IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP5242

This paper appears in *Managing Modern Organizations Through Information Technology*, Proceedings of the 2005 Information Resources Management Association International Conference, edited by Mehdi Khosrow-Pour.

Security Model for Businesses with Network Data Structures

Lech J. Janczewski and Victor Portougal
Dept of Info. Systems & Operations Mgt., The University of Auckland, Private Bag 92019, Auckland, New Zealand
{lech, v.portugal@auckland.ac.nz}

ABSTRACT

The paper discusses a model of security profiles for employees within industrial or commercial organisations. The information objects there are often connected to each other in a network structure. As a result security clearances based individual positions within the organization hierarchy may not be adequate. A method is presented for calculating security values of objects (security categories) and security clearances for employees in relation to the value of information accessible for each employee.

INTRODUCTION

Classic security models like the Bell-LaPadula Disclosure Model (Bell, 1973) or the Biba Integrity Model, (Biba, 1975) were criticised as being not relevant to the real word business environment. Indeed, these models were set up to fulfil needs of the military sector. There were many further attempts to rectify that, both by introducing some changes to these models (like Low-Water Mark Biba Model) or by developing entirely new models, like this by Clark-Wilson (1987). One of the best papers in this field written by John McLean (1994) presents the review of these models.

In any of these cases an important problem was not addressed, which is commonly referred to as the "jigsaw puzzle" intelligence. A watchful analysis of the officially collected materials allows obtaining sometimes highly classified information. For example, close monitoring and analysis of the registration plates of military vehicles at barrack gates could detect movement of military units. The same principle may be applied to business facilities. It is estimated that 80% to 90% of the data collected by intelligence gathering organisations (both civilian and military) originate from entirely legal sources and are obtained without any security breakage.

Reconstruction of classified information (without adequate security clearance) through an analysis of accessible data is based on the fact that the most of data used in business, production, services and military services are logically connected. Knowledge of that connection algorithm allows to reconstruct a relatively accurate model of the reality with the use of only few components.

There are many organizations around the world having a certain type of activities as their main source of income. These organizations are generally labelled as "business intelligence (gathering) organizations". They have their own representation, code of practice and annual conferences (see, for example, google.com results of the "business intelligence" search).

The main argument presented in this paper is that clearances assigned to individuals should not be based on the position of the bearer within the organizational hierarchy. Rather, the individual clearances should be defined by the confidentiality of the documents the employees use in their everyday managerial activity. The methods for defining security clearances depend on the information structure in the organization. For a hierarchical model Portougal & Janczewski, (1998), suggested an algorithm that assigns crisp security categories. Later on they expanded (Portougal & Janczewski, 2000) the algorithm to the security categories treated as fuzzy intervals.

The models with hierarchical data structures showed some unexpected results. Naturally, the security clearances depended on the form of the data tree. A perfect data tree, having at least two branches on each organisational level and no overlapping of data (i.e. any data unit is known to only one person on a given organisational level) would produce security clearances directly adequate to the position of the person with respect to this organisational level. Otherwise, with real-life trees, the differences were dramatic.

This paper is an attempt to expand our result to security policies of organizations that have network information systems structures.

AN EXAMPLE

To illustrate the specific security issues imposed by a network-form database structure in a production environment let us consider a case of the following production facility. It has three production divisions or Production Units (PU1, PU2, and PU3). The organisational structure of the facility is shown in Fig 1.

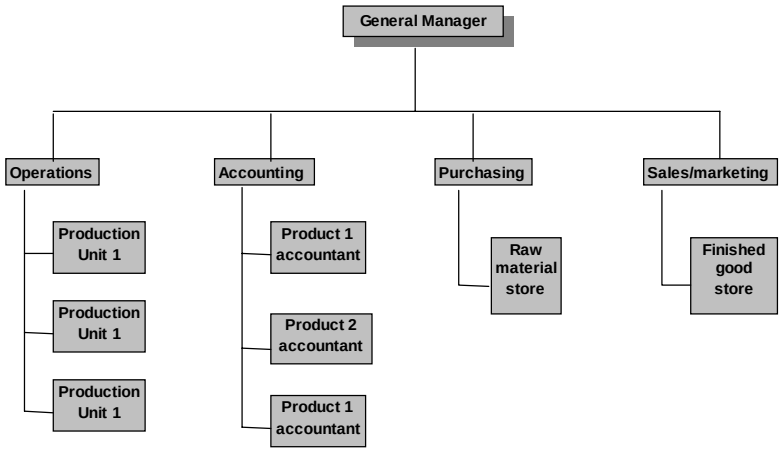
Some of the important properties of this production facility are as follows:

