Lecture №1.10.
The data security in IT. The OS protection, the databases protection, the virus protection.

As ***mechanisms of OS protection*** we will understand all means and mechanisms of protection the data functioning as a part of OS.

OS in which structure means and mechanisms of protection of data function, name often the protected systems.

As ***safety of OS*** we will understand such status of OS at which casual or deliberate infringement of functioning of OS is impossible, and also infringement of safety of resources of system being under control of OS.

We will specify following features of OS which allow to allocate questions of maintenance of safety of OS in a special category:

− management of all resources of system;

− presence of the built in mechanisms which expressly or by implication influence safety of programs and the data working in the environment of OS;

− maintenance of the interface of the user with system resources;

− the sizes and complexity OS.

Majority OS possess defects from the point of view of maintenance of safety of data in system that is caused by performance of a problem of maintenance of the maximum availability of system for the user. We will consider typical functional defects of OS which can lead to creation of channels of data leak.

1. ***Identification.*** To each resource in system the unique name-identifier should be appropriated. In many systems users have no possibility to make sure that resources used by them really belong system.
2. ***Passwords.*** The majority of users is chosen by the elementary passwords which are easy for picking up or guess.
3. ***The passwords list.*** Storage of the list of passwords in not ciphered kind gives the chance it compromise with the subsequent unauthorized access to data.
4. ***Threshold values.*** For prevention of attempts of not authorised input in system by means of pasword selection it is necessary to limit number of such attempts, that in some OS is not provided.

5. ***Meant trust.*** In many cases of the program of OS consider, that other programs work correctly.
6. ***The total memory.*** At total memory use not always after performance of programs sites of operative memory (RAM).
7. ***Communication rupture are cleared.*** In case of rupture of communication of OS should finish immediately a session with the user or repeatedly establish authenticity subject.
8. ***Transfer of parametres under the link, instead of on value*** (by transfer of parametres under the link preservation of parametres in RAM after check of their correctness is possible, the infringer can change these data before their use).
9. ***The system can contain many elements*** (for example, programs), having various privileges.

The basic problem of safety of OS is the problem of creation of mechanisms of control of access to system resources. Pro-cedure of control of access consists in check of conformity of inquiry of the subject to the access rights given to It to resour-ces. Besides, OS contains auxiliary protection frames, such as means of monitoring, preventive control and audit. In aggregate mechanisms of control of access and auxiliary protection fra-mes form mechanisms of management of access. Means of preventive control are necessary for discharge of the user from direct performance critical from the point of view of safety of the given operations and transfer of these operations under OS control. For safety of the data work with system resources is carried out by means of special programs of OS access to which is limited. Monitoring means carry out constant conduc-ting the register in which records about all events in system are brought. In OS alarm system means about unauthorized access which are used at detection of infringement of safety of the data or infringement attempts can be used.

Access control to the data. At creation of mechanisms of control of access it is necessary to define, first of all, sets of subjects and objects of access. Users, tasks, processes and procedures can be subjects, for example. Objects - files, programs, semaphores, directories, terminals, communication channels, devices, blocks OP etc. Subjects can be considered simultaneously and as objects, therefore at the subject can be the rights to access to other subject. In concrete process at present time subjects are active elements, and objects - passive.

For access realization to object the subject should possess corresponding powers. Power is a certain symbol, possession which gives to the subject certain access rights in relation to object, the protection area defines access rights of some subject to set of protected objects and represents set of all powers of the given subject.

THE BASIC PROTECTIVE MECHANISMS OF OS OF FAMILY WINDOWS (NT/2000/XP)

Here the basic mechanisms of protection are:

1) identification and authentication the user at logon;

2) differentiation of access rights to resources in which basis realisation of discretionary model of access (separately to objects of file system, to devices, to OS register, to printers lies, etc.);

3) audit, i.e. registration of events.

Here possibilities of differentiations of access rights to file objects (for NTFS) are obviously allocated (to the best) - the attributes of access established on various hierarchical objects of file system (logic disks, catalogues, files) are essentially expanded. In particular, the attribute "execution" can be established and on the catalogue then it is inherited by corresponding files.

Possibilities of management by access to other protected resources, in particular, to the input equipment are thus essentially limited. For example, here there is no attribute "execution", i.e. it is impossible to forbid start of the unapproved program from the input equipment.

Information security of management systems databases. Management systems databases, in particular relational DBMS, steels the dominating tool of storage of the big files of the information. A little developed information applications rely not on file structures of operating systems, and on multiuser DBMS, executed in technology the client/server. Thereupon maintenance of information security DBMS, and first of all their server components, gets crucial importance for safety of the organization as a whole.

