Model of security for object-oriented and object-attributed applications

[1] *Pavel P. Oleynik, PhD <xsl@list.ru>*
[2] *Sergey M. Salibekyan, PhD <ssalibekyan@hse.ru>*
[1] *Platov Southern Russian State Polytechnic University (NPI),*
1 Lenin sq., Shakhty, 346500, Russian Federation
[2] *National Research University "Higher School of Economics" (NRU HSE), Institute of Electronics and Mathematics,*
20 Myasnitskaya str., Moscow, 101000, Russian Federation

Abstract. The article describes two approaches for control access rights based on role approach (RBAC) and the use of tables (lists) access rights (ACL). At first, an overview of modern approaches to information security and control user access rights of applications with different architectures is provided. After that, two author's methods of data protection is described. The first approach was developed for the protection of object-oriented applications, the second approach was developed for object-attribute applications used to operating network (graph) databases and knowledge bases. The focus of attention is the first author's approach based on the description of access rights for classes, attributes of classes and objects that has a certain criterion. The approach is implemented by the use of a class hierarchy, composition and structure describing in detail in the article. The article gives examples of specific information systems developed by the first author: information system for scientific conferences that was repeatedly used at the conference "Object systems" (objectsystems.ru) and information system of the beauty salon. Further focus is on the second approach required development of new technique to the information security of network (graph) information structures. The approach developed by second author fully duplicates the functionality of the first approach. In particular, it provides permissions copy when copying of the network data structure, just as in the object-oriented paradigm is a transfer of the properties of parent to child class; the article gives a detailed description of such mechanism. For access control, the method involves the use of a special virtual device. Information about access rights is linked to the node network (graph) if restrict access is needed.

Keywords: Security of information systems; Object-oriented applications; Object System Metamodel; Model of Permissions; object-attribute approach.

DOI: 10.15514/ISPRAS-2016-28(3)-3

For citation: Oleynik P.P., Salibekyan S.M. Model of security for object-oriented and object-attributed applications. Trudy ISP RAN/Proc. ISP RAS, vol. 28, issue 3, pp. 35-50. DOI: 10.15514/ISPRAS-2016-28(3)-3

1. Introduction

At present, the greatest number of new applications is being developed by an object-oriented approach. This paradigm, based on the inheritance technology, allows one to reuse the previously developed elements implemented as classes. The result is the reduced development time and the costs of the whole information system. This is the key advantage when large software products are created. Such systems are typically multi-user systems. At the same time, each category of user needs is only a part of the available information, i.e. there is a problem of access control for multi-user applications. The paper presents a model of access control for object-oriented applications, which was developed by the authors and repeatedly used when developing large applications, and a model of access control in object-attribute computation system.

The paper is organized as follows. Section 1 provides a detailed survey of the papers devoted to similar topics. Section 2 describes the model of access control used by the author. Section 3 shows real examples of implementation of this model and the selected roles of users. Section 4 shows the approach to security in Object-attribute system. At the end of the paper, conclusions on this work and plans for the further study are given.

2. A survey of the available research

Access permission is one of the main problems appearing after the development of the required functionality of the program. Therefore, there are a lot of researches representing different approaches to solving this problem. In [1], the authors propose an approach called business-oriented development (Business-Driven Development), in which the key role is given to the security configuration in the application. The authors use the Model-Driven Architecture (MDA) of architecture of the program. They introduce the concepts of business processes and models at the model level, and then determine the security policies and templates specifying certain rules for them. The present research describes principles of access permission assignment at the level of platform-independent models and the further transformation into platform-dependent models. As a result, the authors present a set of templates for access control providing that their configuration can be adjusted if necessary. This solution is tested using a service-oriented architecture (SOA). To improve the efficiency of the description of the software product life cycle and the corresponding access permissions, the authors propose to make several changes in the languages of software development, such as UML and BPEL. An advantage of the paper is the presence of a number of charts illustrating the proposed solution, as well as many code fragments represented as XML.

The research [2] is more practical and special. It describes a model of adaptive security for multi-agent information systems used by the authors in the medical information system called HealthAgents. The authors start from describing the classical model of access control based on Role-based access control (RBAC) and extend it to be used in multi-agent systems. In their research, the authors present a meta-model that allows one to manage access control by using the UML class diagram. To interact with the security role, the authors introduce the base class Subject attributed with different user permissions. The derived class represents users, organizations and agents. An analysis of research shows that the object-oriented approach for describing access rights is implemented. To describe the process of applying the security policies, the authors depict the Interaction Diagram and present, in the XML-code, an example of test description of access rights of certain users, stored in the system.

The research [3] presents the simulation of multi-level security, integrated within a service-oriented application. In a service-oriented architecture (SOA) that allows one to develop different Web applications, the security is critical. The security is provided by the Web service WS-Security controlled by SOAP messages. These messages may be attacked either by anonymous customers or by trusted clients. In addition, there are other possible types of attacks, for example, the so-called denial of service (DoS), which can exhaust the computer resources and make the Web service unavailable. The described security model consists of three levels. Attention is paid to each of the levels. The obtained multi-level security architecture is presented graphically, namely, various security domains, as well as the composition and structure of the software installed on each of them are depicted. After this, various types of possible attacks at each of the levels are discussed. They are described using the UML Class Diagram. This allows one to analyze the results obtained by the authors and then to design the desired security models based on the results.