1. Functions of each organisational unit are presented in Table 1.
2. Each production unit manufactures different products.
3. Each organisational unit employs at least one manager.

DATA ACCESS STATEMENT

Every manager as part of his/her job description has a Data Access Statements (DAS) (Portougal & Janczewski, 1998), that is defined as follows:

Figure 1. Organisational Structure of the Facility



- *Data Access Statements* (DAS) of a staff member is a vector, containing *Data Access Statements Elements* (DASE) as its components.
- Each DASE is an existing or newly created element of the organisation's database.
- Each DASE defines what type of access to information/data is allowed (read, write, delete, etc).
- Each DASE is defined as a result of the analysis of the job description related to the given position.
- Each DASE has a confidentiality parameter CP assigned (see Table 2).

Consequently, DAS is a label describing detail of the security of the set of data necessary to perform all the regular work of an individual. The assignment of the CP to the elementary data units is a job for security specialists. However, when the elements are interconnected as a network, special network algorithms should be used. Below we present such algorithm, and illustrate the assignment of CP to database elements, when the database has a complex network structure. The following settings are used in the example:

1. There are three key indicators ("Production volume", "Sales" and "Costs") calculated in a hierarchical way from elementary data feedback. The feedback is collected regularly (some daily, some weekly, and some monthly) and is accumulated through the year. The detailed structure of "Costs" is presented in Fig 2. "Sales" data are divided into 3 sets: "Sales of Product N1", "Sales of Product N2", and "Sales of Product N3". The structure of "Production Volume" is divided into two subgroups: "Production Volume" and "Work-in-Process". Both subgroups are divided further into 3 categories corresponding to 3 products: N1, N2 and N3.
2. The security categories depend on the total security value of information presented in the documents. It is called the security clearance value (SCV). It is assumed that an employee does not have access to the data other then necessary for performing of his/her duties, or in other words his/her security clearance should not exceed the security category necessary to use information they need to perform their functions properly.

THE MODEL

The key elements of the model are:

1. *The set of key indicators* (which need to be protected). Let the total number of these indicators be K.
2. *Data structures of all key indicators*. Basically, all performance indicators have a hierarchical structure and thus every key indicator can be modelled as a tree (like in the Fig 2). However, because all indicators are formed from elementary data feedback, the general structure of the data flow in the company will be a network, shown in Fig 3. Here, the elementary key feedback indicators are provided by elements, placed at the bottom of the Fig 3 and labelled 29 to 40 corresponding to:
   - 29/31 - Finished goods report, by product, fed in the system daily by finished goods store manager
   - 32/34 - Overhead distributions, by product, prepared weekly by product accountants
   - 35/37 - Material reports, by product, prepared weekly by raw material store manager
   - 38/40 - Sales reports, by product, prepared daily by product accountants

Note that label of each box in Fig 3 has a form of X:Y where X is the type of the report listed in Table 3, while Y is the calculated SCV value for that report. Listing of all the performance indicators is presented in the Table 3.

3. *"Confidentiality Parameter"* (CP_i), which is assigned to every element *i* as follows:
   a. all the elementary data feedback nodes have $CP_i = 1$,
   b. from the network Fig 3 derive a tree, in which the element *i* is a root
   c. CP_i will be equal to the number of elementary data feedback nodes this tree has. The detailed algorithm of assigning the CPs is given below.
4. From the computational point of view the order of assigning the CP_I is immaterial.
5. The goal of the modelling is to assign to every staff member a *Security Clearance Value* (SCV), which will define his/her security clearance. To reach this goal, the following algorithm was developed.