For DBMS all three basic aspects of information security - ***confidentiality***, ***integrity*** and ***availability*** are important. The general idea of protection of databases consists in following to the recommendations formulated for a class of safety C2 in "Criteria of an estimation of reliable computer systems". Basically some DBMS offer additions, characteristic for class B1, however practical application of similar additions makes sense, only if all components of an information structure of the organization correspond to a category of safety B. To reach it is uneasy both with technical, and with financial the points of view. It is necessary to consider two circumstances, besides. First, for the overwhel-ming majority of the commercial organizations the class of safety C2 is sufficient. Secondly, more protected versions lag behind by substantial possibilities usual "colleagues" so advocates of priva-cy as a matter of fact are doomed to use obsolete (though and carefully checked up) products with all that it implies in respect of support. For an illustration of stated concepts and means will be used DBMS

Identification and check of authenticity of users. Usually in DBMS to identification and check of authenticity of users are applied or corresponding mechanisms of an operating system, or SQL-operator CONNECT. For example, in case of DBMS Oracle operator CONNECT has the following appearance:

CONNECT the user [/the password] [@database];

Anyhow, at the moment of the beginning of a session with the server of databases, the user is identified by the name, and authentification means the password serves. Details of this process are defined by realization of a client part of the application.

Management of access. For an illustration of the questions connected with management by access, it will be used DBMS INGRES.

Usually in DBMS any management of access when the owner of object transfers access rights to it (is more often is applied speak - privileges) at own discretion. Privileges can be transfer-red to subjects (separate users), groups, roles or all users.

The group is the called set of users. Association of subjects in groups facilitates administration of databases and, as a rule, is under construction on the basis of formal or actual structure of the organization. Each user can enter into some groups. When the user that or otherwise initiates a session with a database, he can specify, from a name what of the groups it acts. Besides, for the user usually define meant group.

The role is one more possible called carrier of privileges. With a role not associates the list of admissible users - instead roles protect passwords. At the moment of the beginning of a session with a database it is possible to specify a used role (usually by means of flags or the equivalent mechanism) and its password if that is available

Role privileges have a priority over privileges of users and groups. Differently, as to the subject it is not obligatory to user to have access rights to the objects, processed applications with a certain role.

Let's notice that in DBMS Oracle the role is understood as a set of privileges. Such roles serve as means of structurization of privileges and facilitate their updating.

Set of all users is called as PUBLIC. Giving of privileges PUBLIC - a convenient way to set meant access rights.

The basic categories of users. Users DBMS can be broken into three categories:

- The manager of the server of databases. He knows installation, configuring servers, registration of users, groups, roles, etc. the Manager of the server has a name ingres. Expressly or by implication it possesses all privileges which have or other users can have.

- Managers of a database. Any user who has created a database concerns this category, and, hence, being its owner. It can give to other users access to base and to objects containing in it. The manager of base is responsible for its preservation and restoration. Basically in the organization there can be many managers of databases. That the user could create base and to become its manager, it should receive (possibly, from the manager of the server) the privilege createdb.

- Other (final) users. They operate with the data stored in bases, within the limits of the privileges allocated with it.

Let's notice only that the manager of the server of databases as the most exclusive user, needs special protection. Discredit its password actually means discredit the server and all databases stored on it.

To charge administration of various databases to different people it makes sense only when these bases are independent and in relation to them it is not necessary to carry out co-ordinated to the policy of allocation of privileges or reserve copying. In that case each of managers will know exactly so much, how many it is necessary.

It is possible to draw an analogy between the user ingres and managers of databases on the one hand, and the superuser of an operating system (root in case of OS UNIX) and office users (in OS UNIX it can be bin, lp, uucp etc.) on the other hand. Introduction of office users allows to administer functional subsystems, without receiving privileges of the superuser. In the same way the information stored on the server of databases, it is possible to divide into compartments so discredit the manager of one compartment does not mean obligatory discredit another.

Kinds of privileges. Privileges in DBMS can be subdivided on two categories: privileges of safety and the access privilege. Safety privileges allow to carry out administrative actions. Access privileges, according to the name, define access rights of subjects to certain objects.

Safety privileges. Safety privileges are always allocated to the concrete user (instead of group, a role or all) during its creation (operator CREATE USER) or change of characteristics (operator ALTER USER). Such privileges five:

security - the right to operate safety DBMS and to trace actions of users. The user with this privilege can be connected to any database, create, delete and change characteristics of users, groups and roles, to transfer the rights to access to bases to the given other users, to operate record of the registration information, to trace inquiries of other users and, at last, to start INGRES-commands on behalf of other users. The privilege

security is necessary for the manager of the server of databases, and also the person who is personally responsible for information security. Transfer of this privilege to other users (for example, to managers of databases) increases number of potentially weak places in protection of the server of databases.

createdb - the right to creation and removal of databases. This privilege, besides the manager of the server, users by whom it is assigned a part managers of separate databases should possess.

operator - the right to performance of actions which traditionally carry to the competence of the operator. Start and a server stop, preservation and information restoration Mean. Besides managers of the server and databases it is expedient to allocate with this privilege also the manager of an operating system.

maintain_locations - The right to management of an arrangement of bases managers of the server of databases and an operating system.

trace - the right to state transition of flags of debugging trace. The given privilege is useful to the manager of the server of databases and other knowing users at the analysis of difficult, not clear situations.

Access privileges. Access privileges are allocated to users, to groups, roles or all means of operator GRANT and are withdrawn by means of operator REVOKE. These privileges are appropriated, as a rule, by the owner of corresponding objects (it - the manager of a database) or the owner of the privilege security (usually the manager of the server of databases).