The framework for describing the security model of service-oriented applications (SOA) is presented in [4]. The authors focusing on the process of modeling business processes use the BPEL notation. The security model is used with the model of business processes. The authors argue that the difference in approaches of a Business analyst and an Expert to solving the security problems leads to certain permission assignment that ultimately compromise the safety of user data. The authors developed several annotations that allow the security Experts to specify the security model. The proposed approach is demonstrated by an example of business processes of a service-oriented information system providing data about the progress of students. The paper describes a possible implementation of the framework, its basic modules and rules of interaction between the experts and the system.

The paper [5] presents model-oriented templates (patterns) of application security obtained by the authors by an analysis of phases of the application development. The authors examine the applications working in Internet. The templates contain descriptions of solutions to common security problems. The selection of an appropriate pattern depends not only on the situation but on other templates applied earlier, i.e. the dependence between the patterns is taken into account. The authors present an analysis of such dependencies for the first time. The technology of changes of General security templates is proposed on the basis of a rule transformation model based on previously used patterns. This allows one to avoid inappropriate application of the security templates. The authors identify two levels of abstraction: 1) the analysis Phase; 2) the design Phase. Certain modules are responsible for each of them. The software structure and the functions of the modules are considered in detail by the authors. In conclusion, the authors present the syntax of the language used to describe the transformation rules of different patterns. This is similar to languages such as SQL, OCL, LINQ. To demonstrate the obtained results, the authors describe the test information system containing information about the patients of a hospital. The use chart (Use Case) shows the different categories of users and the types of the applied security patterns. Then the structure of the template and the class diagram of the subject area after the application of this decision are illustrated in the form of a UML Class Diagram. This approach is applied to all selected templates, and the complexity of manual and automated applications is evaluated.

In [6], the model-oriented approach to the security applied in the information system of electronic voting is presented. The necessary security requirements, illustrated as the Use Diagrams of UML, were represented as functional requirements at the requirement formalization stage. After this, the authors describe the step-by-step algorithm for identifying and implementing the security requirements and then describe each key element in detail. The paper presents the application architecture and the main computing nodes (computers) which play a certain role. This allows the authors to determine possible vulnerability and attacks against which the system should be projected. The authors also present an approach to the security model implementation in the information system of electronic voting. The model is illustrated by the Sequence Diagram of language UML.

3. The model of access control

Currently, the classical model access control based on roles (Role-based access control, RBAC) has been widely used. Appeared in operating systems, it has the form presented in fig. 1.

This model is popular due to its plain architecture whose functions are as follows. The security system (model) creates multiple roles represented by the Role class. Each role is assigned certain access permissions represented by the Permission class. Permissions are assigned to different objects in the system, which is represented by the class Object. The user described by the User class is attached to at least one role. Moreover, these roles can be inherited, and this can simplify the process of assigning permissions to objects. This scheme is optimal for delineation of rights for objects of one type, for instance, for managing the permissions of access to file system objects (files, directories) in an operating system.

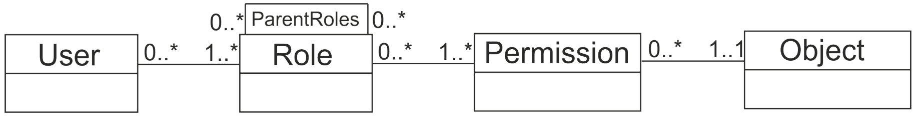

Fig. 1. Classical Role-based Access Control, (RBAC) model

Software applications written in object-oriented programming languages require another security means because it are several types of objects that can be attributed by rights. For the optimal systems design the following optimality criteria (OC) for features are selected:

- access rights for classes (OC1);
- access rights for class properties (OC2);
- access rights for objects (instances of classes) (OC3).

Fig. 2 shows the structure of an optimal model of access rights management for object-oriented applications.

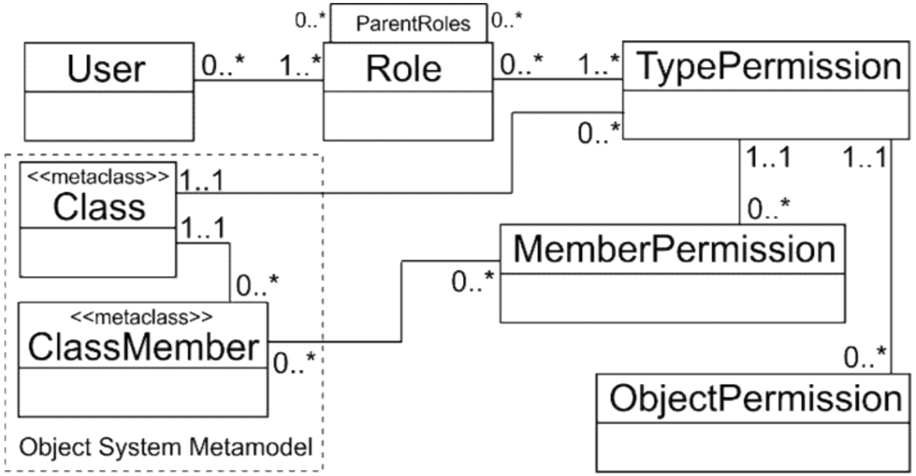

Fig. 2. Classical Role-based Access Control, (RBAC) model

We will examine this figure in more detail. To describe the objects which can be assigned the access rights, an advanced meta-model of the object system is used. In our case, it is enough to have information about the class and attributes (properties) of classes. To match the selected OC1, the class TypePermission which allows differentiating the access rights for the classes is designed. To differentiate the rights according to the properties of classes (see OC2), the class MemberPermission

is introduced. The Class ObjectPermission is used to set permissions on the class copies corresponding to the OC3 requirement.

