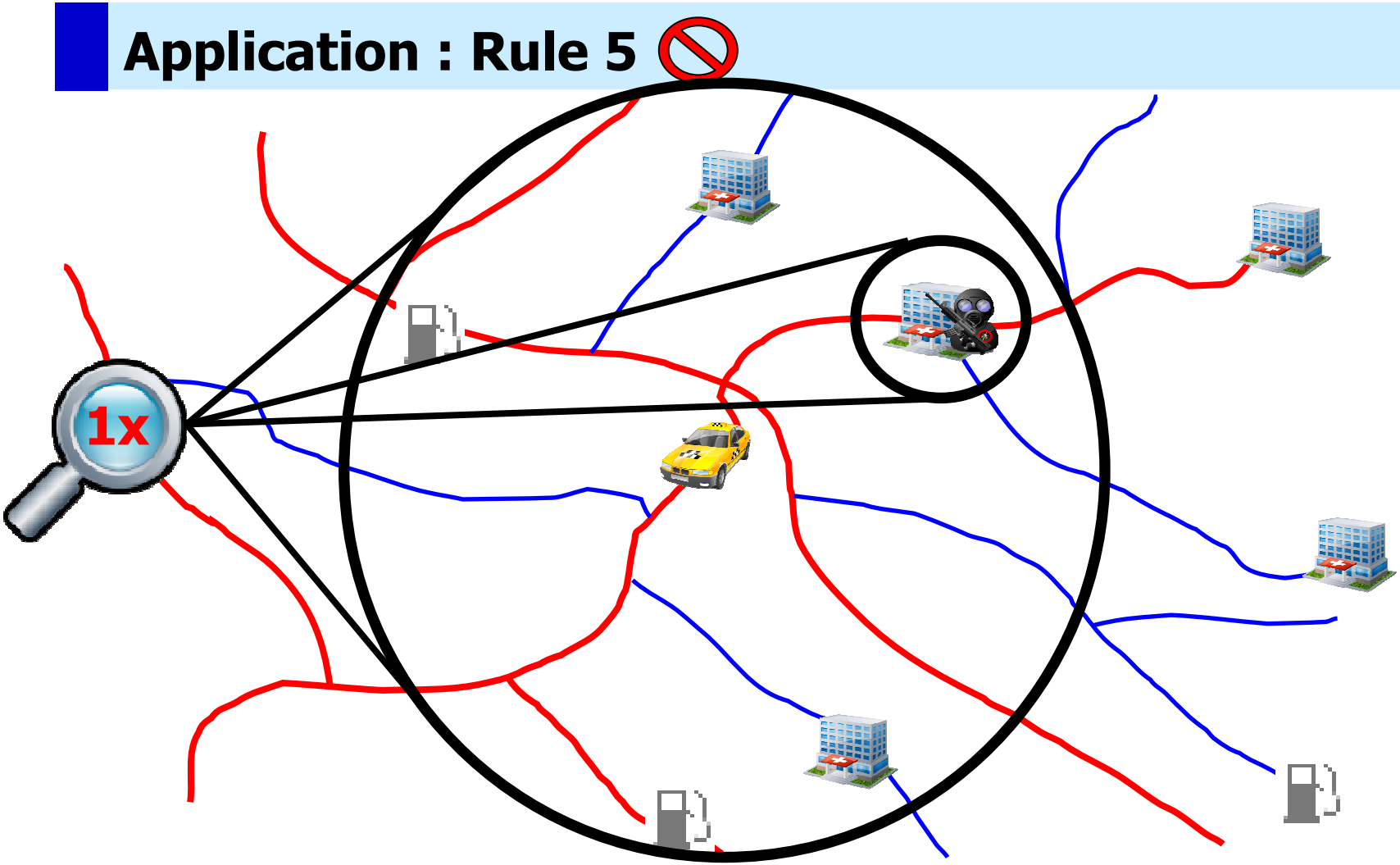
Application : Rule 4



$$Prohibition(TF, Driver, Display, GasStation, \overline{On\_theway})$$

Taxi drivers are prohibited to display **military hospitals** with a mzf greater than 1

Application : Rule 5



Prohibition(TF,TaxiDriver,Display,MilitaryHospital,$\overline{mzf(1)}$)

Application : Rules 6, 7 and 8

Rule 6 ➔

$$Permission(TF, Driver, Query, SpatialObjects, radius(40))$$

Rule 7 ➔ 

$$Prohibition(TF, TaxiDriver, Query, Hospital, Default\_ctx)$$

Rule 8 ➔

$$Permission(TF, Driver, Update, Road, radius(40) \,\&\, Not\_moving)$$

Presentation overview : where are we ?

