Protection of Geographic Data
Alban Gabillon, Patrick Capolsini

To cite this version:

HAL Id: hal-01020250
https://hal.archives-ouvertes.fr/hal-01020250
Submitted on 11 Jul 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Protection of Geographic Data

Alban Gabillon and Patrick Capolsini

Université de la Polynésie Française, BP 6570, 98702 FAA’A, French Polynesia
{Alban.Gabillon,Patrick.Capolsini}@upf.pf

Abstract. A powerful and flexible authorization model should be able to cope with various security requirements. In the first part of this presentation, we define a security model to express security policies for spatial applications. Using this model we show how to express dynamic security rules that depend on various spatial contexts. A security policy specifies which objects are authorized and which objects are forbidden. However, in the framework of a geographic application displaying maps, there are several solutions for protecting a sensitive object. Sensitive objects can be hidden, masked, blurred or even replaced by fake objects. Therefore, in the second part of this presentation, we suggest a framework to specify protection mechanisms to enforce whenever a prohibition is derived from the security policy.

Keywords: Access Control, Geo-spatial Data visualization, Map service, Policy Enforcement Point.

1 Introduction

The core RBAC [3] authorization model considers only static security rules. However, in many applications, there is an increasing need for dynamic security rules. A dynamic security rule can be activated/deactivated depending on some context. A context can be a temporal condition, a spatial condition (like the user location), a provisional condition (like the user previous action) etc. With the growing importance of geographic information in various applications, there is a need for dynamic security rules based on some spatial contexts. In the first part of this presentation [1], we define a logic based language for writing security policies for spatial applications. In particular, we try to figure out various types of spatial contexts, and we show how to model these contexts. The first part of this presentation deals with what is represented inside the dashed rectangle of Figure 1. The security policy determines which objects are authorized and which objects are not authorized.

In the second part of this presentation [2], we define a complete framework for protecting prohibited objects. In a traditional database approach, enforcement of the security policy is simply done by removing the unauthorized objects from the final answer to the query. In a geographic database application, things are more complicated. Let us consider a map service building maps from various spatial objects. Some unauthorized objects are simply removed from the final map as it is the
case in a traditional database application, but some other sensitive objects are
protected by using methods which are specific to geographic applications. Examples
of such specific methods are referred to as *blurring, masking, pixelization* or “cut and
paste” (i.e. overlay a sensitive object with another fake objects). The second part of
this presentation deals with what is inside the dotted rectangle. It breaks down as
follows:
- It defines a formal framework for deriving security mechanisms to be enforced on
  unauthorized objects.
- It proposes a Policy Enforcement Point (PEP) algorithm to display the final map
taking into account the protection mechanisms that should be enforced on
unauthorized objects.
We conclude this presentation by giving a sketch of the implementation of our
proposal within the framework of the OpenGIS® Styled Layer Descriptor (SLD)
Profile of the OpenGIS® Web Map Service (WMS) Encoding Standard. A prototype
showing the feasibility of our approach can be found at the following url:

Fig. 1. Protection Mechanisms Model

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

References
ed.): International workshop on Autonomous and Spontaneous Security (SETOP'09), Vol.
Lecture Notes in Computer Science 5939. LNCS 5939 - Springer-Verlag, St Malo, France
SIGSPATIAL GIS 2010 International Workshop on Security and Privacy in GIS and LBS
(SPRINGL'10). ACM, San Jose, CA, USA (2010) 12-17