PRIVATE GRAPHS – ACCESS RIGHTS ON GRAPHS FOR SEAMLESS NAVIGATION

W. Dorner [*], F. Hau, R. Pagany

DIT, Deggendorf Institute of Technology, Technology Campus Freyung, Grafenauerstr. 22, 94078 Freyung
wolfgang.dorner@th-deg.de, felix.hau@stud.th-deg.de, raphaela.pagany@th-deg.de

ISPRS ThS 9

KEY WORDS: Geospatial Data, Security, Access Control, Navigation Graph, Graph Segmentation

ABSTRACT:

After the success of GNSS (Global Navigational Satellite Systems) and navigation services for public streets, indoor seems to be the next big development in navigational services, relying on RTLS – Real Time Locating Services (e.g. WIFI) and allowing seamless navigation. In contrast to navigation and routing services on public streets, seamless navigation will cause an additional challenge: how to make routing data accessible to defined users or restrict access rights for defined areas or only to parts of the graph to a defined user group? The paper will present case studies and data from literature, where seamless and especially indoor navigation solutions are presented (hospitals, industrial complexes, building sites), but the problem of restricted access rights was only touched from a real world, but not a technical perspective. The analysis of case studies will show, that the objective of navigation and the different target groups for navigation solutions will demand well defined access rights and require solutions, how to make only parts of a graph to a user or application available to solve a navigational task. The paper will therefore introduce the concept of private graphs, which is defined as a graph for navigational purposes covering the street, road or floor network of an area behind a public street and suggest different approaches how to make graph data for navigational purposes available considering access rights and data protection, privacy and security issues as well.

1. INTRODUCTION

The spectrum of geospatial data in form of routing has been a broad research field for many years, not only since the introduction of the Global Positioning System (GPS) to the general public in 1983. The popularity of consumer navigation with applications on mobile devices is constantly rising, while both, corporations and research sector, are focussing on indoor-navigation. But mostly, the fact of access rights due to different user groups hasn't been covered scientific paper in detail. This aspect is very important these days, due to increasing security demands. Different authors already pointed out the lack and necessity of proper security implementations at both, outdoor and indoor, domains (Atluri and Chun, 2004)(Bertino et al., 2008), but solutions how to address this demand are still and open question.

It is a first objective of this report to give an overview of several approaches how to solve navigation problems and especially how these problems are solved for various fields of application, but also how aspects of data security, access rights (physical as well as on data) and privacy are addressed. Secondly, concepts of rights management will be compared and discussed to identify available knowledge and illustrate the current state of technology and research at this specific topic and to identify potentials for the application of access rights management on navigation data. Based on this review, concepts and a case study will present first approaches how possible solutions on a conceptual and implementation level could look like.

2. LITERATURE DISCUSSION

2.1 Current Implementations

The Global Positioning System has been brought from a military use to the general public in the 1980's due to an incident of a catastrophic disaster of the Korean Air Lines Flight 007, where 267 air passengers died (Times, 1983). As a result of that, the GPS technology has been released by former US president Ronald Reagan and can be used by the general public without former "selective availability" since then. This term stands for the intentionally created degradation of the GPS' signal quality for non-US military users, formerly intended to protect the geolocation of significant landmarks, and thus the national security of the United States (Parkinson, 1996, p. 603f). The functional principle of the routing using GPS for positioning is based on the graph theory. A navigation graph consists of nodes and edges to create a network of routing paths, where edges represent the road lines and the nodes represent junctions. Colors and weights represent type of traffic way, maximum or average speed as well as distances between nodes. Thus, it is possible to calculate the shortest route as a shortest path using routing and shortest path algorithms, e.g. Dijkstra's algorithm.

With the aid of this technology, many usages within the outdoor section are conceivable. For civilians, it can be used to navigate through complex and personally unknown areas. IfD Allensbach presents data indicating a rise of the usage of smartphone navigation applications from 11.73 million users in 2013 to a number of 17.19 million users in 2015, either used for pedestrian or car navgiation (IfD Allensbach, n.d.). Navigation is still in the focus of research with a strong focus on solutions

[*] * Corresponding Author

for specific problems such as navigation for outdoor festivals, featuring guiding instructions for a more detailed experience (Lin, 2013), and expos, including autonomous navigation of mobile robots (Arras et al., 2003).

But also industrial application are a driver for research in outdoor and indoor navigation. Examples are the coverage of unpaved roads and tracks, roads inside industrial complexes or in general on private ground. In the study by Weigel, Preuss and Brüstel (2010) an approach for off-road navigation for the timber industry of the State of Brandenburg is presented, which covers the lack of navigation solutions on non-asphalt roads. It seems that this concept is also applicable to other industrial sectors, where unpaved roads are a common situation, like the building industry or agriculture (Patino et al., 2009). But even in the aviation industry, pilots require a step-by-step navigation in new, respectively unfamiliar airport environments to retain their orientation. This fact is demonstrated by Guilloton et al. (2011), describing state-of-the-art methods to assist navigation for pilots and suggest improvements to the scenario, where a low visibility could impact the navigation. Also the defence sector is requiring new concept, especially for troops in foreign territories. Especially air units require the technique of the modern terrain aided navigation, which provides high accuracy, achieving precisions of more than ten meters and a high reliability (Yu and Ze-fu, 2011).