THE ALGORITHM

The algorithm works for every DAS sequentially, matching it against data network also sequentially; the order of the statements is immaterial.

Begin

Step 1. Choose a DAS. Form a tree, in which the DAS is the root, and the next level are all DASE from this DAS. Each DASE complement

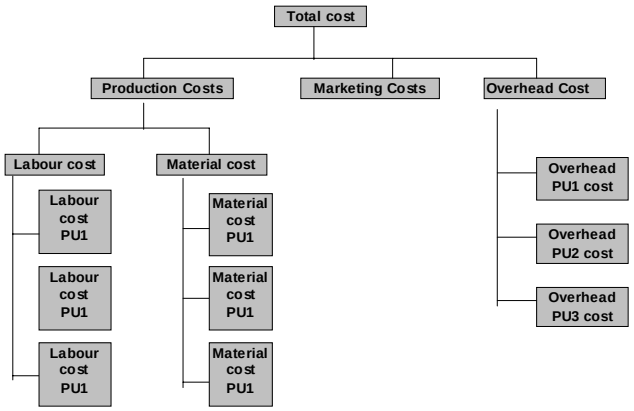
Table 1. Functions of Organisational Units

Operations	Organization, planning and coordination of production facilities in Production Units 1 to 3
Accounting	All accounting operations plus staffing
Purchasing	Supply / storage of the raw materials
Sales/marketing	Storage / distribution of the finished products
Production Units 1 to 3	Mmanagement of production facilities

Table 2. Summary of the CPs plus SCV Calculations

Position name	DAS with listing of DASEs and document numbers	CP	SCV
General Manager (GM)	Sales (2) Production volumes (3) Cost (1)	3 3 12	12
Operations (OP)	Production volumes (3) Labour cost (9) Material cost (10) Production cost (4) Production in process (8) Production finished (7) Overhead cost (6)	3 6 6 6 6 6 6	12
Accountant General (AG)	Production volumes (3) Labour cost (9) Material cost (10) Production cost (4) Production in process (8) Production finished (7) Overhead cost (6))	3 6 6 6 6 6 6	12
Purchasing (PUR)	Material cost (10)	6	6
Sales and Marketing (S&M)	Sales (2) Production volumes (3) Marketing cost (5)	3 3 3	9
Production Unit N (PUN)	Overhead cost product N (11-13) Finished product N (17-19) Product in process N (20-22) Labour cost product N 23-25 Material cost product N 26-28 Overhead marketing cost product N (32-34)	2 2 2 2 2 1	4
Account N Manager (ANM)	Sales product N (14-16) Overhead cost product N (11-13) Finished product N (17-19) Product in process N (20-22) Labour cost product N 23-25 Material cost product N 26-28 Overhead marketing cost product N (32-34)	2 2 2 2 2 2 1	4
Raw material Store Manager (RM)	Material report product N1/N3 (35-37) Material costs (10)	1 6	6
Finished Goods Store (FGS)	Finished good report product N1/N3 (29-31) Sales report product N1/N3 (38-40)	1 1	6

Figure 2. Detailed Structure of Costs



with a tree from the common network (Fig 3) down to the elementary data feedback nodes.

Step 2. Set the confidentiality parameter CP equal to the number of the elementary data feedback nodes in the tree.

Step 3. If this DAS is the last, go to step 4, otherwise choose the next DAS and go to Step 1.

Step 4. End

END

EXAMPLE

Step 1: Calculation of SCV will be presented for *Sales*. The three is built from the following boxes: 2, 14, 15, 16, 38, 39, and 40. Note that for clarity, some reports are graphically grouped like Sales Reports for Product N1, N2, and N3. All the elementary CP values are equal to 1 (boxes 38, 39, and 40).

Step2: At the second level (reports 14,15, and 16) tree is not getting new roots, hence the final SP count for Sales is equal to 3 (the sum of Sales Reports N1/N3) which is indicated in the box 2 in Fig 3.

Note that the value of SCV for the General Manager, Operation Manager and Accountant General must be the same and equal to 12 as all of them have access to all elementary data (boxes 29/40).

Figure 3. Data Flow Network

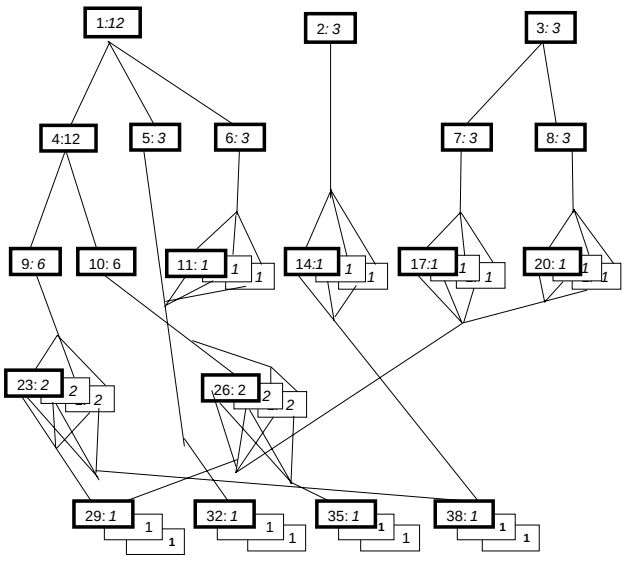


Table 3. Explanation of Elements from Figure 2

	Type of report	Frequency	Position responsible for generation of the report
1	Cost	monthly	Accountant general
2	Sales	monthly	Accountant general
3	Production volumes	monthly	Operations manager
4	Production cost	monthly	Accountant general
5	Marketing cost	monthly	Sales/marketing manager
6	Overhead cost	monthly	Accountant general
7	Production finished	monthly	Operations manager
8	Production in process	monthly	Operations manager
9	Labout cost	weekly	Accountant general
10	Material cost	weekly	Raw material store manager
11	Overhead cost product N1	weekly	Product accountants 1
12	Overhead cost product N2	weekly	Product accountants 2
13	Overhead cost product N3	weekly	Product accountants 3
14	Sales product N1	weekly	Finished goods store manager
15	Sales product N2	weekly	Finished goods store manager
16	Sales product N3	weekly	Finished goods store manager
17	Finished product N1	weekly	Production unit manager 1
18	Finished product N2	weekly	Production unit manager 2
19	Finished product N3	weekly	Production unit manager 3
20	Product in process N1	weekly	Production unit manager 1
21	Product in process N2	weekly	Production unit manager 2
22	Product in process N3	weekly	Production unit manager 3
23	Labour cost product N1	weekly	Product accountants 1
24	Labour cost product N2	weekly	Product accountants 2
25	Labour cost product N3	weekly	Product accountants 3
26	Material cost product N1	weekly	Product accountants 1
27	Material cost product N2	weekly	Product accountants 2
28	Material cost product N3	weekly	Product accountants 3
29	Finished goods report product N1	daily	Finished goods store manager
30	Finished goods report product N2	daily	Finished goods store manager
31	Finished goods report product N3	daily	Finished goods store manager
32	Overhead marketing cost product N1	weekly	Product accountants
33	Overhead marketing cost product N2	weekly	Product accountants
34	Overhead marketing cost product N3	weekly	Product accountants
35	Material report product N1	weekly	Raw material store manager
36	Material report product N2	weekly	Raw material store manager
37	Material report product N3	weekly	Raw material store manager
38	Sales report product N1	daily	Product accountants
39	Sales report product N2	daily	Product accountants
40	Sales report product N3	daily	Product accountants

The model may be also formally presented as a variant of the network flow model. The CP's are the flow capacity of its arcs. Any DAS defines a cut in a tree. It is required to define the maximum capacity of the cut. With the simple structure of the network there is no need to use the general model, and that is why the above practical algorithm may be recommended for use in practice.