After clearing the structure and concept implementation, we begin to study of the final system. Fig. 3 shows the implemented-by-authors model of access control for object-oriented applications in the form of class diagrams.

We will consider fig. 3 in more detail. All base classes implementing the key functionality of the security system have names ending by the suffix Base. So the SecuritySystemRoleBase and SecuritySystemUserBase classes form the root class for representing the roles of security and the system user respectively. The TypePermissionMatrixItem class is used to specify the data type (class name) which needs the access rights. The following permission types are used for the classes:

- AllowCreate allows the user to create objects (class instance);
- AllowCreate allows the user to delete objects (class instance);
- AllowNavigate allows the user to display a menu item to view the class instance;
- AllowRead allows the user to view objects of the class;
- AllowWrite allows the user to replace some objects of the class by other.

The class SecuritySystemMemberPermissionsObject allows one to describe the rights to some individual properties and to implement a complex security policy in which the user is prohibited from reading certain attributes of the class.

The class SecuritySystemObjectPermissionsObject is used to distinguish the rights between individual objects of the class which satisfy some predicate. This condition holds in the property Criteria.

The UML diagram shows the relationship between associations which allows one to understand the relationship between classes. In the end, it should be noted that the developed security system allows an unlimited description of the types of access rights in an object-oriented system, which corresponds to the previously identified optimality criteria.

4. Examples of using the model of access control

To implement the above-described model of access control, it is very important to have the meta-information of the object system. The model is physically stored in a relational database according to the principles described in [7]. When designing a meta-model, the key challenge was to develop a hierarchy of meta-classes which allows one to save information about literal types and different classes of domain entities [8-9]. The design of the developed meta-model allows one to realize the subject-oriented approach to designing database applications for different fields [11-13]. In [14-16], the use of the metamodel in the design of information systems is described.

Then paper [16] describes the previously-used security model for access rights applied to an information system used to carry out scientific conferences. The model was repeatedly employed to manage the conference "Object system" (objectsystems.ru). Attention was paid to the security issues at the design stage. For this, the following roles were allocated to the users in the system:

1. The organizer of the conference. He is the main person and the user of the system. His responsibilities include the following tasks:

1. to register the publications;
2. to appoint the reviewer;
3. to verify the corrections made by the authors according to the reviewer comments;
4. to check the payments;
5. to prepare the journal;
6. to send the proceeding books and certificates to the authors of the papers.

2. **The author** writes a paper and sends it to the conference. The author's responsibility is also to revise the paper according to the reviewer's comments about the paper and, if necessary, to pay the registration fee.

3. **The reviewer** checks the author's paper and evaluates its quality. The review includes: to write a review indicating the observations and recommendations for its improvement; to formulate the review result (to accept the paper for publication or to reject it or to send it back for revision). During the preparation of the conference proceedings, the reviewers award nominations to the best papers submitted to the conference. However, in the general case, there are several reviewers.

On the basis of this information, classes and types of access are detected for different roles. Next, instances of classes presented in Figure 3 are created.

The paper [17] describes an information system of a beauty salon. Studying the business logic in this field shows that the system must implement a variety of different financial calculations determining the costs and profitability of the salon. This information can be presented only to the owner of the salon. The following roles are emphasized:

1. **Master**. Main task of the master is to provide services to clients. Therefore, each master can only view (read) the main system directories such as: Operating Schedule, Record/Visit, Schedule of visits, Customer, Leave/Sick leave/Compensatory leave/Absence, Service, Commodity, Certificate, Price, Interest, Master, master Category, room Category, Remnants of goods, Work schedule, Working hours;

2. **Salon administrator**. The main task of a manger is to monitor the activities of the salon. Namely, an administrator registers clients and monitors progress of master work. In the system, an administrator has right to add/edit/delete data from the directories: Visiting Schedule, Customer Master, work Schedule, Record/Attendance, Vacation/Sick leave/Compensatory leave/Absence, Service, Commodity, Certificate, Discount, goods Receipt, Inventory, Price, Stock, Percent, client Category, master Category, service Category, Document, Movement of goods, remaining Stock, Sales, Salon, Working hours, Working time;

3. **Owner of the Salon** has all the same rights as the Administrator of the salon. In addition, he has right to view information from processed forms such as: Wages, Profit, and Profitability. The salon owner can also introduce new users in the system and add them only to the existing roles.

