The optimal setting of access rights by generating output set of access roles

MONIKA SIMKOVA\textsuperscript{a}, JIRI STEPANEK\textsuperscript{b}
\textsuperscript{a}Department of quantitative methods and informatics, \textsuperscript{b}Department of information technology
University of Hradec Kralove
Rokitanskeho 62/26, 50003 Hradec Kralove
CZECH REPUBLIC
monika.simkova@uhk.cz http://www.uhk.cz

Abstract: - This paper describes the designed system for modelling of user roles, which is part of the research project Connection of system for identity management for algorithms for the analysis of access privileges and modelling of user role within the innovation project which was carried out by companies AG COM C. and Ortex Ltd. in collaboration with the University of Hradec Kralove, together operating in association HIT cluster. The proposed system aims to achieve an optimal, least or the most fitting number of roles that are consistent with the needs of the organization. It's also necessary to avoid a situation when in consequence of the bad roles Catalogue gets a user more rights than he/she needs or the result of system roles will be hardly controllable and comprehensible. Currently, this issue doesn't have available software due its complexity. The subject of further investigation may be the Identity Management – SSO, Lifecycle Management.

Key-Words: - user roles, modelling of access privileges, system of user roles, modelling of user role, security of user roles, system for modelling of user roles

1 Introduction
The aim of project was linking existing identity management systems, respectively parts relating to the system of roles to an external component that provides design and life cycle of roles system. The basis of the project is the development of algorithms applicable to the analysis of access rights and modelling user roles from the state of the permission settings to the final systems. One of the security requirements for access to information is achieve optimal in defining user access in systems. Based on the classification of user roles has been to classify all necessary permissions of accesses in systems. [3,4,5, 9]

The project includes these key activities:

- Development of appropriate algorithms which are applicable to modeling the catalog of user roles.
- Implementation of selected set of algorithms over existing database of user accounts and their subsequent optimization in real environment.
- Finding suitable restrictive conditions as input parameters of each algorithm for generating a catalogue of roles.
- Comparison of various algorithms and their suitability for a particular configuration of input parameters.
- Development of the connectors on the catalogue roles of existing system for identity management

The project includes these several steps:

- The life cycle of roles in the organization, idM software, RBAC model.
- Analysis of the ability to connect to the LDAP protocol and presentation roles in idM.
- The exact formulation of the concept and HiLevel design of all solution.
- Selections of inputs, the choice of solvers post-processing, connectors.
- Basic design of GUI and possibility of integration.
- Analysis of safety requirements and regular principles for catalogs of roles.
- Analysis of requirements for function of solvers.
- The definition of boundary conditions.
- Detailed design of GUI.
• Prepare preliminary set of test data for development.
• Introduction to function solvers – algorithms (Hill Climb, genetics, SAT – Boolean satisfiability problem).
• Development of FUI over algorithms.
• Development LDAP connectors and connectors for connection to the idM system. Connection (import and export) using the LDAP protocol (LDIF file format)
• Preparation of the test plan.
• Practical verification of the usability of selected types of algorithms for basic types of tasks (maximization and minimization problems) in search of the optimal catalogs of roles.
• Design of use of verified algorithms in the context of program of works that deal with the issue.
• Optimum functionality.
• Documentation and presentation of project results.

2 Identity management (IdM)
In order to manage the accounts in one place and have access to current information about events in the system software is used to centrally manage user accounts, so-called identity management. Identity management (IdM) is an information system that can operate in one place all the life cycle of all user accounts in the organization and monitor their changes. The basic process of identity management is life cycle of user identity. The life cycle start form the first day of the user in the system, usually occurs only to the basic approaches (end station, intranet, corporate mail) As the name implies the cycle changes with the user who gets new privileges or some of his privileges are removed.

