A Security Model For A Defence-Related Organization

Chiew Pheng Goh

A dissertation submitted in partial fulfilment of the requirements for the degree of Master of Science in Computer Science in the University of Wales.

Supervisor: Professor M F Bott

University of Wales, Aberystwyth
30 November 2003

DECLARATIONS

The content of this dissertation is the result of my own independent work and investigation except otherwise stated. All sources are acknowledged by explicit references to the bibliography.

Signed: .....(Chiew Pheng Goh)
Date: .....

I declare that this work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed: .....(Chiew Pheng Goh)
Date: .....

I hereby give consent to the dissertation, if successful, to be available for photocopying and for inter-library loan, and for the title and summary to be made available to outside organizations.

Signed: .....(Chiew Pheng Goh)
Date: .....

Acknowledgements

I am grateful to my supervisor, Professor M F Bott, for his invaluable help, guidance and support during the time I have spent working on this dissertation. His patience and kind consideration shown during the course of my work is deeply appreciated. I am also thankful to him for introducing me to the intriguing field of IT security and believing that I could pursue the topic worthwhile of a dissertation. I would also like to acknowledge the incredible support I received from my family, especially my husband, without which I could not have completed this work. Last but not least, I thank God for giving me the strength and inspiration whenever I need fresh insights and encouragement to go on.

Abstract

Modern computer systems of a defence-related organization are vulnerable to a myriad of digital threats. The organization needs to have a security model(s) that is/are able to handle the variety of infosecurity needs that arise from the threats. Three security models are studied for their capabilities in handling the threats of a typical defence-related organization. They are the Bell LaPadula model, the Biba model and the Domain Based Security approach. The models are also compared and contrasted for their ability in meeting the infosecurity needs of the organization. Domain Based Security is eventually selected as for its practicality and ability to meet most of the infosecurity needs of a defence-related organization.

Contents

Chapter 1: Background and Introduction

1.1 The Need for Security in the Networked World

As the world becomes more electronically connected and integrated, systems running on networked computers become more vulnerable to digital threats and this has posed a serious challenge for information security. In this dissertation, we are interested in the threats that a typical department charged with the development and advancement of the science and technology relating to defence for a small and developed nation would face. It is the main business of such an agency to provide leading edge technological solutions to its military customers for the defence and security needs of the nation. To have a formidable fighting force, it is important that the IT systems of such an agency are adequately protected from attacks that could undermine the MoD's own operational capabilities. Damage resulting from assaults to IT systems (including databases) and acts of sabotage could result in irreparable damage to the nations' defence efforts. It is therefore important that there is a security model that addresses the needs of this agency. From this security model, appropriate processes and measures can be identified and put in place to ensure the integrity, availability and security of the IT systems at all times.

1.2 Digital Threats to IT Systems of Military / Defence-Related Organization:

There could be many types of adversaries that IT systems belonging to a military / defence related organizations have. Many such organizations have their own internet websites and often the web servers are connected to their corporate networks. With the rising cyber crime rate, corporate networks constantly face digital threats such as spamming, infection with malicious codes and Trojan Horses, and hacking. ".gov" and ".mil" domains are often the prime targets hackers like to explore.
The following subsections describe the different types of threat [1, 2] to which all systems are subject and discuss the implications of these in the context of a defence-related science and technology agency.

1.2.1 Unauthorized access

This is the most basic security threat. Someone gets information from the system that they are not entitled to have and which the owners of the system wish to keep private.
In the context of a defence-related science and technology agency, there is much information that must be kept private. Such information might include, for example,

- performance figures relating to a new weapons system;
- the location of weapons stores;
- contingency plans for dealing with attacks.

In the more general military field, operational plans and communications might also be the subject of unauthorized access.
The threat of unauthorized access comes principally from potentially hostile nations. However, journalists often seek information of this type and there is also the risk of unauthorized access by hackers who do it for enjoyment.

1.2.2 Malicious damage

That is, making changes to the system, or destroying parts of it, so as to prevent it from functioning correctly.
For most defence-related science and technology organizations, there are a lot of information about research and development work done for the military customers kept in the IT system. Any unauthorized changes made or destruction caused to the system could cause the loss of critical information, for example,

- maintenance and repair manuals (and maybe even operation manuals) of military peacetime and operational systems;
- technical architecture of peacetime and military systems (this would include various specification documents such as requirement specifications and technical specifications, and source codes);
- business architecture that describes the processes during peacetime and war;
- network architecture of military systems;
- work and findings of ongoing and past research of proposed capabilities prior to actual development of systems.

The threat of malicious damage comes from various sources. Info warriors working for the interest of potentially hostile nations who would seek to wreak havoc on IT infrastructure of its target. Some hackers may like the challenge of pitting their hacking skills against the security might of military or its related organizations. There are, of course the script-kiddies, who would do it simply out of boredom and fun.