Now, if we restrict the navigational area to a smaller environment, the idea of indoor-navigation would come up, where industry and production environments are also potential fields of application. Spampinato et al. (2009) “proposes a stereo-vision-based localization and mapping strategy for vehicular navigation within industrial environments” by the use of natural landmarks, which illustrates the current industrial assignment of autonomous vehicles with implemented navigation solutions, following a route from a start- to an endpoint. The concept of an indoor-navigation can also be found in consumer locations, where the layout plan can be complex and comprehensive, leading to orientation and navigation problems. One example are shopping malls, where Wilk and Karciarz (2014) optimized the map matching algorithm in such buildings with the intention to create a more accurate indoor navigation. Other examples can be found in expos (Pei et al., 2010), etc.

2.2 Security issues and demands

Considering the aforementioned methodologies for indoor-navigation concepts, the aspect of data security hasn’t been addressed yet. In indoor-navigation, several constraints have been listed by Stoffel, Lorenz and Ohlbach (2007):

- Locked doors, requiring authorization to unlock
- Time limited access
- Restricted access in public buildings
- Exits used in special cases

An illustration for this circumstance can be found in Figure 1 where in contrast to a public graph access to a private area, building or individual rooms or floors could be restricted also with regard to a data level.

This central idea is decisive for the question of how to implement the security aspect into the navigation graph. One predestined technology would be the concept of existing rights management, giving only permitted users an access to secured data files, which has a wide range of application in computer and information science. The following examples show real-life implementations of access restrictions, such as secure storage of money, valuable objects, significant information, etc.
According to Bouwman, Mauw & Petkovic the adoption of new applications in a “very complex healthcare environment has led to new security requirements”, which otherwise leads to privacy concerns regarding the external access of sensitive patient records (2008). Therefore, the hospital appears to be one environment where lots of rooms/areas grant restricted access to visitors and patients as well as employees. For protecting relevant data, e.g. patient records, and consider privacy concerns, access to specific rooms should only be granted to authorized personnel. But navigation solutions could contribute to increased physical security if data security and restricted navigation is considered. While being “burdened by health concerns and uncertainty”, patients and visiting relatives or friends have trouble navigating through large buildings, which, if it comes to the worst, leads to forbidden entries of restricted accessible rooms or areas (Fixova et al., 2014).

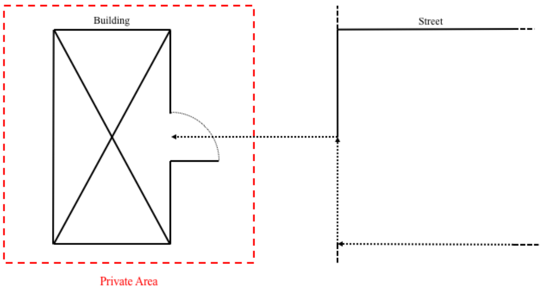


Figure 1 Seamless navigation from a public area to a private one

Additionally, Shih et al. provided a surveillance method for unauthorized access to specific premises, stating that there is a lack of entrance control in diverse sections, e.g. information desks at airports, cash counters in shops, etc. (2006). Especially US airports, where the security level increased since the terrorist attack on 11th September 2011 at the former World Trade Center in New York City and the Pentagon in Washington, D.C., has led to the signing of the Aviation and Transportation Security Act by former US president George W. Bush (*Aviation and Transportation Security Act*, 2001). Thus, this law founded the Transportation Security Administration (TSA) and tightened preliminary security measures (*Aviation and Transportation Security Act*, 2001, p. 17). Examples for this scenario can be found in the areas behind the check-in counter, which airport visitors or family members, not having the intention to travel, aren’t allowed to enter. Furthermore, air passengers also have restricted access at the border control, which is not being allowed to be entered unsolicited, otherwise causing alarm and insurgency. But also underlying geospatial basis data, e.g used for the visualisation of map based navigation information needs to be considered as one facet such as the security of high-resolution geospatial image, road or floor plans. Atluri and Chun point out that a high level of detail information of a vital national building, can lead to espionage, terrorism or cross-border attacks, if such relevant data comes to the wrong hands (2004).

These mentioned examples show the urgency and importance of access restriction and rights management, detaining illegitimate or unauthorized persons from sensitive data or objects.

