Managing Security Clearances within Government Institutions

Lech Janczewski
The University of Auckland, New Zealand

Victor Portougal
The University of Auckland, New Zealand

INTRODUCTION

An Internet search (Google) on government + security clearances + policy indicates that at present, establishment of individual security clearances within the government departments (and within U.S. State Departments in particular) are based on two factors:

- Evaluation of the candidate past
- Need to know policy

Evaluation of the candidates past (done very often with the polygraph use) is aimed at establishing past activities of that person. Special emphasis is placed on finding possible contacts with organizations/countries hostile to the evaluating agency. For instance, all CIA agents must periodically undergo such tests (Mahle, 2005). The results would determine possible range of security clearances of an individual.

The *Need only policy* (discussed later in the article) is further used to adjust security clearances of individuals. We (the authors) we unable to find practical realization of the *Need to know* policy and the presented research is an attempt to cover this gap.

Managing information security depends on business environment, people, information technology, management styles—to list the most important. Within this domain, the following seem to be recognised as routine procedures:

- **Development of a Strategic Plan to Protect Information Resources of the Business Organisation:** Despite the existence of enough evidence indicating constantly increasing number of security violations and resulting losses, the majority of business organisations failed to develop their security managing strategic plans. Fifty percent of them do not have even a disaster recovery plan (Jordan, 1999). Without such a plan, any effort to tighten up security of information within the organisation is a non-effective procedure
- **Development of Information Security Policy (ISP):** ISP is a document that outlines the main checkpoints that are directed specifically at an individual organisation's operations (Forcht, 1994). ISP could be a page or many pages depending on the level of details of the checkpoint procedures (Leung, 1998).
- **Classification of Security Levels, Security Clearances, and Security Labels:** This is the domain of the security models, starting from classic Bell-La Padula, Biba and USA Department of Defence Orange Book models. Security levels deal with the classification of information in terms of its accessibility. Security clearances determine the rights of persons/program to access the data. Security label is a mechanism to match security levels and security clearances
- **Development of Reference Monitor:** Virtually every security policy can be modelled in terms of subjects (people and programs) accessing objects (information either in electronic form or hard documents). This view of security policy implies that some decision procedure should exist to decide which requested accesses should be allowed and which should not. It acts as a filter through which all access requests made by subjects must pass. The term "access" means rights to read a document only, or to change it, or even destroy. This type of filter has come to be known as a Reference Monitor. (Amoroso, 1994). There are numerous publications presenting research in the field (e.g., Janczewski & Low, 1998). The research concentrates mainly on the issue of how to build and run a reference monitor
- **Technical Issues Related to the Development of a Security Kernel:** The reference monitor manages the controlled access to particular information but there are numerous technical issues related to the development, implementation and running of a sys-

Figure 1. Taxonomy of assigning security clearances methods

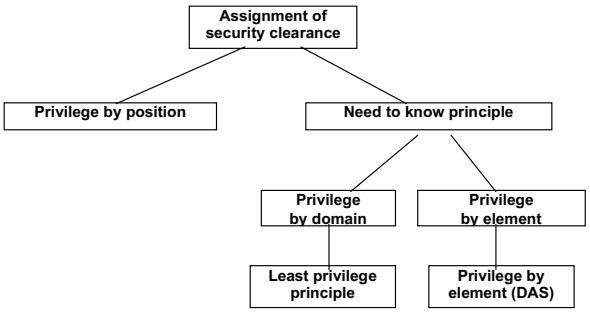
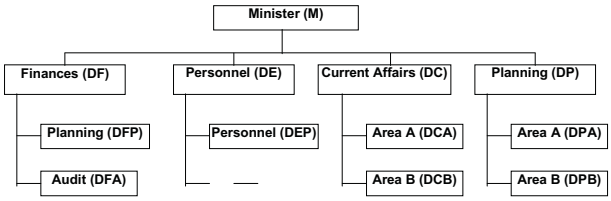


Figure 2. Organisational structure of the department



Note: Abbreviations (in brackets) will be used later in the text to denote the positions

tem in a secure way. "Secure way" means that information is protected against unauthorised access or change, and is available on request.

An analysis of the previous chain of security arrangements shows a significant weak point. It is the procedure of assigning security clearances to an individual. 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 a person is within the company hierarchy the higher security clearance he or she must have." This approach clearly incurs significant problems. In the one extreme a person might have a security clearance that is too high for his or her job, which increases the total cost of the security system. Higher security clearance incur higher cost (for instance of security training). On the opposite side a person with a security clearance too low for his or her job must obtain temporary authority for accessing specific documents. This could be costly as well, time consuming and it could decrease the efficiency of operations. Portougal and Janczewski (1998) demonstrated in detail the consequences of the described approach in complex hierarchical structures.

A competing and more logical idea is to apply the "need to know" principle. Under this principle, everybody has access only to the information needed to perform direct duties. 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, p. 298-299) describes the "principle of least privilege." The recommended application is based on subdividing the information system into certain data domains containing secret or confidential information of similar types. 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. 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.