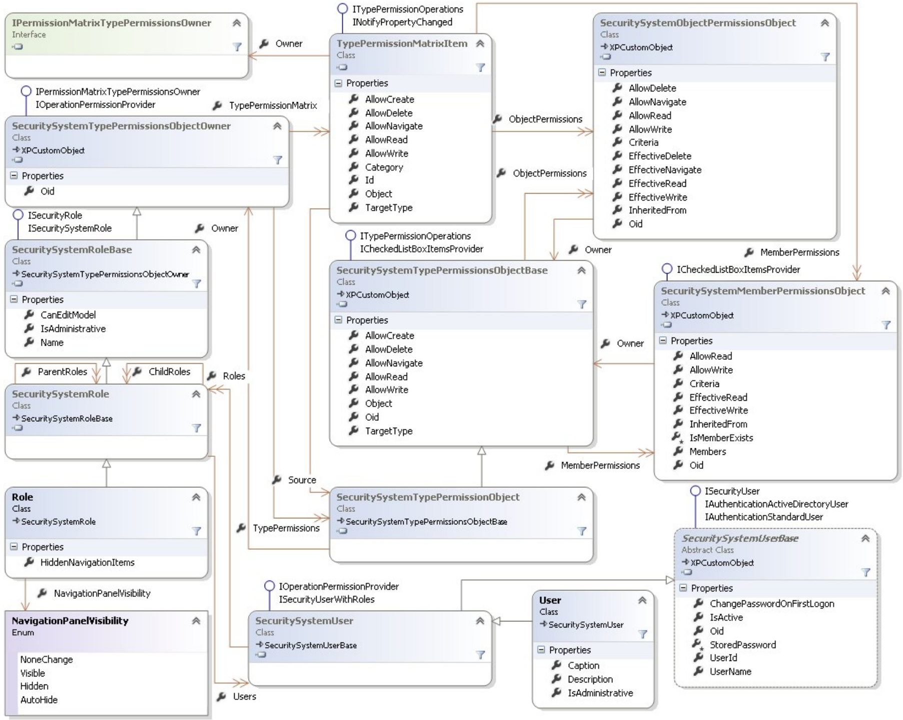

Fig. 3. UML class diagram of the implemented model of access rights differentiation

The papers [18-20] describe the information system architecture of fast food restaurants. The key feature of application of this class is that they are used in the places of public service with a large number of clients. In such software products, the critical maintenance time is very important, and so the graphical interface of the user must be ergonomic. The monoblocks with touch screens are often used as the hardware platform in such systems. Therefore, in such applications, attention is paid to the graphical interface of the user and to the principles of security settings. In this case, the following roles are selected:

- **Waiter**. The waiter's main task is to create purchase orders, to add the goods purchased by clients to the orders, and to arrange the payment;
- **Cashier**. A cashier cannot create new orders but can remove erroneous orders, view all orders issued in the current and previous shifts, and also issue the payment orders;
- **Manager**. His main task is to form consolidated reports on the work of a shift and to add new waiters and cashiers to the system;
- **Merchandiser**. The main task of the merchandiser is to introduce information about new food into the system.

When designing each of the above-described applications, the role of system administrator, who sets permissions for the existing roles and creates new roles, was also assigned. In fact, this role corresponds to the system administrator of a domain of the Windows operating system.

5. Information security in OA-systems

The OA-approach to organization of the data structure and the computational process is currently being developed. The approach implements the object-oriented (OO) programming principle with a few other features [21,22,23]. The OA-approach requires new methods for the information security organization.

Unlike the OO paradigm, in OA, there is no distinction between the concepts of class and object. Instead of the class, a semantic network template, which is copied to generate a new semantic network, is used [24]. Also, there is no such a concept as the field of an object: a data and a program are represented as an information capsule (IC). Therefore, in the OA-system, the data security is focused on an information capsule (IC), and the OA-graph is protected through it. Let us explain it. The functional unit (FU) processes an OA-graph. Let us call it a processing FU. The processing FU usually takes reference to one of the IC (starting IC) of the OA-graph and produces a traversal from the IC. The traversal is performed as follows. A FU looks for the information pair (IP) in the IC with a specific attribute and goes by the link contained in its load to another IC of the OA-graph. Thus, the OA-graph security is provided through the security of the starting IC. Any other IC may be secured in the OA-graph similarly to the protection of the object field in the OO paradigm.

For the implementation of information security, a specialized FU, called the "Guard", is required. The functions of the FU are the control of the user accounts and roles (if the RBAC approach is used) and the creation and control of the access control list (ACL) for IC contained in the OA-graph. The Guard integrated to the processing FU controls the access permissions to a IC. The control is ensured as follows: operating FU before the analysis, the IC passes a reference to the access controller that checks the access permission to IC. If the access is denied, then the Guard blocks the FU performing the OA-graph traversal.

The access permissions information is stored in the ACL (fig. 4). The ACL can be attributed to the IC of the OA-graph by adding IP, called the security IP, with the attribute "ACL", the load of the IP contains a pointer to the ACL (one ACL can be assigned to one or several IC.). To prevent unauthorized access to the ACLs, the manipulation protection of security IP is included in the algorithm for controlling the processing FU: prohibition to remove the secure IP (the IP can only be removed during the removal of the IC, where the IP is located), prohibition to use the reference of the secure IP load, etc. The ACL is processed (creation, destruction and modification) by the Guard.

The proposed mechanism well emulates the protection class in the OO paradigm. If the secure IP is contained in the OA-graph, then when copying the OA-graph, the secure IP with the load containing the reference to the access rights matrix is copied too.