This contribution has been peer-reviewed.
doi:10.5194/isprsarchives-XLI-B4-579-2016

3. METHODOLOGY

3.1 Technical approach

Bertino et al. brings up several elements to ensure a secure access of such data (2008):

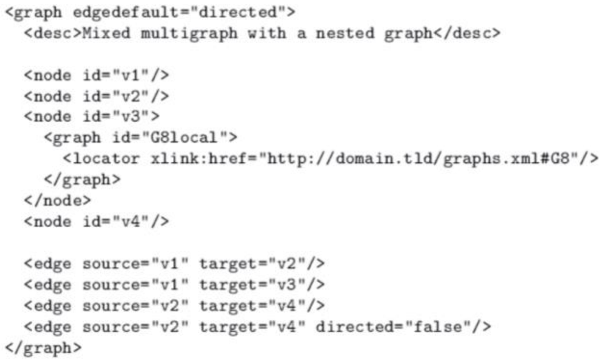
- Design a trust management, which evaluates the level of trust of the end user
- Develop techniques, which allows users to verify the level of trust of geospatial data
- Develop a fundamental security policy, which handles trusted, as well as untrusted GIS applications

As a result of the abovementioned arguments, the explicit field of navigation in restricted areas requires further work to ensure a secure and authorized navigation or better access to underlying geodata (graphs as well as basic data). Therefore, a design concept for that type of navigation is needed, where the information and degree of security can be stored as additional information and the edges of the graph are logically partitioned to hide areas and routes from unauthorized users.

The concept of server-based authentication and authorization can be discussed as a prototype. In this process, a user or a piece of software proves its identity to an application on a server. After a successful authentication, the user or application can be authorized to retrieve a particular kind of function or information (Purser, 2004, p. 51). An applicable scenario would be the storage of geospatial data onto a hosting server, where the access is only available after a successful authentication attempt by the requesting client. The type of authentication can range from a simple model with an identifier and a password to an advanced authentication protocol, based on encryption methods (Purser, 2004, p. 14f).

Another strategy for this purpose would be the concept of a file format, where the content (nodes and edges) contains also additional access data, stored as meta information. Such kind of data can be seen as attributive information, giving more detail to specific geospatial data. This system is commonly occurring in computer science, especially, as already mentioned, in file formats. An appropriate example for that would be the Extensible Markup Language (XML) for the storage of metadata. Those are mostly stored as attributes, which describes the properties and characteristics of some particular main data. Retrospectively, a predestined example, which is used to give a description of graphs, would be GXL (Graph eXchange Language), which “is designed to be a standard exchange format for graph based tools”, although it is now used for tool interoperability (Winter et al., 2002). The XML-based syntax is represented by a list of unordered <node> elements, in combination with a unique identifier, and a connection between a starting and an ending node, called by an <edge> tag. The storage of additional data, a possibility to store edge weights, layout attributes, etc., can be done via the <attr> tag, a child element of a node- or edge-element. While it can be extended by further describing attributes, it lacks the ability to describe information independently from the actual graph data. The paper from Winter et al. stated the addition of further attribute information only with basic data types, e.g. <bool>, <int>, <string> (2002, p. 328). As a consequence, the implementation of an authorized-based XML-syntax with specific elements would cause difficulties.

In contrast to that, the approach via GraphML, an also XML-based file format for graphs, offers the possibility to extend graph data by meta information (Brandes et al., 2002). The basic concept is already described in the beginning of this chapter, containing directed and undirected edges connecting a set of nodes together. However, the relevant key feature is the easy extensibility with other XML-based attributes with the aid of the <key>- and <data>-tags. With that in mind, it seems to be possible to describe further security information (Brandes et al., 2002, p. 8). An example is provided by Brandes et al., featuring a GraphML representation of a nested graph, shown in Figure 2, that could be used to split navigational data depending on access rights.



```
<graph edgedefault="directed">
  <desc>Mixed multigraph with a nested graph</desc>

  <node id="v1"/>
  <node id="v2"/>
  <node id="v3">
    <graph id="G8local">
      <locator xlink:href="http://domain.tld/graphs.xml#G8"/>
    </graph>
  </node>
  <node id="v4"/>

  <edge source="v1" target="v2"/>
  <edge source="v1" target="v3"/>
  <edge source="v2" target="v4"/>
  <edge source="v2" target="v4" directed="false"/>
</graph>
```

Figure 2. A GraphML representation of a nested graph (Brandes et al., 2002, p. 6)

For a concept of a proper rights management, the insight of existing proven techniques is a prerequisite. To give an understanding about the storage of permission rights as metadata, the following section describes the functional principle of a regular local rights management in computer science. Establishd concepts in UNIX systems us a user-group based system to handle access rights and distinguishes:

- User/Owner
- Group
- Other

This proven concept of rights management can be described as followed: The owner of a file or directory is automatically assigned at the creation and determines the file’s user class. Dedicated to this circumstance, a group of users can be assigned with the permission to read or write the file with the assigned owner optionally being a member of this group. The third entity “others” affects all users who either are not the owner, nor a member of the permitted group. Each of those entities has three types of access rights, distributed into the reading, writing and executing privilege. The first one assigns the right to read and display the content of a directory or file for a user group. While the second privilege provides the access to create and edit the content of files, the third allows to execute program files and to switch to permitted directories (Wolfinger, 2013, p. 175f). The combination of that permission system with the access restriction on a navigational perspective would be a recommended choice. While routing edges would be visible to authenticated, thereby permitted users, other could be excluded to view or edit the graph and its routing elements.