I. Goals of the study
II. Or-BAC model presentation
III. Spatial data model
IV. Taxonomy of spatial contexts
V. Example of a security policy
VI. Comparison with related works
VII. Conclusion and future works

Comparison with related works

GeoRBAC and GSAM

- *Ad-hoc* models for specific applications : mainly based on user's location (geo-RBAC) or mainly dedicated to satellite imagery (GSAM)
- No formal definition of the concept of context
- Spatial role leads to the multiplication of roles
  - ➔ policy administration becomes complex
- No conflict detection and resolution

Presentation overview : where are we ?

I. Goals of the study
II. Or-BAC model presentation
III. Spatial data model
IV. Taxonomy of spatial contexts
V. Example of a security policy
VI. Comparison with related works
VII. Conclusion and future works

Conclusion

- Proposed to extend the core Or-BAC language with some spatial primitives
- Proposed a typology of various spatial contexts
- Illustrated some potential applications of geo-temporal contexts with a real life application

Future works

- Describe new visualization contexts
- Extend MotorBAC with the defined spatial functions and predicates
- Define methods to derive automatic answers to questions like:
  - Where should I be located to gain access to this object ?
  - Which objects can be accessed according to my current position ?
- Investigate the emerging concept of *spatial/location privacy protection policies*

Alban Gabillon

Patrick Capolsini

Nov. 2009

Thank you for your attention
Any question ?

This work was conducted as part of the ANR funded project under reference
ANR-SESUR-2007-FLUOR

Université de la Polynésie Française (UPF)
BP 6570 Faa'a aéroport
TAHITI – Polynésie Français

Or-BAC Model (1/8) : The Basis

- Uses the concept of role (as RBAC) to abstract subjects
- Introduces 2 innovative abstract concepts
  - views to abstract actions
  - activities to abstract objects
- Default **Closed** security policy

Or-BAC Model (4/8) : Contexts composition

Three Boolean operators to compose contexts:

AND ➔

$$\forall org \in Org, \forall s \in S, \forall a \in A, \forall o \in O, \forall c_1 \in C, \forall c_2 \in C,$$
$$Hold(org, s, a, o, c_1 \,\&\, c_2) \leftrightarrow Hold(org, s, a, o, c_1) \wedge Hold(org, s, a, o, c_2)$$

OR ➔

$$\forall org \in Org, \forall s \in S, \forall a \in A, \forall o \in O, \forall c_1 \in C, \forall c_2 \in C,$$
$$Hold(org, s, a, o, c_1 \oplus c_2) \leftrightarrow Hold(org, s, a, o, c_1) \vee Hold(org, s, a, o, c_2)$$

NOT ➔

$$\forall org \in Org, \forall s \in S, \forall a \in A, \forall o \in O, \forall c \in C,$$
$$Hold(org, s, a, o, \bar{c}) \leftrightarrow \neg Hold(org, s, a, o, c)$$

Or-BAC Model (5/8) : Security rules

Two levels of security rules:

- Abstract level
  - Defined on a role, an activity, a view and a context

  Permission(hospital, doctor, modify, medical_record, treating_doctor)
- Concrete level
  - Concrete rules are generally automatically derived from abstract rules

  ➔Defined on a subject, an action and an object

Or-BAC Model (7/8) : Security rules

- Derivation of concrete rules

$$\forall org \in Org, \forall s \in S, \forall o \in O, \forall a \in A, \forall r \in R, \forall v \in V, \forall t \in T, \forall c \in C,$$
$$Permission(org, r, t, v, c) \wedge Empower(org, s, r) \wedge Use(org, o, v) \wedge$$
$$Consider(org, a, t) \wedge Hold(org, s, a, o, c) \rightarrow Is\_permitted(s, a, o)$$

- Example: If,
  - Permission(hospital, doctor, modify, medical_record, treating_doctor)
  - Empower(hospital, Alice, doctor)
  - Use(hospital, bob_record, medical_record)
  - Consider(hospital, modify, modify)
  - Hold(hospital, Alice, modify, bob_record, treating_doctor)

Is_permitted(Alice, modify, bob_record)

Spatial data model (3/8) : Geometric objects

- Geometric attributes defined by the OGC may be used to specify contexts
  - If P is a **Point** then *x(P)* and *y(P)* represent the X and Y coordinates of point P
  - If L is a **LineString** then *pointN(L, 3)* returns the third point of LineString L