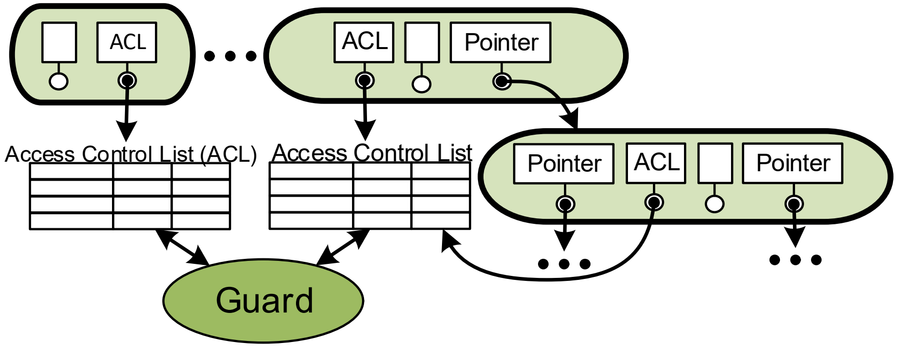

Fig. 4. The mechanism of data security in OA-computing system

The proposed methodology provides maximum flexibility of the security mechanism of the OA-graph and corresponds to all three criteria (OC1, OC2, OC3) applicable to the security of OO systems, i.e., protection of OA-graph (similar to object), a separate IC (similar to object fields), and OA-graphs copied from the OA-graph template (similar to the class protection). Moreover, all criteria are satisfied with a single protection mechanism.

6. Conclusions and further research

The above description shows that the established model of differentiation of access rights can successfully be used in applications in various domains, i.e. it is universal. Several applications where the security comes first are currently designed and implemented. This allows testing the proposed model completely and modifying it in accordance with the discovered drawbacks.

The model was developed in the OA-approach. The model is quite simple and satisfies all criteria for the security in the OO approach.

References

[1]. Nagaratnam N., Nadalin A., Hondo M., McIntosh M., Austel P. Business-driven application security: from modeling to managing secure applications. IBM Systems Journal, vol. 44, issue 4, 2005, pp. 847-867.

[2]. Xiao L., Peet A., Lewis P., Dashmapatra S., Saez C., Croitoru M., Vicente J., Gonzalez-Velez H., Lluch i Ariet M. An Adaptive Security Model for Multi-agent Systems and Application to a Clinical Trials Environment. 31st Annual International Computer Software and Applications Conference, COMPSAC 2007, 24-27 July 2007, Beijing, China, 2007, pp. 261-268.

[3]. Fengyu Zhao, Xin Peng, Wenyun Zhao. Multi-Tier Security Feature Modeling for Service-Oriented Application Integration. Eighth IEEE/ACIS International Conference on Computer and Information Science, ICIS 2009, 1-3 June 2009, Shanghai, China, 2009, pp. 1178-1183.

[4]. Saleem M.Q., Jaafar J., Hassan M.F. Model Driven Security Framework for Definition of Security Requirements for SOA Based Applications. 2010 International Conference on Computer Applications and Industrial Electronics (ICCAIE), 5-8 Dec. 2010, Kuala Lumpur, 2010, pp. 266-270.

[5]. Shiroma Y., Washizaki H., Fukazawa Y., Kubo A., Yoshioka N. Model-Driven Security Patterns Application Based on Dependences among Patterns. ARES '10 International Conference on Availability, Reliability, and Security, 15-18 Feb. 2010, Krakow, Poland, 2010, pp. 555-559.

[6]. Salini P., Kanmani S. Application of Model Oriented Security Requirements Engineering Framework for Secure E-Voting. 2012 CSI Sixth International Conference on Software Engineering (CONSEG), 5-7 Sept. 2012, Indore, 2012, pp. 1-6.

[7]. Oleynik P.P. Resentating metamodel of object system in a relational database. Izvestiya vysshikh uchebnykh zavedeniy. Severo-Kavkazskiy region [UNIVERSITY NEWS. NORTH-CAUCASIAN REGION]. Spetsvypusk «Matematicheskoe modelirovanie i komp'yuternye tekhnologii» [Special Issue "Mathematical modeling and computer technologies»], pp. 3-8, 2005 (in Russian).

[8]. Oleynik P.P. Implementation of the Hierarchy of Atomic Literal Types in an Object System Based of RDBMS. Programming and Computer Software, vol. 35, no.4, pp. 235-240, 2009.

[9]. Oleynik P.P. Class Hierarchy of Object System Metamodel. Ob’ektnye sistemy – 2012: materialy VI Mezhdunarodnoj nauchno-prakticheskoj konferencii, Rostov-na-Donu, 10-12 maja 2012 g. [Object Systems – 2012: Proceedings of the Sixth International Theoretical and Practical Conference. Rostov-on-Don, Russia, 10-12 May, 2012]. pp. 37-40 (In Russian). Available at: http://objectsystems.ru/files/2012/Object_Systems_2012_Proceedings.pdf

[10]. Oleynik P.P. Domain-driven design of the database structure in terms of object system metamodel. Ob’ektnye sistemy – 2012: materialy VI Mezhdunarodnoj nauchno-prakticheskoj konferencii, Rostov-na-Donu, 10-12 maja 2012 g. [Object Systems – 2014: Proceedings of the Eighth International Theoretical and Practical Conference, Rostov-on-Don, 10-12 May, 2014], pp. 41-46 (In Russian). Available at: http://objectsystems.ru/files/2014/Object_Systems_2014_Proceedings.pdf

[11]. Oleynik P.P. Using metamodel of object system for domain-driven design the database structure // Proceedings of 12th IEEE East-West Design & Test Symposium (EWDTS’2014), Kiev, Ukraine, September 26 – 29, 2014, pp. 79-86. DOI: 10.1109/EWDTS.2014.7027052