A further strategy for our purpose would be the concept of an access control list (ACL). Its objective is to only allow permitted users to access a form of data or information if they have an explicit entry on that list. Analogically, a present real-world application is the reservation of dining tables in the gastronomy, where only the person, who made the reservation is allowed to take a seat (Chin and Older, 2010, p. 60). The workflow of an ACL can be described as the following: An entity identifies themselves to the server and creates a request to access some sort of particular data. In the following, the server, with an implementation of an ACL, compares the inquirer with the entries of the list. If a match exists, the entity will be granted access. The abstract scheme for this description can be seen in Figure 3. In general, the authority, which is the entity controlling the ACL, holds an entry for the permitted subject, which is assigned to an object with pre-set access rights.

$$\mathit{authority}\ \text{controls}\ \left(\mathit{subject}\ \text{controls}\ \langle \mathit{access\ right},\ \mathit{object}\rangle\right)$$

Figure 3. The scheme for the general policy of an ACLs process (Chin and Older, 2010, p. 63f)

On the other hand, the actual access control list can be abstractly expressed in Figure 4. An ACL is usually filled with multiple access control entries (ACEs), each holding an entry of a subject, who is granted to read some specific resource with predefined access rights.

$$\mathit{ACL}\ \text{says}\ \begin{cases} \mathit{subject}_1\ \text{controls}\ \langle \mathit{access\ right}_1, \mathit{object}_1\rangle \wedge \\ \mathit{subject}_2\ \text{controls}\ \langle \mathit{access\ right}_2, \mathit{object}_2\rangle \wedge \\ \cdots \wedge \\ \mathit{subject}_n\ \text{controls}\ \langle \mathit{access\ right}_n, \mathit{object}_n\rangle \end{cases}$$

Figure 4. Abstract scheme of an ACL structure

Finally, the abstract scheme of a request, made by a subject, would look similar to Figure 5.

$$\mathit{subject}\ \text{says}\ \langle \mathit{access\ right},\ \mathit{object}\rangle$$

Figure 5 Abstract scheme of an ACL request

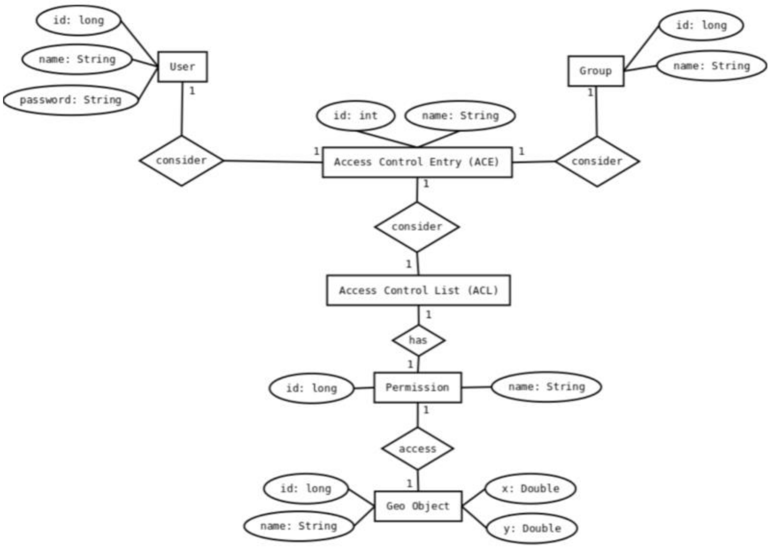


Figure 6 ER model of an Access Control List

Another concept, which should be considered, is the assignment of users to relevant roles, which leads us to the concept of the Role-Based Access Control model (RBAC). Due to the distribution of users to one or multiple groups, it is clearer to control multiple users by having a better overview.

To provide a better illustration of both access control models, the following section describes the corresponding ER model of an ACL and RBAC implementation. As you can see in Figure 6, a user can be assigned with an identifier, a name and an essential password as attributes. That specified user is considered as a record in an Access Control Entry (ACE), which also has a unique ID and particular name of the type String. This record is part of a whole List, called the Access Control List (ACL), where the user/group has some sort of permission to access the needed geospatial object, attributed with an ID, a name and spatial information, e.g. latitude, longitude, altitude.

