Security Management of Intelligent Technologies in Business Intelligence Systems

Alexander Kadan

Yanka Kupala State University of Grodno, 22, Ozheshko str., Grodno, Belarus, 230023,
alexander.kadan@gmail.com, http://mf.grsu.by

Abstract: *The article discusses the security methods of intelligent technologies in Business Intelligence (BI) systems. Security technologies are considered taking into account BI four-layer architecture which includes: a) transactional systems layer; b) ETL-procedures – extraction, conversions and data loading layer; c) data warehouses and data marts layer; d) OLAP-tools and user interface layer. The characteristic of the general BI systems security technologies, data storage security strategies and intellectual data mining subsystems and OLAP-tools is resulted. For data mining models and to provide them with the analyst, considered the requirements of access rights to the analyzed information, database backups creation necessity, the requirements to hide sensitive data.*

Keywords: Computer security, business intelligent, intelligent technologies, data warehouse, OLAP-technologies, model of intellectual data analysis.

1. BUSINESS INTELLIGENCE SYSTEMS

Scales of implementation of computer technologies in work of the organizations, volumes of the stored data, the modern economic conditions have generated growth of need for obtaining of the qualitative and authentic analytical information necessary for acceptance of management decisions. For many companies, implementations of the analytical system, known as Business Intelligence systems (BI), has become a priority and defining projects implementing need for creation of more perfect management and control systems, allowing not to use local solutions and providing high efficiency of business processes.

BI class includes systems based on the use of data warehousing technology, multidimensional reporting technologies and OLAP-technologies. The main hypothesis of their development and use assumes that integration of the heterogeneous data and new forms of their organization and representation allow managers and analysts not only to receive new knowledge of data domain, not only provide an opportunity to independently search and analysis of information, but also provide the identification of non-obvious patterns and facts that are not detected by standard methods of classical statistics, artificial intelligence and machine learning.

Furthermore, the use of these systems promotes the considerable saving of material, temporal and work forces. The demand for BI systems is confirmed in recent years by steady growth in the number of scale projects. According to DSS Consulting the amount of BI class systems implementations in 2010 in Russia has increased on 48 % in comparison with 2009 which shows a steady increase in demand for business intelligence. Belarusian BI system market doesn’t yet have such a dynamic role.

2. BUSINESS INTELLIGENCE SYSTEMS ARCHITECTURE AND SECURITY REQIUREMENTS

Data protection is critical at use of BI systems, since almost all information related to the enterprise work is located in the BI bases being critical for the company, its personnel and partners. It is also very important to ensure the safety of the system, protecting it from intrusion and sabotage.

The authors have almost ten years' experience of BI system and their components engineering. Within the confines of the Regional scientific and technical program of the Grodno region the automated system of information support has been developed for the collection, storage, protection and analysis of statistical information for decision support of local government for which the security challenges put forward as a priority [1], started work on University BI system [2]. Realization of all specified systems was conducted with OC Windows 2003 use, MS SQL Server databases, MS Analysis Services, IIS various versions.

BI solutions are based on a four-layer architecture [2], which includes:

1. operating data sources layer (transactional systems);
2. primary database extraction, transformation and loading layer;
3. data warehouse and data mart layer;
4. OLAP-tools and user interface layer.

3. BUSINESS INTELLIGENCE SYSTEMS TECHNOLOGICAL GROUPS OF SECURITY

Security technologies underling the system protection, data protection and organization of the protected exchange of confidential information in the BI system, can be traditionally divided into six main technology groups and give them a brief description taking into account used by the software:

- **Identification and authentication** – on the basis of a name and the password with use: at connection on TCP/IP technologies of authentification Negotiate, Kerberos, NTLM, Anonimous User; at connection on HTTP methods of authentification IIS (Internet Information Services) – Integrated Windows Autentification, Basic-authentication, anonymous access.
- **Authorization** – process of establishing the rights of the object (user, user group, server, client) in relation to resources (the whole system, files, printers, database tables, cubes and marts, the elements of a multidimensional data model, etc.). The basic mechanisms of authorization: *Access control lists*, describing the possible manipulation of the resource; *Privileges*, describing the ability of users to various operations such as start of services, remote registration in system; *Permissions* to creation,

reading, updating and removal of various Microsoft SQL Server objects;.

- **Audit** - conducted to gather information about access attempts to objects, the application of privileges and other, important in terms of security operations and recording these events for further analysis. The following audit logs are supported: operating system security log, Internet- server log, databases server log, OLAP-server log.
- **Confidentiality and integrity** - are interrelated groups. Maintenance of the data confidentiality helps to prevent their disclosing and illegal updating/removal. Integrity infringement can lead to decisions based on unreliable information. Their Maintenance is realized by use: Secure Sockets Layer (SSL); Transport Layer Security protocol; IPS Protocol.
- **Availability** - implemented using failover hardware and software, built-in tools used in the system.
- **Inability denial of the transaction** - is provided by means of authentication, authorization, auditing, and data integrity. Besides, the principal is informed that for the action that he intends to take, he is liable (legally).