Let us examine implementation of the defined model and algorithm to the example presented this paper. Following the outlined algorithm the calculated SCV are placed in the Table 2. Few additional comments must be made:

1. In the reality set of the key indicators is more elaborate, but data suggested in Table 2 are essential.
2. For the purpose of this example it is also assumed that sales are generated only through the sales of products N_1, N_2 and N_3 and that the volume of products can not be generated from the stock of the raw materials.
3. In this production facility the security clearances were defined using SCV as it is shown in Table 5.

DISCUSSION

Before implementation of the model described above, the company had three security categories: "Secret", "Confidential" and "Internal use" defined in Tab 4.

Key indicators showing total production volume, sales and costs were considered "secret". The security clearances were related to the position of given employee within the organisational framework and are summarised in Table 5. As the result, the security clearances for each organisational unit were as presented in Table 6.

After the introduction of the algorithm calculating the real security clearance values, and the proper definition of security clearances (Tab 5), the structure of security clearances changed (Table 6, last column).

Table 4. Structure of the Security Clearances

Security category	Security clearance associated with
Secret	General manager
Confidential	Level 2 management
Internal use	Level 3 management

Table 5. Definition of Security Clearances

Security clearance	SCV
Secret	greater or equal to 10
Confidential	greater or equal to 6
Internal use	less then 6

Table 6. List of Individual Security Clearances

Level	Position name	Initial Security clearance	Calculated Security clearance
1	General Manager	S	S
2	Operations manager	C	S
3	Production Unit 1 mgr	IU	IU
3	Production Unit 2 mgr	IU	IU
3	Production Unit 3 mgr	IU	IU
2	Accounting mgr	C	S
3	Product 1 accountant	IU	IU
3	Product 2 accountant	IU	IU
3	Product 3 accountant	IU	IU
2	Purchasing mgr	C	C
3	Raw material store mgr	IU	C
2	Marketing mgr	C	C
3	Finished goods store mgr	IU	C

Analysis of the information flow in the company shows that in a number of cases the security clearances are not matching the amount and confidentiality of information the employees are having an access to. "Finished good store" manager is perhaps the best example. By the virtue of that person's activities he/she could have a total knowledge of production and sales volumes, while this person security clearance was set-up only on the "internal use" level.

The general tendency is that application of the above mentioned analysis raises security clearances of some people occupying pivotal positions in the terms of access to data, but placed low at the company organizational hierarchy.

CONCLUSION

In this paper we defined security models, which take into consideration the actual structures of industrial databases. In reality information processed and stored in a database is interconnected. These connections may allow calculation or estimation of, sometimes quite confidential, information. Knowledge of these relationships therefore might influence significantly the content of security labels attached to objects and subjects. We addressed this problem under assumption that the database has a network structure.

In the literature very often we read that the "information has value". The presented method of calculation security clearances is directly related to this statement.

There are several possible ways to expand this work. The main direction is connected with the dynamics of data generation. In our models we assume that data is always available. In reality generation of information may be done in many different ways: all the data could be generated in one day, everyday, or any other pattern is possible. Information contained in a batch could have the same security value, or the value could be proportional to the number of days covered by the batch. The static models are simple and easy to understand; therefore they are attractive as an approximation of the dynamic reality. But in a complex case, when these effects are significant, a dynamic model is more appropriate.

REFERENCES

Bell, D., LaPadula, L. (1973), Secure Computer Systems: Mathematical Foundations, ESD-TR-306, Mitre Corporation.

Biba, K. (1975), Integrity Considerations fro Secure Computer Systems, MTR-3153, Mitre Corporation.

Clark, D., Wilson, D., (1987), A Comparison of Commercial and Military Computer Security Models, Proceedings of the IEEE Symposium on Security and Privacy.

Portougal, V., Janczewski, L. (1998), Industrial Information-weight security models, Information Management & Computer Security, Vol. 6. No 5, UK.

Portougal, V., Janczewski, L., (2000), Need-to-know" principle and fuzzy security clearances modelling, Information Management & Computer Security, Vol. 8. No 5, UK.

McLean, J. (1994), Security Models, Encyclopaedia of Software Engineering, John Wiley \& Sons.