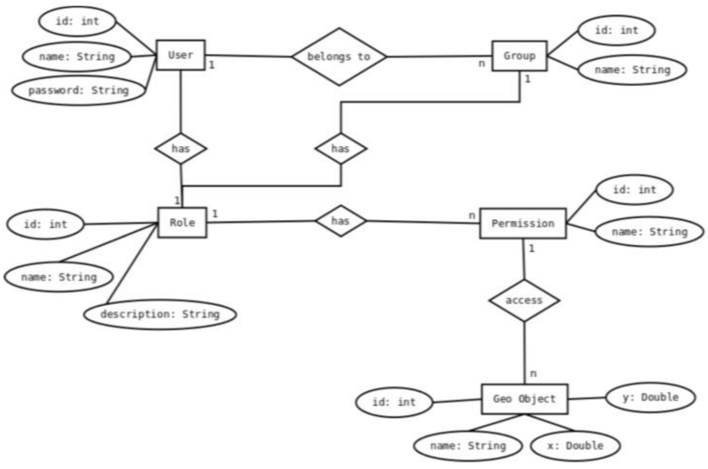


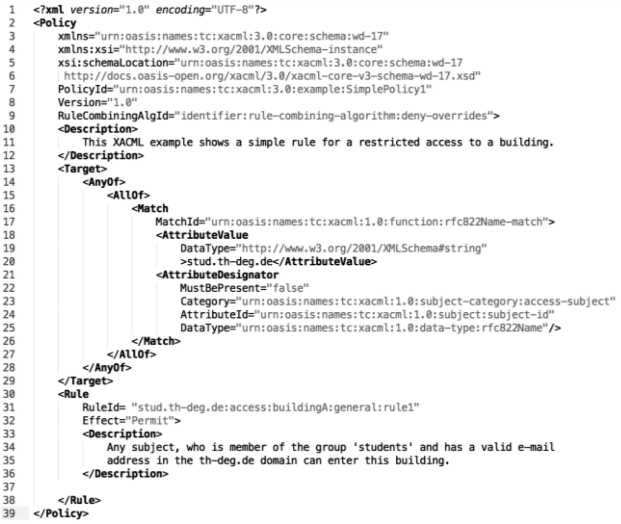
Figure 7 ER model of a Role-Based Access Control model

Although the RBAC model is similar to the ACL model, the differences are in the role model, as a user can be assigned to multiple roles based on his responsibilities. To demonstrate that fact, an ER model to a RBAC model is presented, shown in Figure 7. While a user, equivalently assigned with attributes like the ACL model, can be in multiple groups, it is referred to a role, also having a name, description and an ID. Based on the general RBAC model, it can have, unlike the previous ACL model, multiple permissions, which the user can access his required geospatial objects.

3.1.1 XACML

The realization of an implementation concept can be approached in different ways. A possible implementation strategy would be the storage of access control information with the aid of a XML-compatible language, thus to extend the GraphML file with additional data. Therefore, the Attribute-based Access Control Model (ABAC) XACML is suitable for this task. Even though XACML is primarily developed for ABAC models, it supports RBAC and ACL implementations. The semantic of XACML is distributed into multiple XML-based tags, which allows to define the various access restrictions. An approach with GraphML is used with the extensibility feature, allowing to combine the core features of GraphML with the access control features of XACML.

A simple example for an access control for students permitting to enter a building is shown in Figure 8. This example is based on the examples provided by the OASIS standard manual (OASIS Standard, 2013, p. 25f).
But this technique also comes with some drawbacks. Besides its precision and complete policy description method, the whole structure is complex and hard to understand and use. Furthermore, the fact, that XACML is a low-level language, makes it very difficult to express advanced access control policies. Also, due to its complexity and difficult learning curve, it limits its potential to support the security of web services for developers (El-Aziz and Kannan, 2013, p. 160). Another drawback of this method would be the restriction of having an active connection to the server in case of the request of geospatial data. At this point, the XACML rules cannot be applied to offline usages.



```
<?xml version="1.0" encoding="UTF-8"?>
<Policy
    xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17
     http://docs.oasis-open.org/xacml/3.0/xacml-core-v3-schema-wd-17.xsd"
    PolicyId="urn:oasis:names:tc:xacml:3.0:example:SimplePolicy1"
    Version="1.0"
    RuleCombiningAlgId="identifier:rule-combining-algorithm:deny-overrides">
    <Description>
        This XACML example shows a simple rule for a restricted access to a building.
    </Description>
    <Target>
        <AnyOf>
            <AllOf>
                <Match
                    MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match">
                    <AttributeValue
                        DataType="http://www.w3.org/2001/XMLSchema#string"
                        >stud.th-deg.de</AttributeValue>
                    <AttributeDesignator
                        MustBePresent="false"
                        Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                        AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                        DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name"/>
                </Match>
            </AllOf>
        </AnyOf>
    </Target>
    <Rule
        RuleId= "stud.th-deg.de:access:buildingA:general:rule1"
        Effect="Permit">
        <Description>
            Any subject, who is member of the group 'students' and has a valid e-mail
            address in the th-deg.de domain can enter this building.
        </Description>

    </Rule>
</Policy>
```

Figure 8 Example of an XACML rule

3.1.2 Role-based method

According to the work of Zeng et al., a table, which stores all the information about the relationship of roles and authorities, is saved on the database server (2007). The first phase is about the authentication between server and client. After a successful registration to the database server, the Registration Authority (RA) distributes a role and the client is now able to send a valid request to that particular server with his own certificates and role model. If the server confirms his validity of the clients' certificate, it matches his authorities based on his role. The advantage of this model is, that it doesn't need to redefine certificates and identity authentication interfaces, relying on additional models.

A concept for a framework is presented by Zeng et al., showing several important modules. The CAS (Certificate Authority Service) is the main module, responsible for the publishing and management of certificates. The RA does the management of the registrations of the clients and the distribution of the roles. Between the Spatial Database Enterprise (SDE) and the spatial database the server agent is located. Hence, clients are able to submit their access request to the Spatial Database Management System (SDBMS). In return, the SDE transmits the requested data from the server to the client.