3. Role based access control – RBAC
Extended principle in the management of privileges is currently Role-Based Access Control (RBAC) which uses repeatedly the assignable objects – roles. The user than have a role gets privileges indirectly via the assigned role. The actual role can contain other attributes, such as addition to the name of the owner or approver roles or description. It is possible to follow the exclusive rules of roles called Segregation of Duties (SoD), when a user cannot have for example role that it authorizes to issue invoice together with the role which controls the invoices. IdM represents a partial authorization in a power system using an application role. Roles have usually the basic in their labor organization or permission levels or geographic breakdown. For a typical RBAC roles may be considered: The customer (the role of “customer” = access webs server in the DMZ), New Employee (role of “basic user” = Active Directory Lotus Notes Mail), Senior Employee (the “basic user” and “accounting”) Manager. Of course there are other access models such as DAC and MAC.[6,7,8]

4 Description of system Role Modeler
System will set analysis of setting access privileges based on the input parameters and generating the output set of user roles. The system reads the accounts from LDAP or LDIF single format – all will be have the same number and type of constant attributes. The user enters the key attributes for generating roles, defines rules for addition roles and asks questions. The problem that is solving with the
query is the similar problem of finding an optimal schedule or route.

The task of min-algorithm is to find the smallest set of roles that will be able to cover minimum percentage of real accounts in other words to find the minimum number of roles that cover at least X% of accounts (usually 95% or 98%).

Questions:

- Find the X role to cover maximum of account (f.e. to find a fundamental role that covers nearly all user accounts)
- Find the least roles as possible which cover at least X% accounts (usually 95% or 98%).
- Fixation of the role of the chosen attribute. The number of roles will be equal or greater than is the domain of this attribute. Analysis of the roles be going on the fact that it is interested in the combinations of the remaining attributes.
- After the system finds the combinations of roles, the user can choose option preview for changes in the model including the ability to export or import roles or filtration accounts. The system shows which accounts are not covered and from which reason, statistics on the percentage to sharing on cover of account with different roles.

4.1. Maximization task
The task of max-algorithm is to find the largest subset of accounts, which will be covered by the number of generated roles or in other words to find X role to cover most accounts (e.g. to find fundamental role, which covers nearly all accounts).

4.2. Minimization task

5 Connection to LDAP and test
Modelling roles is tested over the four key attributes of which was one in the type multi-value. Number of accounts retrieved from a directory structures by LDAP protocol is 10, 500, 1000 and 2000. This corresponds to the real conditions for load solver.
6 System structure
Account Colector – collector current authorization – allows read access permissions from LDAP or LDIF input, performs to store them in an internal database.
Role analyzer – computing core for generating sets of roles based on the input parameters.
Application GUI
Role of Exporter – performs data export set to LDAP or CSV.

7 Technology
The role modeler is developed in Java (JDK 5) and as a development environment was used NetBeans version 6. The Java language was used from reason their multiplatform, speed of development of created works, availability of development tools for all platforms and richness of libraries.

Subversion – system for managing and versioning source code.
Lightweight Directory Access Protocol (LDAP) - is defined to store and access data on the directory server. Under this protocol are individual items on the server stored in the form of records and arranged in a tree structure.
LDIF – is a standardized format for representation of data in the directory server.
CSV (Comma-separated values) file – is a simple format for exchange of tabular data.

8 Libraries
JLDAP – technology allows you to use LDAP and LDIF. It’s actually a java wrapper over fully functional free OpenLDAP library of C language.
JUnit – the most common test library for Java JUnit. It was mainly used for regression testing of data structures.
SAT4j – this library contains a Java implementation of algorithm Minis, which is an algorithm solving the SAT problem for large limited instances.

9 Conclusion
Most current information systems requires user authentication for access to the system. All data associated with the access privileges are stored in the database user account, password, permission settings and application data. Today’s constantly growing requirements place demands on organizations requiring the use of several information systems. This trend, however, brings even very desirable solution, a condition where one user has multiple user accounts. With this approach leads to an increasing number of user accounts and increasing dangers associated with decreasing clarity about what is happening in the system. Role Modeler allows a certain extent to prevent such situations and by its using it’s possible to gain such settings which make it easier the analysis of user permissions. In the future, is planned to extend this program after all the real test and adapting still evolving requirements. [1,2]

Acknowledgements
This work was supported by the project No. CZ.1.07/2.2.00/28.0327 Innovation and support of doctoral study program (INDOP), financed from EU and Czech Republic funds.

References: