ASSIGNMENT OF SECURITY CLEARANCES IN AN ORGANIZATION

Lech J. Janczewski, Victor Portougal
Department of Management Science and Information Systems, The University of Auckland, Private Bag 92019, Auckland, New Zealand

Abstract: The paper discusses the assignment of security clearances to employees in a security conscious organization. New approaches are suggested for solving two major problems. First, full implementation of the 'need-to-know' principle is provided by the introduction of Data Access Statements (DAS) as part of employee's job description. Second, for the problem of setting up border points between different security clearances, the paper introduces a fuzzy set model. This model helps to solve this problem, effectively connecting it with the cost of security. Finally, a method is presented for calculating security values of objects security clearances for employees when the information objects are connected to each other in a network structure.

Key words: Information security, data security, security models, security clearances, fuzzy sets, Data Access Statement.

1. INTRODUCTION

Managing Information Security depends on business environment, people, information technology, management styles, and time – to list the most important. An analysis of the chain of security arrangements shows a significant weak point. It is the issue of assigning security clearances to an individual. This paper presents an attempt to solve this problem by the optimisation of an information security system subject to cost constraints. As a result, an optimisation procedure that assigns formally the security clearances to all employees of an organisation has been developed. In a typical business environment this procedure is based on the position of a

given person within the hierarchy of an organisation. The general principle is that "the higher you are within the company hierarchy the highest security clearance you must have". Such an approach clearly incurs significant problems. In the one extreme a person might have a security clearance that is too high for his/her job, which increases the total cost of the security system. The higher the security clearance, the higher the cost (for instance, of security training). On the opposite side a person with a security clearance too low for his/her job must obtain temporary authority for accessing specific documents. Such a procedure could be costly, time consuming and decrease the efficiency of operations. Portougal & Janczewski (1998) demonstrated the consequences of the described approach in complex hierarchical structures.

A competing and more logical idea is to apply the "need to know" principle. Unfortunately, this principle does not give adequate guidance to the management as to how to set-up security clearances for each member of the staff. Amoroso, (1994) describes the "principle of least privilege". The recommended application is based on subdividing the information system into certain data domains. Data domains in the main contain secret or confidential information. Users have privileges (or rights to access) to perform operations for which they have a legitimate need. "Legitimate need" for a privilege is generally based on a job function (or a role). If a privilege includes access to a domain with confidential data, then the user is assigned a corresponding security clearance. It is easy to see the main flaw of this approach is that a user has access to the whole domain even if he/she might not need a major part of it. Thus the assigned security clearance may be excessive. A similar problem arises regarding the security category of an object. A particular document (domain) could be labelled "confidential" or "top secret" even if it contains a single element of confidential (top secret) information. In this paper we suggest another realisation of the "need to know" principle. Our method is based on the Data Access Statements (DAS), defined for every employee as part of their job description. DAS lists all data elements needed by an employee to perform her/his duties effectively. Thus we shift the assignment of security clearance from the domain level to the element level.

Our approach allows not only the solving of the difficult problem of defining individual security clearances. It also connects this problem to more general problems of the security of the organisation as a whole, to the problem of security cost and cost optimisation.

2. DATA ACCESS STATEMENT

There is a lot of attention in literature to employee specifications and job analysis. It is strange though, that the one of the most important aspects of the job analysis, which is information use, is completely out of specification. We suggest that in addition to the main content of a job description a Data Access Statement (DAS) for every employee is added.

Schuler (1992) defined the following components of a job description:

- Job or Payroll title,
- Job number and job group to which the job belongs,
- Department and/or division where the job is located,
- Name of incumbent and name of job analyst,
- Primary function or summary of the job,
- Description of the major duties and responsibilities of the job,
- Description of the skills, knowledge and abilities,
- Relationship to other jobs.

The job description is the best place to define the security clearance of employee through DAS. It could be, for instance, an additional "bullet point' in the above list.

DAS was introduced earlier by (Portougal & Janczewski, 1998), and was defined as follows:

1. *Data Access Statements* (DAS) of a staff member is a vector, containing *Data Access Statements Elements* (DASE) as its components.
2. Each DASE defines what type of access to information/data is allowed (read, write, delete, etc)
3. Each DASE is defined as a result of the analysis of the job description document related to the given position
4. Each DASE has a confidentiality parameter CP assigned (being an element of the organization's database it should have the same value CP, e.g. 1, if we think they are all of equal value).

An example of DAS statements is presented in Table 1. At the bottom of the column the total value of information accessible is shown. We shall call it SCV – *Security Clearance Value*, thus tying the assignment of a security clearance to the volume of accessible information.

Any production facility has an information system. Table 1 lists all the data elements used within an organization. Every data element has an assigned confidentiality parameter (CP), which characterizes its importance from the point of view of security. For more about assigning CP's refer (Portougal & Janczewski, 1998).

Table 1. Database elements listing and DAS for all employees of the production facility

	CP	A	B	C	D	E	F	G	H	I
Volume of products	**1**	√	√	√		√				√
Sales	**1**	√		√		√				√
Labour cost	**1**	√	√	√						
Material cost	**1**	√	√	√	√				√	
Cost	**1**	√	√	√		√				
Labour cost (of N)	**1**	√	√	√			√	√		
Materials cost (of N)	**1**	√	√	√	√		√	√	√	
Sales (by products)	**1**	√		√		√	√	√		√
Volume of products (by product)	**1**	√	√	√		√	√	√		√
Costs (by products)	**1**	√	√	√			√	√		
Costs (by materials)	**1**	√	√	√	√		√	√	√	
TOTAL (SCV)		11	9	11	3	5	6	6	3	4

Positions Codes:

A: General Manager
B: Operations
C: Accountant General
D: Purchasing
E: Sales and Marketing
F: Production Unit N
G: Account N Manager
H: Raw material Store Manager
I: Finished Goods Store

In this example we assume that each data element is independent, so knowledge of a particular element does not allow one to find the value of the other. In order not to overcomplicate the example we assume all CP equal to 1.

3. MODELLING SECURITY CLEARANCES

The security clearance allows a person to access a certain part of a database. We can assume that the optimum security clearance is assigned strictly in accordance with the "need to know" principle. Unfortunately, the "need to know" principle assigns to every employee a specific area of the database, and generally there will be as many different areas as the number of employees. At the same time, there are always a limited (2-4) number of security clearances. Thus the assigned clearance will practically always be different from optimum, below or above that optimal point.

Clearly, the probability of an information leak goes up, when the difference between the actually assigned clearance and the optimum clearance is increasing. At the same time assigning extra security clearance involves extra cost. Let us analyse the cost of assigning security clearances to particular persons in a more detailed way.

There is a correlation between security of the system, numbers of security measures, and their costs, i.e.

more security measures ⇒ more secure system ⇒ more costs

Many sources, e.g.: (Frank, 1992) indicate the above correlation is not linear but has a tendency to grow exponentially. Similar situations exist in the case of assigning security clearances. The higher security clearance of an employee means a higher expenditure to the employer. The structure of costs would be somehow different from the security measures listed above. The costs like those listed below would be of significance:

- Examination of candidate credentials,
- Security training,
- Security equipment (especially for accessing protected zones, either physical or system),
- Management of the system controlling the security clearances.

Again one might expect that there is a correlation of security clearances with costs:

higher security clearance granted ⇒ higher costs for the organization

The security clearances should be directly related to the jobs and should follow the "need to know" principle. The security clearances are designed to subdivide the employees of the organization into classes according to data access privileges, e.g. secret, confidential and general. Following the usual approach, borderlines should be drawn, defining the minimum amounts and

importance of data in use for each category. It was analyzed in the Introduction that, before our development of quantitative measures of confidentiality (CP), this subdivision was performed either by employees' position or by assigning security categories to data domains, and then using these categories for defining clearances. With the CP and SCV defined the problem becomes much easier and more logical to solve.

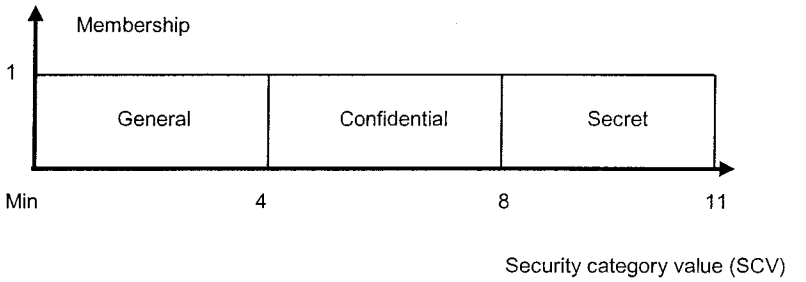

Figure 1. Security categories (crisp representations)

In our example (Figure 1), let us have three security categories: *general*, *confidential* and *secret*. We shall define the borderline SCV between *general* and *confidential* as 4, and the borderline SCV between *confidential* and *secret* as 8. If the total SCV of information in use by an employee is less or equal to four, then this person is not required to follow special security procedures at all, and he/she would be assigned a general clearance. If the total SCV is between five and eight, then the *confidential* clearance should be applied, meaning that this employee is under an obligation to use and follow all the security procedures defined for this clearance. Similarly, if the SCV of data in use is more than eight, then this employee should be assigned the *secret* clearance.

Though this procedure is simple and easy to understand, nevertheless it has two weak points:

1. This procedure implies that the security experts will be able to define the borderlines. In reality it is not so easy, and sometimes the decision about the borderlines is provided by reasons well outside the model, for example by position.
2. Under this procedure it is hard to explain why employees with SCV close to the borderline from different sides have different clearances. What is the crucial reason for an employee with SCV equal to 0.79 has a clearance *confidential*, but his colleague with SCV = 0.81 has *secret* clearance?

Both points indicate an inadequacy in our security clearance modeling. Basically, the inadequacy comes from using a classical *crisp set* for modeling, like this used by (Pfleeger, 1997). The crisp set is defined in such a way as to dichotomise the individuals into two groups: members (those that certainly belong to the set) and not members (those that certainly do not). A sharp distinction should exist between members and non-members of the class. This is definitely not so in our case. The classes of security clearances do not exhibit this characteristic. Instead, the transition from member to non-member of one class appears gradually rather than abruptly. This is the basic concept of fuzzy sets.

In the first fuzzy model we shall assume only two security clearance classes: *general* (set G) with no security cost and *secret* (set S) with a security cost A for each member of the class. The membership functions of class S are given in Figure 2. The vertical lines on Figure 2 represent the employees of the example company and the value of their membership function in the set S. General Manager and Accountant General have the value equal to 11 (A,B), Operations Manager has it equal to 9/11 (C), Purchasing Manager has it equal to 3/11 (I), etc.

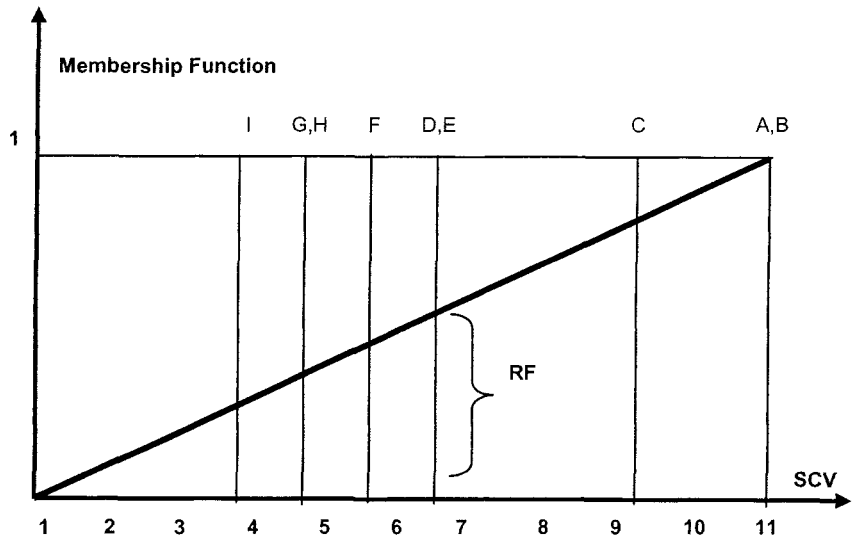

Figure 2. Membership function for the fuzzy set "secret"

If we assign to every manager the security clearance *secret*, then the cost of the security system will be equal to 9A (As there are 9 managerial

positions in the company). If this is not affordable, then some of the managers will be put into G class. This involves a risk of information leak.

Let us assume that this risk is proportional to SCV (the more a person knows the higher is the risk). We shall introduce the *risk factor* (RF) for an employee *i* as:

$$\mathbf{RF}_i = \mathbf{SCV}_i / \mathbf{SCV}_{max}$$

A good estimate for the *company risk factor* (CRF) would be either:

$$\mathbf{CRF}_{max} = \mathbf{max}_i \mathbf{RF}_i, \text{ or}$$
$$\mathbf{CRF}_{av} = \Sigma_i \mathbf{RF}_i / \mathbf{N},$$

where N is the total number of employees.

CRF_{max} characterises the risk of information leak from the most informed employee. It is better for evaluation than CRF_{av}, when the SCV_i of the employees are diverse. Sometimes both are useful.

The risk factor can not be used directly for the evaluation of real security threats. It is only a coefficient in a more complex equation with unknown chances of a breach of security and losses from it. But the assumption of its proportional value to the security risk gives it a good comparative meaning.

Let in our example postulate that the company has a security budget of 3A, or that it can afford to assign the secret clearance only to three employees: GM, AG and OP. The security risk factors will be:

$$\mathbf{CRF}_{av} = (3+3+4+5+6+6+0+0+0)/11/9 = 27/99.$$
$$\mathbf{CRF}_{max} = 6/11$$

If we increase the security spend to 4A (33% increase, one more person classified as S), then the CRF_{av} will drop to 21/99 (22% decrease), but CRF_{max} would not change. It is worth to think whether to increase the security spend or not in this situation. Thus, the main benefit of the CRF is the possibility to use it for comparing different assignments of security clearances.

Though the two class model is too simplistic, nevertheless it shows the main problem of a security system design. The problem is that practically no organisation can afford a security system with a zero risk factor, and it is forced to look for a suitable trade-off between the cost and the risk factor

We shall show that introduction of intermediate classes helps in security improvement without cost increases.

Let we introduce an intermediate clearance *confidential* (set C). We shall assume that the security procedures designed for this clearance eliminate the risk of data leakage for all employees with SCV_i no more than 4. Let the cost of these procedures be B = A/3, and the security budget as before is 3A. The possible variant of assigning clearances to employees is shown in Figure 3.

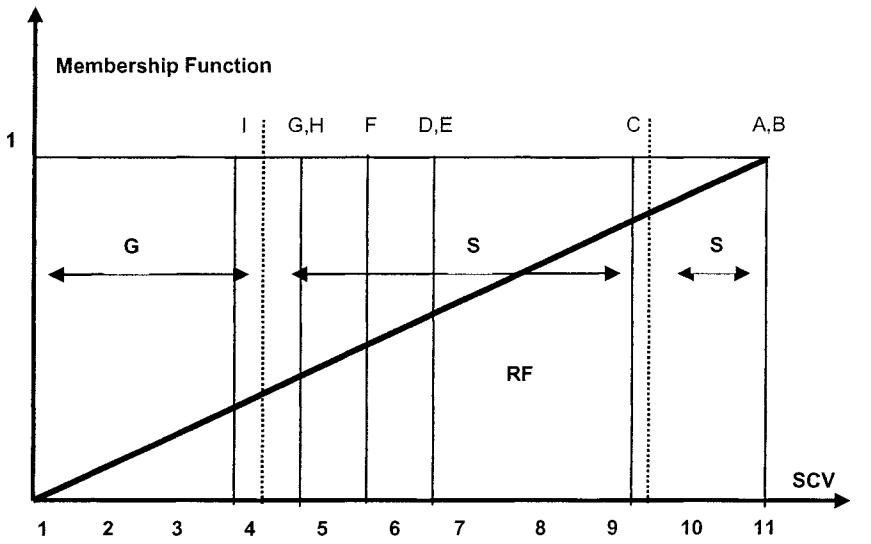

Figure 3. Risk function and its cover by 3 classes G, C and S

In this variant we sacrifice the clearance S for the Operations Manager (OP), changing it to C, which incurs a security risk factor of (9 – 4)/11. It allows the provision, within the limits of our budget, two more employees with higher risk factors, PUN and ANM, with the same clearance C. This will decrease their risk factors by 4/11 each. The security risk factors will be:

$$\mathbf{CRF_{av} = (3+3+4+5+2+2+5+0+0)/11/9 = 24/99.}$$
$$\mathbf{CRF_{max} = 5/11.}$$

This shows a significant improvement in security estimates.