3.2 ACL vs. RBAC

Nevertheless, the RBAC model and group-based ACL system are very similar to each other, while only a few differences can be pointed out. Barkley states, that a group-based ACL "is equivalent to RBAC$_M$", with the condition, that the access control policy described with ACL can be also described with RBAC (1997, p. 129). Therefore, an access control policy described with ACL is equivalent to the RBAC model, if a user can be related to a role, if he is a member of a group, which maps the competencies of the given role. A difference would be, that groups in ACL are implementation-specific. An example can be found in UNIX file systems, where a user can be assigned to only one permitted group while other operating systems have multiple-group support (Ferraiolo et al., 2003, p. 53). Furthermore, a significant difference is the established session relevant access from the RBAC model. Therefore, "with an ACL mechanism, if a user is a member of a group, it is also a member of that specific group for every prospective session established." (Barkley, 1997, p. 130). Meanwhile, the RBAC model features session-based access control, and with that the difficulty of an implementation appears, where it is necessary to find a solution for the case a user requests access to multiple entities. Barkley gives some hints for restricting a user to a single session at a time, which, however, denies the possibility of multi-session access. Another solution would be to restrict a user to only one session on several workstations at a given location (Barkley, 1997, p. 130).

Due to the similarity of both access control models and renunciation of the introduction of session-based access control, we decided to apply the Access Control List paradigm onto the graph structure. The approach can be realized with the role-based solution. However, there may be cases, where not every laboratory worker has access to any arbitrary laboratory. Therefore, this example clarifies the decision for an ACL-based solution.

3.3 Graph partitioning

A further encountering problem would be the handling of the seamless transition from public accessible to private areas at graph level. The difficulty regarding this issue is to separate the graph for each group, depending on their range of duties. For example, a laboratory worker at a university is granted access to dedicated personnel areas and workspaces, while students and visitors shouldn't be allowed to enter it. It is necessary to store the geospatial information in a way, that authorized users are able to access this information while keeping the information invisible for illegitimate users.

Adopting from the basis of graph theory, the methodology of "cut" would be a possible approach for the first step. This method divides a graph at the edges to create multiple subsets. The partitioning of a navigation graph into a subset of publicly available data and a subset of private data is visualized in Figure 9.

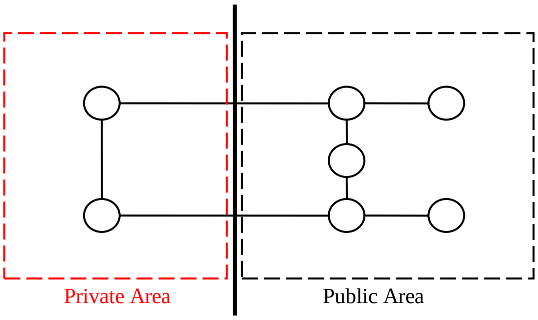


Figure 9 Performing a cut on a navigation graph to create a private and public subset

While this algebraic method sounds suitable for our purposes, it leaves the problem unsolved to store the containing geospatial information. After the division of the graph into multiple subsets, the division of the included meta information is also relevant. Whether this information is stored in subset A or subset B, depends on the rights assigned to each group, if the data should be visible to the members of the group or not. The weighted edges on the graph should be divided in a way, where the public information should be moved to the public subset and private information should remain in the private subset, where an authentication and authorization is needed to view the data.

4. CASE STUDY

For testing the campus of the Deggendorf Institute of Technology was selected. It can be divided into several areas with individual access rights. As mentioned above, the whole campus can be divided into a public and a private area. Publicly accessible areas are the cafeteria, canteen and library. However, inside faculty buildings, the restrictions can be more complex. While lecture rooms and sanitary installations are publicly accessible in the broadest sense, offices and laboratories can only be accessed by keys or keycards. Restrictions regarding the permitted accesses can thereby be time limited (outside of the opening times) or set in case of emergencies. The latter one will be especially important in cases, where the regular navigation path is limited to avoid potentially dangerous places, e.g. elevators, for the safety of the user. Instead, the navigation path will be calculated with the integration of emergency exits and fire escape staircases.

The corresponding roles to the accessible campus area can be divided into the roles student, professor, personnel and visitor. Restrictions regarding the accessibility can differ due to the varying authorities. In general, every person with the intention to attend a lecture can access the lecture rooms during the opening and lecture times. However, the role of a professor or laboratory worker is granted access to their particular office/workplace, while students and visitors aren't permitted to enter it unauthorized.

As an example, the Zollner Elektronik AG Forum building at the campus of DIT can be seen as a seamless transition from a public section to a private area. While it is possible for visitors to enter the building at the front door and to reach the foyer, it is impossible for them to open the doors to the corridor without a functioning keycard. The illustration in Figure 10 helps to clarify the mentioned situation.