When considering the BI systems security problems all listed factors and a context in which the decision will be applied should be considered. From four mentioned above architecture layers we will consider two last, as immediately reflecting singularities of BI systems.

4. DATA WAREHOUSE AND DATA MARTS SECURITY MANAGEMENT

Strategy of data security used in BI systems are based on security strategies that are implemented in Microsoft SQL Server, which acts as a secure database platform, provides secure storage and exchange of confidential data. SQL Server work in integrated mode, with the use of OS authentication means, implemented through the SSPI interface on the basis of login accounts of the Windows Security Account Manager or Active Directory credentials is supposed.

Besides objective (resolutions for objects) and command (resolutions for operators) access rights, it is supposed a combination of various components of a SQL Server to simplify administration and to improve security system:

- security systems management with roles. Members of one group receive identical based on roles access rights to objects;
- the use of representations for data security. Allows to restrict data amount, access to individual rows and columns of tables that the user can view and modify;
- use stored procedures for data security. Allows to reduce process of access rights output to all tables and representations that have links in the stored procedure;
- the triggers use for data check. The trigger type that ensures that those who has fulfilled last modification in the table and when it has happened is applied.

As by default, almost all data except the user ID and password are transmitted unencrypted over the network, then the network traffic between client and server should be encrypted by IPS protocol means. SQL Servers traffic encryption by its built-in mechanisms. SQL Servers incoming and outgoing traffic encryption provides tools of specialized multiprotocol network library.

5. SECURING OLAP-LAYER TOOLS

The OLAP Server security model includes five subsystems which interaction ensures the safety of the system: access to the server (responsible for authentication and authorization necessary to define a set of user rights); multidimensional model managing (provides multidimensional data model administration at the user’s level rights); data access of multidimensional model (access control at different detail levels); access to data sources (access rights to exterior data sources (relation database, file system); run user code.

Restricting access to the OLAP Server and specific databases and cubes of these databases is based on use of the role mechanism. The users fulfilling identical functions are grouped into roles. At the OLAP Server database level defines the roles of system administrator, database administrator, the user.

However, the security level of the cube absolutely insufficient for practical OLAP database purposes, therefore more detailed security levels - at the level of measurement (with restriction of multidimensional space) and at the cell level of the cube (without restriction of multidimensional space) are implemented. It is possible – unlimited, completely restricted and customizable access to cube measurements. It is possible to adjust the route of access to sections. There is a chance to unrestricted, restricted and completely customizable access to measurements of the cube. It is possible to provide read access to certain levels of measurement. For example, it is possible to install security options for the role of department heads, allowing to data view within the organization at their level and below.

Ability to restrict access rights to individual cube elements (cells) is very important for OLAP applications. The concept of security at the cell level allows to create cubes that contain all the necessary data, and then to restrict access to them on the basis of various criteria. The security settings on the cell level are set for the role at the cube level instead of for the role of database level. The special attention is demanded by operation with models of intellectual data analysis (IDA). The analyst must have administrative permissions on the database in which these models are stored, and it allows changing the objects which have been not connected with IDA. One solution is to create a separate database specifically for use with IDA models or separate databases creation for each analyst. Although IDA models creation typically require the highest level of permits access for other operations such as viewing or queries that can be controlled by role-based security means.

Besides, IDA models often refer to the data sources, containing confidential information, therefore measures to conceal such information are necessary.

6. CONCLUSION

Methods of data mining in Business Intelligence systems represent a powerful set of technologies, models and tools for search unobvious (which are very difficult or impossible to detect using classical methods of mathematical statistics and decision suport theory) relationships and dependencies. However their use frequently demands to provide for the expert broad authority for access to the entire data space. This requirement is often at odds with the concept of corporate use of Business Intelligence systems, which use demands a separation of user's powers. Moreover, the system used to store of confidentional information (for example, the medical data) using intellectual methods of the analysis is difficult in the absence of the expert required level of access to information.

Data mining models and methods development for use in Business Intelligence systems, using confidential data or the limited access data, must necessarily take into account the requirements of this data security.

7. REFERENCES

[1] Kadan A. Technologies Microsoft SQL Server the decision of problems of storage and the analysis of the statistical information of region // *Proceedings of The Third International Conference "Network computer technologies (IST-2008)" (1-3 November 2006). –* Minsk, Belarus, 2006. – PP.81-85. (in Russian)

[2] Kadan A. Information technology solutions based on Business Intelligence in the field of university management // *Bulletin of GrSU. Ser. 2: Mathematics. Physics. Computer science, computer engineering and management. Biology*. — 2010. — N 2(96) — P. 123-131. (in Russian)