ASPECTS REGARDING THE SECURITY OF INFORMATION AND DATABASES OF THE STRATEGIC INFORMATION SYSTEM

Ion BĂLĂCEANU, Eugen POROJAN

"Center for Analysis and Security Studies" Association, Bucharest, Romania

Abstract: *The permanent objective of any information system is to ensure, in conditions of maximum precision and efficiency, the information required by management and executive structures in order to decide and act efficiently and in a proper manner. Direct and indirect methods of action used against this desideratum, although it seems unimaginable under the current conditions of "total transparency" of the battlefield, are actions of masking and deceit in order to achieve surprise and to avoid being caught by surprise.*

Keywords: *information; information channels, information security, information systems, databases, security mechanism, information environment, information culture.*

1. INTRODUCTION

The information system, as part of the whole management of the military structure, contributes to directing and focusing the effort of decision and action, under maximum convenience and efficiency. Increasing the performance of an information system is given by the need to adapt to the new conditions of the current security environment, the continuous development of techniques and information technologies, structural, economic and financial limits.

The structure of the security mechanism is hierarchically functional with structured security elements that are able to cover the physical, technological, and personnel information and ensure all security services: protection, deterrence, detection, delay, stops; limiting or annihilating consequences of unwanted security events; resuming the production and post factum analysis to improve security reactions.

2. INFORMATION SECURITY WITHIN THE STRATEGIC INFORMATION SYSTEM

Regarding *information security* during their movement through the information system, (given that the information system is vulnerable, especially in terms of ensuring security of information circulation outside the structures of the Ministry of National Defense), the main problem is ensuring protection of data content in the transmission of information. This environment may consist of national communications network, allocated or leased trunks from fixed telephony operators, or air environment for radio communications.

Analyzing this perspective, we believe that information security can be achieved, depending on the nature of the information conveyed, primarily through *cryptography*. The digital encryption allows information to be reduced to a stream of binary data. Specialized cryptographic mechanism creates a long stream of binary repetitive digits, based on a traffic encryption code (TEK - Traffic Encryption Key).

Data flow along with string of random numbers, properly mixed, creates the encrypted data or cipher text. A binary stream carried in this way will be unpredictable, providing a very secure way to defense information. The entire analog signals specific to information systems are more predictable and obviously less secure.

A new type of key control system, used due to its efficiency, is the cryptography made with public keys. Under this level, each user produces two keys. One is the public key "Y" and the other is the private key "X". Using this system, one can communicate a piece of information, from anywhere, encrypted with the Y key, which can be decrypted only by the user who holds the X key. Thus, in a system that uses this way of working with the public keys, exchanges classified on two levels are possible. This is called asymmetric key set. On the other hand, there is a set of symmetric keys which, by working with the same key, encrypts or decrypts data. Since both the operator and the operator issuing the received message must have the same key, this set offers the highest level of security.

An effective solution, recently developed for the radio networks, uses radio system reprogramming (OTAR - Over The Air Rekeying). This technical way of working almost eliminates the requirement to manually load the keys, providing secure management. OTAR is a way of key distribution that contains an encryption / hide key (KEK - Key Encryption Key) used to hide the encryption key of work, and more functional keys, TRANSEC or COMSEC. Such process is called 'packing' to be distinguished from traffic encryption. The unique initial key to be accessed both in emission units and in the receiver is the key KEK. After packing, the phase that follows is distribution, a process that can use any physical or electronic means. In OTAR, the "wrapped" keys are trapped in a message transmitted by radio link and to the desired station; using link protocols without error (any error would bring the keys in an ineffective situation). The link is permanently encrypted by the available traffic encryption key.

The content of the key is twice protected during radio transmission, effectively eliminating any possibility of discredit.

For higher security level, it is customary to digitize through a coder, the digital signal being then treated as a real data stream.

Basic security services for each local computer network of the information system included in the security architecture OSI (Open Systems Interconnection) are as follows:

- *authentication*, away identity verification of a communication unit (message) and its source;
- *access control*, which provides protection from unauthorized use of resources;
- *data privacy*, data protection against unauthorized reading;
- *data integrity*, ensures true content of all data belonging to users of the network or of selected fields in messages exchanged by a link connection-oriented or non-oriented, ensuring detection of any changes, insertions or deletions of data;
- *provenience or delivery confirmation.*

3. DATABASE SECURITY WITHIN THE STRATEGIC INFORMATION SYSTEM

The overall objective of the management system for distributed databases is to obtain full software support to enable developing database exercises. But this objective cannot be achieved without taking into account the operational objectives of the information system. Mainly, these operational objectives consist of providing security for circulating data and ensuring the achievement of strategic information in real time.

The database security means protecting databases against unauthorized use and especially against unwanted changes and destruction of data or unauthorized data readings. Technical and administrative measures are taken in order to gain information security. Database security is generally associated with the following conditions: illegal access to data, loss of confidentiality, loss of character of data, loss of data integrity, loss of data availability. It is more difficult to protect the data against fraudulent access. In fact, it is known that there can be no safe protection systems, but only security measures and information protection with greater or lesser effectiveness.

Fraudulent access to databases is represented by: unauthorized data reading, unauthorized data editing, unauthorized data deleting. The database security concept is associated with bad intended access, while integrity means avoiding accidental loss in the data consistency.

Security measures for database protection are taken on many levels: *physical level* – the room in which the PCs are situated is protected against unauthorized access; *human level* – limited information access is recommended, while authorizations should be given carefully, with written evidence of authorized persons; *operating system level* – data protection weaknesses may be eliminated or compensated with other measures; *database management level* – the system should allow privileges in order to consolidate data protection.