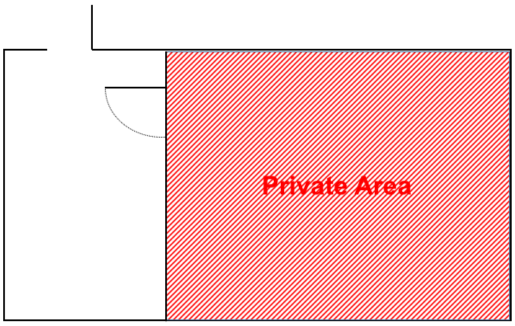


Figure 10 Abstract building plan of the Zollner Elektronik AG Forum's ground floor at DIT

This example is suitable for our intention, to conceal important geospatial data from unauthorized persons and only make it visible to legitimate users. This way the safety and integrity of those data can be retained.
The role based model would allow general navigation on the campus. Access to indoor data can be granted to any user to get navigation in the building and to lecture rooms. The "private" area indicated in red (**Figure 10**) can only be accessed by authorized personal. This can be in general for labs professors or lab workers, in case of additional restrictions due to specific research projects navigation access as well as a view on room layouts could be restricted to an additional role e.g. project-personal.

5. CONCLUSION

As shown above, the discipline of navigation is broadly expanding: Whether it can be found in the outdoor sector, ranging from usual pedestrian and in-car navigation to autonomous navigation in complex structures with multiple levels of floors, e.g. hospitals, airports, shopping malls, etc., adding the difficulty of the third dimension to current navigation solutions. One main aspect to consider in prospective solutions is the security concerning restricted areas, only accessible by authorized users. Several authors indicate the lack of proper security methods for securing geospatial data, which could lead to serious security concerns. Furthermore, various real-life applications of restricted areas/entries were described in previous chapters, where unauthorized entry could risk the security of individuals and safety-relevant data. Places, like hospitals, airports, military bases and industrial sites are relying on the protection of sensitive data.

Therefore, to encounter those issues, several established implementations for rights management and data security were presented, commonly used to ensure the security and integrity of sensitive information. Those approaches range from a user-group access control (ACL) to an advanced access control implementation with the standardized XACML. With it, we are able to implement a high-level structured access control policy on the basis of XML.

With the security issue on one side, we plan to combine those security mechanisms with a navigation graph. As an example, the campus area of the DIT seems to be suitable for our purposes, including many roles and restricted areas, where unauthorized persons are not allowed to enter.

The models presented in this paper ensure a proper security for geospatial graph data. However, this work hasn't involved scenarios, where geospatial data is saved on the clients' storage. Even if those data is only cached, it still could be easily extracted. To avoid these problems concepts are needed, where locally stored data can't be read by potential intruders. One way would be an adequate encryption, which enhances and guarantees information security and privacy.

REFERENCES

Arras, K.O., Philippsen, R., Tomatis, N., de Battista, M., Schilt, M., Siegwart, R., 2003. A navigation framework for multiple mobile robots and its application at the Expo.02 exhibition, in: *IEEE International Conference on Robotics and Automation, 2003*. Proceedings. ICRA '03. Presented at the IEEE International Conference on Robotics and Automation, 2003. Proceedings. ICRA '03, pp. 1992–1999 vol.2. doi:10.1109/ROBOT.2003.1241886

Atluri, V., Chun, S., 2004. An authorization model for geospatial data. *Dependable Secure Comput. IEEE Trans*. On 1, 238–254.

Aviation and Transportation Security Act, 2001. , Public Law.

Barkley, J., 1997. Comparing simple role based access control models and access control lists, in: *Proceedings of the Second ACM Workshop on Role-Based Access Control*. ACM, pp. 127–132.

Bertino, E., Thuraisingham, B., Gertz, M., Damiani, M.L., 2008. Security and privacy for geospatial data: concepts and research directions, in: *Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS*. ACM, pp. 6–19.

Bouwman, B., Mauw, S., Petkovic, M., 2008. Rights Management for Role-Based Access Control, in: *5th IEEE Consumer Communications and Networking Conference, 2008. CCNC 2008*. Presented at the 5th IEEE Consumer Communications and Networking Conference, 2008. CCNC 2008, pp. 1085–1090. doi:10.1109/ccnc08.2007.246

Brandes, U., Eiglsperger, M., Herman, I., Himsolt, M., Marshall, M.S., 2002. GraphML progress report structural layer proposal, in: *Graph Drawing*. Springer, pp. 501–512.

Chin, S.-K., Older, S.B., 2010. *Access Control, Security, and Trust: A Logical Approach*. CRC Press.

El-Aziz, A.A.A., Kannan, A., 2013. A comprehensive presentation to XACML, in: *Third International Conference on Computational Intelligence and Information Technology*, 2013. CIIT 2013. Presented at the Third International Conference on Computational Intelligence and Information Technology, 2013. CIIT 2013, pp. 155–161. doi:10.1049/cp.2013.2585

Ferraiolo, D., Kuhn, D.R., Chandramouli, R., 2003. *Role-based Access Control*. Artech House.

Fixova, K., Macik, M., Mikovec, Z., 2014. In-hospital navigation system for people with limited orientation, in: *Cognitive Infocommunications (CogInfoCom)*, 2014 5th IEEE Conference on. IEEE, pp. 125–130.

Guilloton, A., Arethens, J.-P., Macabiau, C., Escher, A.-C., Koenig, D., 2011. State of the art in airport navigation, in: *Digital Avionics Systems Conference (DASC)*, 2011 IEEE/AIAA 30th. Presented at the Digital Avionics Systems Conference (DASC), 2011 IEEE/AIAA 30th, pp. 4B3–1–4B3–11. doi:10.1109/DASC.2011.6096072

IfD Allensbach, n.d. *Handyfunktionen - Nutzung der Navigationssystem-Funktion in Deutschland 2015* | Statistik [WWW Document]. Statista. URL http://de.statista.com/statistik/daten/studie/214977/umfrage/umfrage-zur-nutzung-der-navigationssystem-funktion-des-handys-smartphones/ (accessed 1.9.16).

Lin, H.-T., 2013. The comprehensive guiding and navigation services on smart phones, in: *Computer Science and Engineering Conference (ICSEC)*, 2013 International. Presented at the Computer Science and Engineering Conference (ICSEC), 2013 International, pp. 97–102. doi:10.1109/ICSEC.2013.6694760

Parkinson, B.W., 1996. *Global Positioning System: Theory and Applications*. AIAA.

Patino, H.D., Tosetti, S., Capraro, F., 2009. Adaptive Critic Designs-based autonomous unmanned vehicles navigation: Application to robotic farm vehicles, in: *IEEE Symposium on Adaptive Dynamic Programming and Reinforcement Learning*, 2009. ADPRL '09. Presented at the IEEE Symposium on Adaptive Dynamic Programming and Reinforcement Learning, 2009. ADPRL '09, pp. 233–237. doi:10.1109/ADPRL.2009.4927550

Pei, L., Chen, R., Liu, J., Tenhunen, T., Kuusniemi, H., Chen, Y., 2010. An Inquiry-based Bluetooth indoor positioning approach for the Finnish pavilion at Shanghai World Expo 2010, in: *Position Location and Navigation Symposium (PLANS)*, 2010 IEEE/ION. Presented at the Position Location and Navigation Symposium (PLANS), 2010 IEEE/ION, pp. 1002–1009. doi:10.1109/PLANS.2010.5507274

Purser, S., 2004. *A Practical Guide to Managing Information Security*. Artech House.

Shih, J.-L., Han, C.-C., Yan, K.-C., 2006. Illegal Entrant Detection at a Restricted Area in Open Spaces Using Color Features, in: *Carnahan Conferences Security Technology, Proceedings* 2006 40th Annual IEEE International. Presented at the Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International, pp. 68–74. doi:10.1109/CCST.2006.313431

Spampinato, G., Lidholm, J., Asplund, L., Ekstrand, F., 2009. Stereo vision based navigation for automated vehicles in industry, in: *IEEE Conference on Emerging Technologies Factory Automation*, 2009. ETFA 2009. Presented at the IEEE Conference on Emerging Technologies Factory Automation, 2009. ETFA 2009, pp. 1–4. doi:10.1109/ETFA.2009.5347238

Standard, O., 2013. eXtensible Access Control Markup Language (XACML) Version 3.0.

Stoffel, E.-P., Lorenz, B., Ohlbach, H.J., 2007. Towards a semantic spatial model for pedestrian indoor navigation, in: Advances in *Conceptual Modeling–Foundations and Applications*. Springer, pp. 328–337.

Times, D.S., Special To The New York, 1983. THE LAST HOURS OF FLIGHT 007: RETRACING THE FATEFUL NIGHT OVER SAKHALIN. N. Y. Times.

Weigel, M., Preuss, T., Brustel, J., 2010. Generating Navigation Capable Maps from User Provided Data with Woodtracker, in: *2010 International Conference on Complex, Intelligent and Software Intensive Systems (CISIS)*. Presented at the 2010 International Conference on Complex, Intelligent and Software

Intensive Systems (CISIS), pp. 544–548. doi:10.1109/CISIS.2010.163

Wilk, P., Karciarz, J., 2014. Optimization of map matching algorithms for indoor navigation in shopping malls, in: *2014 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. Presented at the 2014 International Conference on Indoor Positioning and Indoor Navigation (IPIN), pp. 661–669. doi:10.1109/IPIN.2014.7275541

Winter, A., Kullbach, B., Riediger, V., 2002. An overview of the GXL graph exchange language. *Softw. Vis*. 528–532.

Wolfinger, C., 2013. *Keine Angst vor Linux/Unix*, Xpert.press. Springer Berlin Heidelberg, Berlin, Heidelberg.

Yu, L., Ze-fu, T., 2011. Research and Design of Terrain Aided Navigation System, in: *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*. Presented at the 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), pp. 1–4. doi:10.1109/wicom.2011.6040601

Zeng, Y.H., Wei, Z.K., Yin, Q., 2007. Research on Spatial Database: A Secure Access Mechanism, in: *2007 International Conference on Machine Learning and Cybernetics*. Presented at the 2007 International Conference on Machine Learning and Cybernetics, pp. 2174–2178. doi:10.1109/ICMLC.2007.4370505

This contribution has been peer-reviewed.
doi:10.5194/isprsarchives-XLI-B4-579-2016