Use of representations for management of access. DBMS give a specific control facility access - representations. Representations allow to make visible for subjects certain columns of base tables (to realise a projection) or to select certain lines (to realise selection). Without giving subjects of access rights to base tables and having designed suitable representations, the manager of a database will protect tables from unapproved access and will supply each user with the vision of a database when inaccessible objects as though do not exist.

Hierarchy of access rights. Operator GRANT and other control facilities access DBMS allow to realise following kinds of restriction of access:

Operational restrictions (at the expense of access rights SELECT, INSERT, UPDATE, DELETE, applicable to all or only to some columns of the table);

Restrictions on values (at the expense of the mechanism of representations);

Restrictions on resources (at the expense of access privileges to databases).

At processing of inquiry DBMS at first checks access rights to objects. If operational restrictions appear broken, the inquiry is rejected with delivery of corresponding diagnostics. Infringement of restrictions on values influences only quantity of resultants of lines; any diagnostics thus does not stand out (the previous point) see. At last, after the account of two previous restrictions, the inquiry arrives on processing optimizer. If that finds out excess of restrictions on resources, the inquiry will be rejected with delivery of corresponding

It is possible to look at hierarchy of privileges and from other point of view. Each user, besides, own, has privileges PUBLIC. Besides, it can enter into various groups and start applications with certain roles. How the rights given to various called carriers of privileges correspond among themselves?

The hierarchy of authorization looks for DBMS INGRES as follows:

Role (the higher priority)

The user

Group

PUBLIC (the lowest priority)

For each object to which access is provided, INGRES tries to find in hierarchy the privilege concerning a required kind of access (SELECT, EXECUTE, etc.). For example, at access attempt to the table for the purpose of updating, INGRES checks privileges of a role, the user, group and all users. If at least at one level of hierarchy privilege UPDATE is available, the inquiry is transferred for the further processing. Otherwise the meant access right which orders to reject inquiry is used.

Labels of safety and compulsory control of access. Means of any management by access, characteristic safety for level C have been above described. As it was already specified, they basically are sufficient for the overwhelming majority of commercial applications. Nevertheless, they do not solve one rather important problem - problems of tracking information transfer. Means of any management of access cannot prevent to receive justly to the authorized user the classified information

and then to make its accessible to other, not authorised users. It is easy to understand, why it so. At any management of privilege access exist separately from the data (in case of relational DBMS - separately from lines of relational tables). As a result the data appears "depersonalized", and nothing prevents to transfer them to everybody even means most DBMS.

In "Criteria of an estimation of reliable computer systems", with reference to systems of level of safety B, the mechanism of labels of the safety, realized in version INGRES/Enhanced Security (INGRES with the raised safety) is described. To put this version into practice it makes sense only in a combination to an operating system and other program components of the same level of safety. Nevertheless, realization label consideration in DBMS INGRES is interesting to safety from the informative point of view, and the approach based on division of the data on levels of privacy and categories of

appear useful at designing of system of privileges of numerous users in relation to the big data files.

In DBMS INGRES/Enhanced Security to each relational table the column containing labels of safety of lines of the table is implicitly added. The safety label consists of three components:

Privacy level. The sense of this component depends on the application. In particular, the traditional spectrum of levels from "top secret" to “unclassified“ is possible.

Categories. The concept of a category allows to divide the data into "compartments" and by that to raise reliability of system of safety. "Finance", "shots", "material assets" can serve in commercial applications as categories, etc. More low appointment of categories is explained in more details.

Areas. Is additional means of division of the information for compartments. In practice a component "area" can really have geographical sense, designating, for example, the country

Each user DBMS INGRES/Enhanced Security is characterized by degree of reliability which also is defined the well-aimed safety, appropriated to the given user. The user can get access to the data if degree of its reliability meets requirements of a corresponding label of safety. More precisely:

Level of privacy of the user should be not below level of privacy of the data;

The set of the categories set in a label of safety of the data, should contain entirely in a label of safety of the user;

The set of the areas set in a label of safety of the user, should contain entirely in a label of safety of the data.

Let's notice that the mechanism of labels of safety does not cancel, and supplements any management of access. Users still can operate with tables only within the limits of the privileges, but even in the presence of privilege SELECT the

At addition or change of lines they, as a rule, inherit labels of safety of the user initiating operation. Thus, even if the authorized user will copy the classified information in the popular table, less reliable users cannot read it.

The special privilege, DOWNGRADE, allows to change safety labels, associated with the data. Similar possibility is necessary, for example, for correction of the labels, for whatever reasons appeared the wrong.

It is represented natural that DBMS INGRES/Enhanced Security supposes not only hidden, but also obvious inclusion of labels of safety in relational tables. There was a new data type, security label, supporting corresponding operations of comparison.

INGRES/Enhanced Security - the first DBMS, received the certificate equivalent to certification on a class of safety B1. Possibly, safety labels gradually will enter into standard repertoire of management systems databases.

Дякую за увагу!!!