[12]. Oleynik P.P. Unified Metamodel of Object System. Ob’ektnye sistemy – 2015: materialy X Mezhdunarodnoj nauchno-prakticheskoj konferencii, Rostov-na-Donu, 10-12 maja 2015 g. [Object Systems – 2015: Proceedings of X International Theoretical and Practical Conference, Rostov-on-Don, 10-12 May, 2015], pp. 79-85. Available at: http://objectsystems.ru/files/2015/Object_Systems_2015_Proceedings.pdf

[13]. Oleynik P.P. The Elements of Development Environment for Information Systems Based on Metamodel of Object System. Biznes-informatika [Business Informatics], №4(26), pp. 69-76, 2013 (In Russian). http://bijournal.hse.ru/data/2014/01/16/1326593606/1BI%204(26)%202013.pdf

[14]. Oleynik P.P., Kurakov Yu.I. The Concept Creation Service Corporate Information Systems of Economic Industrial Energy Cluster. Prikladnaja informatika [Applied Informatics], №6. pp. 5-23, 2014 (In Russian).

[15]. Kurakov Y. I., Oleynik P. P. Implementation method a unified information system of economic production and energy cluster in coal industry. Gornyj informacionno-analiticheskij bjulleten' [Mining information-analytical Bulletin, no. 6, pp. 260-273, 2015 (In Russian).

[16]. Borodina N.E., Oleynik P.P., Galiaskarov E.G. Reengineering of Object Model by the Example of Information System for Cataloging Scientific Articles for International Conferences. Ob’ektnye sistemy – 2014 (zimnjaja sessija): materialy IX Mezhdunarodnoj nauchno-prakticheskoj konferencii, Rostov-na-Donu, 10-12 dekabrja 2014 g. [Object Systems – 2014 (Winter session): Proceedings of IX International Theoretical and Practical Conference, Rostov-on-Don, 10-12 December, 2014], pp. 17-23 (In Russian). Available at: http://objectsystems.ru/files/2014WS/Object_Systems_2014_Winter_session_Proceedings.pdf

[17]. Kozlova K.O., Borodina N.E., Galiaskarov E.G., Oleynik P.P. Domain-Driven Design of Information System of a Beauty Salon in Terms of Unified Metamodel of Object System. Ob’ektnye sistemy – 2015: materialy X Mezhdunarodnoj nauchno-prakticheskoj konferencii, Rostov-na-Donu, 10-12 maja 2015 g. [Object Systems – 2015: Proceedings of X International Theoretical and Practical Conference, Rostov-on-Don, 10-12 May, 2015], pp. 86-90 (In Russian). Available at:http://objectsystems.ru/files/2015/Object_Systems_2015_Proceedings.pdf

[18]. Oleynik P.P, Yuzefova S.Yu., Nikolenko O.I. Experience in Designing an Information System for Fast Food Restaurants. Ob’ektnye sistemy – 2014 (zimnjaja sessija): materialy IX Mezhdunarodnoj nauchno-prakticheskoj konferencii, Rostov-na-Donu, 10-12 dekabrja 2014 g. [Object Systems – 2014 (Winter session): Proceedings of IX International Theoretical and Practical Conference, Rostov-on-Don, 10-12 December, 2014], pp. 12-16 (In Russian). Available at: http://objectsystems.ru/files/2014WS/Object_Systems_2014_Winter_session_Proceedings.pd

[19]. Nikolenko O.I., Oleynik P.P, Yuzefova S.Yu. Prototyping and Implementation of Graphical Order Form for the Information System of Fast Food Restaurants. Ob’ektnye sistemy – 2015: materialy X Mezhdunarodnoj nauchno-prakticheskoj konferencii, Rostov-na-Donu, 10-12 maja 2015 g. [Object Systems – 2015: Proceedings of X

International Theoretical and Practical Conference, Rostov-on-Don, 10-12 May, 2015], pp. 68-72 (In Russian). Available at: http://objectsystems.ru/files/2015/Object_Systems_2015_Proceedings.pdf

[20]. Pavel P. Oleynik, Olga I. Nikolenko, Svetlana Yu. Yuzefova. Information System for Fast Food Restaurants. Engineering and Technology, vol. 2, no. 4, 2015, pp. 186-191. Available at: http://article.aascit.org/file/pdf/9020895.pdf

[21]. P. B. Panfilow, S. M. Salibekyan Dataflow Computing and its Impact on Automation Applications. Procedia Engineering, vol. 69, 2014., pp. 1286-1295. URL: http://www.sciencedirect.com/science/article/pii/S1877705814003671

[22]. Pavel P. Oleynik, Sergey M. Salibekyan. The Approaches to Implementation of Patterns of Static Object Models for Database Applications: Existing Solutions and Unified Testing Model. International Journal of Applied Engineering Research, vol. 10, no. 24 2014, pp 45513-45516.

[23]. Salibekyan S.M., Panfilov P. B Object-Attribute Architecture is a New Approach to Object Systems Developing. Informacionnye tehnologii [Information technologies], no.2, 2012, pp 8-14.

[24]. Salibekyan S. M., Belousov, A. Yu., Graph Database Implemented by Object-Attribute Approach. Ob'ektnye sistemy – 2014 (zimnjaja sessija): materialy IX Mezhdunarodnoj nauchno-prakticheskoj konferencii, Rostov-na-Donu, 10-12 dekabrja 2014 g. [Object Systems – 2014 (Winter session): Proceedings of IX International Theoretical and Practical Conference, Rostov-on-Don, 10-12 December, 2014], pp. 70-75 (In Russian). Available at: http://objectsystems.ru/files/2014WS/Object_Systems_2014_Winter_session_Proceedings.pdf

Модель разграничения прав доступа для объектно-ориентированных и объектно-атрибутных приложений

[1] *П.П. Олейник <xsl@list.ru>*
[2] *С.М. Салибекян <ssalibekyan@hse.ru>*
[1] *Шахтинский институт (филиал) Южно-Российского государственного политехнического университета (НПИ) им. М.И. Платова,*
346500, Россия, Ростовская обл., Шахты, пл. Ленина, 1.
[2] *Национальный исследовательский университет «Высшая школа экономики», Московский институт электроники и математики,*
101000, Россия, г. Москва, ул. Мясницкая, д. 20.

Аннотация. В статье приводится описание двух методик разграничения прав доступа, основанных ролевом подходе (RBAC) и применении таблиц/списков прав доступа. Вначале приводится обзор современных подходов к организации безопасности и разграничения прав доступа пользователей в приложениях различной архитектуры. Далее приводится описание двух методик защиты информации. Первая разработана для защиты объектно-ориентированных приложений, вторая приложений объектно-атрибутных, применяемых для управления сетевыми базами данных и базами знаний. Далее внимание уделяется первой авторской методике, основанной на описании прав доступа для классов, атрибутов классов и объектов, удовлетворяющих определенному критерию. Подход, разработанный первым автором, реализован с помощью иерархии классов, состав и структура которых детально описана в работе. Также приводятся примеры конкретных информационных систем, разработанных первым автором: информационная система проведения научных конференций, используемая многократно при проведении конференции «Объектные системы» (objectsystems.ru), а также информационная система салона красоты. Далее приводится описание второй методики, потребовавшей разработки новых подходов к организации защиты информации. Вторая методика, разработанная вторым автором, полностью дублирует функциональность первой. В частности, она обеспечивает копирование прав доступа при копировании части сетевой структуры данных, подобно тому, как в объектно-ориентированной парадигме происходит передача свойств родителя к потомку класса; в статье приводится подробное описание такого механизма. Для управления правами доступа в такой методике применяется специальное виртуальное устройство, а информация о правах доступа привязывается узлу сети (графа), если необходимо ограничить доступ к нему.

Ключевые слова: защита информационной системы, объектно-ориентированные приложения, объектно-ориентированная метамодель, модель разграничения прав, объектно-атрибутный подход.

DOI: 10.15514/ISPRAS-2016-28(3)-3

Для цитирования: Олейник П.П, Салибекян С.М. Модель разграничения прав доступа для объектно-ориентированных и объектно-атрибутных приложений. Труды ИСП РАН, том 28, вып. 3, 2016 г. стр. 35-50 (на английском). DOI: 10.15514/ISPRAS-2016-28(3)-3

Список литературы

[1]. Nagaratnam N., Nadalin A., Hondo M., McIntosh M., Austel P. Business-driven application security: from modeling to managing secure applications. IBM Systems Journal, vol. 44, issue 4, 2005, pp. 847-867

[2]. Xiao L., Peet A., Lewis P., Dashmapatra S., Saez C., Croitoru M., Vicente J., Gonzalez-Velez H., Lluch i Ariet M. An Adaptive Security Model for Multi-agent Systems and Application to a Clinical Trials Environment. 31st Annual International Computer Software and Applications Conference, COMPSAC 2007, 24-27 July 2007, Beijing, China, 2007, pp. 261-268

[3]. Fengyu Zhao, Xin Peng, Wenyun Zhao. Multi-Tier Security Feature Modeling for Service-Oriented Application Integration. Eighth IEEE/ACIS International Conference

on Computer and Information Science, ICIS 2009, 1-3 June 2009, Shanghai, China, 2009, pp. 1178-1183

[4]. Saleem M.Q., Jaafar J., Hassan M.F. Model Driven Security Framework for Definition of Security Requirements for SOA Based Applications. 2010 International Conference on Computer Applications and Industrial Electronics (ICCAIE), 5-8 Dec. 2010, Kuala Lumpur, 2010, pp. 266-270

[5]. Shiroma Y., Washizaki H., Fukazawa Y., Kubo A., Yoshioka N. Model-Driven Security Patterns Application Based on Dependences among Patterns. ARES '10 International Conference on Availability, Reliability, and Security, 15-18 Feb. 2010, Krakow, Poland, 2010, pp. 555-559

[6]. Salini P., Kanmani S. Application of Model Oriented Security Requirements Engineering Framework for Secure E-Voting. 2012 CSI Sixth International Conference on Software Engineering (CONSEG), 5-7 Sept. 2012, Indore, 2012, pp. 1-6

[7]. Олейник П.П. Представление метамодели объектной системы в реляционной базе данных. Известия высших учебных заведений. Северо-Кавказский регион. Спецвыпуск «Математическое моделирование и компьютерные технологии», стр. 3-8, 2005.

[8]. Oleynik P.P. Implementation of the Hierarchy of Atomic Literal Types in an Object System Based of RDBMS. Programming and Computer Software, vol. 35, no.4, 2009, pp. 235-240.