The next step will be to sacrifice the S clearance of either GM or AG and to provide C clearances for him/her and additional two employees with higher risk factors. This will leave only 2 persons in the G class; 6 persons will be in the C class, 2 of them having a non-zero risk factor. The security risk factors for this distribution show the following improvement:

$$\mathbf{CRF_{av} = (3+3+0+1+2+2+5+6+0)/11/9 = 22/99.}$$
$$\mathbf{CRF_{max} = 6/11.}$$

The first criterion has decreased, but the second shows an increase. We can choose either the previous variant of clearances distribution if we prefer the second criterion, or to go further on if we prefer the first one. Then the final logical step is to use the budget for assigning all employees a uniform clearance C. In our case this does not show further improvement. Generally, an analysis of both company risk factor functions CRF_{av} and CRF_{max} show the best way for their optimisation, but this analysis is outside the scope of this paper.

4. SECURITY MODELLING FOR DATABASES WITH NETWORK DATA STRUCTURES

In any of these cases some important problems were not addressed, which is commonly referred to as the "jigsaw puzzle" intelligence. A watchful analysis of the officially collected materials allows to obtain 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 are logically connected. Knowledge of that connection algorithm allows one to reconstruct a relatively accurate model of the reality with the use of only few components.

The main argument presented in this paper is that individual clearances should not be based on the position of an individual 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 for the case when the security categories are 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 organizational level and no overlapping of data (i.e. any data unit is known to only one person on a given organizational level) would produce security clearances directly adequate to the position of the person with respect to this level. Otherwise, with real-life trees, the differences were dramatic. The specific features of the models are as follows.

- The set of key indicators (which need to be protected).
- 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. However, because all indicators are formed from elementary data feedback, the general structure of the data flow in the company will be a network.
- An algorithm that assigns Confidentiality Parameter (CP) to every element works for every DAS sequentially, matching it against data network also sequentially.

An experimental implementation in a company showed the following results.

Before implementation of the model described above, the company had three security categories: "Secret", "Confidential" and "Internal use" defined in Table 2.

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 organizational framework.

Table 2. Structure of the security clearances

Security level	**Associated security clearance**
Secret	General manager
Confidential	Level 2 management
Internal use	Level 3 management

After the introduction of the algorithm calculating the real security clearance values, and the proper definition of security clearances, the structure of security clearances changed (Table 3, last column). 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.

Table 3. List of individual security clearances

Level	Position name	Initial clearance	Calculated 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

5. CONCLUSION

The main results of this paper may be summarized as follows:

1. For the full and complete implementation of the 'need-to-know' principle we introduced data access statements (DAS) as part of employee's work description. Thus the access to the information is granted to every employee on the data element level as opposed to the existing practice of granting access on a domain level.
2. We suggest changing the existing practice of assigning security categories to data base domains, and to assign instead a confidentiality parameter (CP) to every element of the data base. The data base will be characterized from the confidentiality point of view in more detail.

3. We showed that current crisp models of assigning security clearances do not include cost and efficiency optimization. Instead we developed optimization models, based on fuzzy sets theory.
4. As a measure of efficiency of the security system we introduced the company risk factor (CRF), which makes possible to compare different ways of security organization under a limited budget.
5. Most of information processed and stored in a database is related to each other. These relationships may allow calculation or estimation of, sometimes quite confidential, information. Knowledge of these relationships therefore might influence significantly content of security labels attached to objects and subjects. We addressed this problem under assumption that the database has a network structure.

Further research in this direction might include the development of optimization models, based on analysis of both company risk factor functions CRF_{av} and CRF_{max} and the structure of the set of feasible solutions. Another direction of research includes the development of models optimizing costs of the security system under risk constraints.

REFERENCES

Amoroso, E., (1994), Fundamentals of Computer Security Technology, Prentice Hall, USA.

Frank, L., (1992), EDP-Security, Elsevier Science Publishers, The Netherlands.

Pfleeger, C., (1997), Security in Computing, Prentice Hall, USA.

Portougal, V., Janczewski, L., (1998), Industrial Information-weight Security Models, Information Management & Computer Security, Vol. 6. No 5, Great Britain.

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

Schuler R. et all, (1992), Human Resource Management in Australia, Harper Educational, Australia.