Regarding data security only authorized and controlled access should be allowed, the main responsibility belonging to the database administrator. The main aspects of providing database security, according to us, are: authorized building access, through passwords, operator classes and operator profiles; use of views for external database schemes; special access procedures and data encryption through encryption/decryption schemes.

For *authorizing building entrance* by passwords, classes of operators (with certain privileges) and operator profiles (name, password, class, code, level of access, potential resources), each user is given different operating limits for portions of the database, at certain levels, such as: relation, record, page, attribute, etc.. Limits or data access rights refer to the possibility of reading, insertion, deletion or modification of data, and editing of reports. Identity verification is usually done by codes or passwords approved either by the database head / administrator or system administrator.

Using views for external database schemes is achieved by defining logical partitions of a database for different users (how does an operator see the information in the database at a specific moment). Ability to "protect" part of the information in the database is used for setting a certain degree of data protection. In this perspective, we can discuss about relationship-based access (table) or view-based access.

In human resources management system, for some users, view changes are not accepted.

Such views are read-only and are used mainly in applications where data can be accessed by all users (such as vacancies, graduates of educational institutions etc.), but changes are made only by authorized persons and with upper echelon approval. Information changes are not permitted as they can cause side effects that concern parts that are not visible for database users. For example, deletion of information may involve removal of other components related to the deleted item which are not visible for users at the time.

Special data access procedures govern access to the database management system only for certain authorized users. In this respect, a strict record of operating rights for each user is kept, for each portion of the database. Rules and procedures are also set for transmitting the operating right from one user to another.

Data encoding is done by indexing schemes and procedures for encryption / decryption. Specific input algorithms and keys (passwords) to routines are used in order to encrypt data. Because one may access data by other means than database management application (eg direct reading from the electromagnetic environment), security can be achieved by keeping the data encrypted in the electromagnetic environment. Decoding of information is performed only after user identification associated with individual passwords.

Database integrity involves ensuring the accuracy of the information and involves detection, correction and prevention of errors that can distort data in databases. In this respect, we believe that the data is validated relative to any restrictions formulated by database design and, therefore, data is regarded as valid.

The integrity conditions are rules or restrictions that prevent entry into the database of false information and are expressed in terms of data conditioning. Structural conditions are connected to certain equality between values and are expressed by functional dependencies or by declaring some unique fields (in some cases these are key fields). They can be classified by the unit to which the restriction refers: restrictions on areas (targeting specific attribute values) or table restrictions (relations).

Given the need for data security between computer networks, we consider as relevant the following activities: providing semantic

data integrity, concurrent access to data, saving and restoring data. Ensuring semantic integrity of data is achieved by: determining an *application code* that can be implemented as stored procedure in the database or as software applications; executable *operational programs* (eg PL / SQL by ORACLE) only when an event occurs, such as: insert, update, delete and so on; *statement integrity restrictions* designed to improve operating performance of databases, which are introduced according to the data structure of the database. These are easy to be stated and modified in the application and can be automatically verified and respected for all operations performed in the database when manipulating data.

To conclude, database security can be achieved primarily through authorization policies for operators. In this respect, they will receive adequate operating rights, according to hierarchical level and nature of data and operating information that they work with. To accomplish this goal, one may be given the following types of authorization: read (consultation), insert (add), update (without deletions), authorized deletions (*tuple* level) and authorized editing (obtaining reports). This does not involve scheme changes in the database. Also, database security is achieved through data encryption by using (automatically or on operator demand) encoding or decoding routines that make the access impossible for unauthorized users.

BIBLIOGRAPHY

1. Alexandrescu, C., Boaru, Ghe., (2009). *Sisteme informaționale – fundamente teoretice*, Bucureşti: UNAp „Carol I”.
2. Alexandrescu, G., Ilie Ghe., Stoian, I. (2005). *Modelarea sistemelor şi proceselor.* Bucureşti: UNAp „Carol I”.
3. Berlinger G., Castro D., Mills A., *Data, Information, Knowledge and Wisdom,* http:// www.outsight.com/ system/dikw/Dikw/htm.
4. Constantinescu, Carmen. (2006). *Particularități ale tehnologiei informației pentru managementul strategic*. Bucureşti: Ed. Economică.
5. Gruia, Timofte. (1999). *Comunicații militare moderne.* Bucureşti: AISM.
6. Nicolaescu, Ghe., Simileanu, V. (2005). *Restructurarea sistemelor informaționale*. Bucureşti: UNAp „Carol I”.
7. Neacşu, D., (2012). *Perfecționarea sistemului informațional strategic în contextul noului mediu operațional*. Bucureşti: UNAp „Carol I”.
8. Savu, Ghe., Pârlog A., (2008). *Producția de intelligence*. Bucureşti: Ed. Medro.
9. Teodorescu, Constantin, (2005). *Războiul informațional – Agenții şi servicii de informații.* Bucureşti: UNAp „Carol I”.
10. ***, (2004). *Doctrina națională a informațiilor pentru securitate.* Bucureşti: Ed. SRI.
11. ***, (2004). *Concepția C4ISR în Armata României*. Direcția Comunicații şi Informatică. Bucureşti.
12. ***, (2005). *I.P.S.-3, Doctrina pentru informații, contrainformații şi securitate a armatei*, Bucureşti.
13. ***, (2012) Studiul C4I2SR pentru Armata României, Bucureşti.