[9]. Олейник П.П. Иерархия классов метамодели объектной системы. Объектные системы – 2012: материалы VI Международной научно-практической конференции (Ростов-на-Дону, 10-12 мая 2012 г.), стр. 37-40. Доступно по ссылке: http://objectsystems.ru/files/2012/Object_Systems_2012_Proceedings.pdf

[10]. Олейник П.П. Предметно-ориентированное проектирование структуры базы данных в понятиях метамодели объектной системы. Объектные системы – 2014: материалы VIII Международной научно-практической конференции (Ростов-на-Дону, 10-12 мая 2014 г.), стр. 41-46. Доступно по ссылке: http://objectsystems.ru/files/2014/Object_Systems_2014_Proceedings.pdf

[11]. Oleynik P.P. Using metamodel of object system for domain-driven design the database structure. Proceedings of 12th IEEE East-West Design & Test Symposium (EWDTS'2014), Kiev, Ukraine, September 26 – 29, 2014, pp. 79-86. DOI: 10.1109/EWDTS.2014.7027052

[12]. Oleynik P.P. Unified Metamodel of Object System. Объектные системы – 2015: материалы X Международной научно-практической конференции (Ростов-на-Дону, 10-12 мая 2015 г.), стр. 79-85. Доступно по ссылке: http://objectsystems.ru/files/2015/Object_Systems_2015_Proceedings.pdf

[13]. Oleynik P.P. Элементы среды разработки программных комплексов на основе организации метамодели объектной системы. Бизнес-информатика, №4(26), 2013, стр. 69-76. Доступно по ссылке: http://bijournal.hse.ru/data/2014/01/16/1326593606/1BI%204(26)%202013.pdf

[14]. Олейник П. П., Кураков Ю. И. Концепция создания обслуживающей корпоративной информационной системы экономического производственно-энергетического кластера. Прикладная информатика, №6, 2014, стр. 5-23

[15]. Кураков Ю.И., Олейник П.П. Методика реализации унифицированной информационной системы экономического производственно-энергетического кластера угольной промышленности. Горный информационно-аналитический бюллетень, № 5, 2015, стр. 260-273.

[16]. Бородина Н.Е., Олейник П.П., Галиаскаров Э.Г. Опыт выполнения реинжиниринга объектной модели на примере информационной системы каталогизирования научных статей при проведении международных конференций. Объектные системы – 2014 (зимняя сессия): материалы IX Международной научно-практической конференции (Ростов-на-Дону, 10-12 декабря 2014 г.), стр. 17-23 Доступно по ссылке: http://objectsystems.ru/files/2014WS/Object_Systems_2014_Winter_session_Proceedings.pdf

[17]. Козлова К.О., Бородина Н.Е., Галиаскаров Э.Г., Олейник П. П. Предметно-ориентированное проектирование информационной системы салона красоты. Объектные системы – 2015: материалы X Международной научно-практической конференции (Ростов-на-Дону, 10-12 мая 2015 г.), стр. 86-90. Доступно по ссылке: http://objectsystems.ru/files/2015/Object_Systems_2015_Proceedings.pdf

[18]. Олейник П.П., Юзефова С.Ю., Николенко О.И. Опыт проектирования информационной системы для ресторанов быстрого питания. Объектные системы – 2014 (зимняя сессия): материалы IX Международной научно-практической конференции (Ростов-на-Дону, 10-12 декабря 2014 г.), стр. 12-16. Доступно по ссылке: http://objectsystems.ru/files/2014WS/Object_Systems_2014_Winter_session_Proceedings.pdf

[19]. Николенко О.И., Олейник П.П. Прототипирование и реализация графической формы заказа для информационной системы ресторанов быстрого питания. Объектные системы – 2015: материалы X Международной научно-практической конференции (Ростов-на-Дону, 10-12 мая 2015 г.), стр. 68-72. Доступно по ссылке: http://objectsystems.ru/files/2015/Object_Systems_2015_Proceedings.pdf

[20]. Pavel P. Oleynik, Olga I. Nikolenko, Svetlana Yu. Yuzefova. Information System for Fast Food Restaurants. Engineering and Technology, vol. 2, no. 4, 2015, pp. 186-191. Доступно по ссылке: http://article.aascit.org/file/pdf/9020895.pdf

[21]. P. B. Panfilow, S. M. Salibekyan Dataflow Computing and its Impact on Automation Applications. Procedia Engineering, vol. 69, 2014, pp. 1286-1295. doi:10.1016/j.proeng.2014.03.121. Доступно по ссылке: http://www.sciencedirect.com/science/article/pii/S1877705814003671

[22]. Pavel P. Oleynik, Sergey M. Salibekyan. The Approaches to Implementation of Patterns of Static Object Models for Database Applications: Existing Solutions and Unified Testing Model. International Journal of Applied Engineering Research, vol. 10, no. 24, 2015, pp 45513-45516.

[23]. Салибекян С. М., Панфилов П. Б. Объектно-атрибутная архитектура – новый подход к созданию объектных систем. Информационные технологии, № 2, 2012, стр. 8-13.

[24]. Салибекян С.М., Белоусов А.Ю. Сетевая база данных, построенная по объектно-атрибутному принципу. Объектные системы – 2014 (зимняя сессия): материалы IX Международной научно-практической конференции (Ростов-на-Дону, 10-12 декабря 2014 г.), стр. 70-75. Доступно по ссылке: http://objectsystems.ru/files/2014WS/Object_Systems_2014_Winter_session_Proceedings.pdf