1.2.3 Impersonation

Impersonation is falsely taking on the identity of an authorized and authentic user to gain unauthorized use of IT systems.
In a military-related organization there are much classified information or discussion being exchanged within different parts of the systems. Unauthorized access through impersonating a legal identity could seriously breach the sensitivity of the classified information. For example, this could happen by

- impersonating a user to gain access into restricted parts of the systems such as a private discussion forum where his communication partner can be easily induced to disclose sensitive information.

Impersonators could come external and internal to the organization. External impersonators include spies from potentially hostile nations, and journalists seeking news worthy pieces of classified information. Internal impersonators include inquisitive staff who work out of their "need-to-know" boundary.

1.2.4 Denial of service

The idea of denial-of-service attacks is simply to flood the targeted computer system with so much stuff that it stops working. This is mainly to deny the legitimate users the use of services from the system.
Although the internal computer network of military-related organizations are normally very much shielded from the internet, they are still vulnerable to denial-of-service attacks. For example,

- an internal staff store information that contains malicious code in the intranet and the malicious code triggers a denial-of-service attack.

During peacetime, the threat comes mainly from unsuspecting staff who unwittingly downloaded information from the internet which contains malicious code, a disgruntled employee with ill intent who introduced the malicious code deliberately into the network, or even a mischievous or bored employee who just wants to have some fun when he introduced the malicious code into the network.

1.3 Infosecurity Needs for a Defence-Related Organization:

In a defence science and technology agency, there are three security classifications for sensitive information: Top Secret, Secret and Confidential. Access is granted only on a need-to-know basis to authorized users. It is important that IT systems, including databases, that hold these information have robust security measures put in place to enforce the information security policies of the organization effectively to ensure not only the confidentiality of information, but also the integrity and availability of information, so that the information is what it is intended to be and it would be available anytime an authorized user requests for it to

fulfill a legitimate business objective. It is also important that the management system of access control for sensitive information works effectively to deter and block unpermitted access to these information. In summary, the infosecurity needs for a defence-related organization include multilevel security, information confidentiality, information integrity, authentication and information availability.

1.4 Defining the Business Environment of a Defence-Related Organization:

For a defence science and technology agency which serves the armed forces of a small nation presumably surrounded by potentially hostile countries, it is important that it provides advanced knowledge and technology that are relevant and up-to-date for that competitive edge over its adversaries that not only effectively deters possible invasions, but provides the combat defence capability to defend and defeat when necessary. The defence-related organization does not itself handle operational information, although part of its remit is to give advice to the armed forces on the security of their operational information. This organization would place a great prerogative on acquiring knowledge and technology through research, development and acquisition that would deliver formidable operational capabilities for its customers. In fact, there would be a lot of information generated in the work units of this organization that is highly classified. The people in this organization are segregated according to their job functions and domains. For example, the people dealing with human resource and the planning and development of command and control systems would be placed in two different departments. Within the department, there could be further separation of duties according to the area of work. Using the example of the people in the department planning and developing C2 systems, they could be further segregated into army, navy and airforce. Although their area of work might separate the people and thus the systems they are working from, there sometimes exist the need to share information to reduce repetition or duplication of work to the minimum level. Relating to the need to minimize the repetition of work (as given above) between different groups of people with the organization, it is important to promote inter-departmental cooperation for projects to bring in the right expertise at the right time serving the needs of a common client. This would also minimize the duplication of job functions and contribute to the building of a trim organization. Since there is a need for different groups of people, possibly coming from different departments or domains to work together and share information, it is necessary to have a framework or guidelines to govern the sharing of classified information amongst the appropriate people so that they may work synergistically and use the knowledge in developing capabilities that are useful to its customers without compromising information security.

There also needs to have knowledge management so that knowledge is not lost upon the closure of project works, or subject to the inclination of employees to share. The point is that if someone is authorized to find out about certain information, he or she should not be prevented to do so simply because the knowledge bearer guards the information for egoistic reasons.

A high level of security awareness and strict adherence of security measures are necessary in a defence-related organization. Security awareness seminars are held regularly to educate all employees on the extreme importance placed on the protection of the confidentiality of classified information. During the seminar, employees are told never to leave printed classified documents lying around, but to lock them up properly in assigned cabinets. Password protected screen-savers (meaning an entry of password is required for the system to come out of screen-saver mode) should be activated, or else they should log out of the computer system before they leave their workstations. Employees are also reminded to be vigilant of espionage. It is emphasized many times that classified information should only be disclosed to authorized personnel (personnel who have sufficient security clearance) on a need-to-know basis.

Sometimes there might be a need to link up the systems to trusted vendors who may be involved in the development and or maintenance of systems for the organization. It would be

inconvenient if employees cannot log on to the internet at their work place to find information that might be relevant to their work. There might also be times when employees need to communicate with peers from other defence-related organizations of friendly nations to exchange ideas and share information. The internet is also necessary to liaise with external vendors through their company websites or emails, and have them send attachments (for example of Request For Information documents) back.
Recently a lot of commercial companies have initiatives that envision a "paperless" work environment. The US DoD also has an initiative to go "paperless". The defence-related organization described in this thesis is no exception. This initiative serves not only an environmentally friendly purpose to cut down paper usage, it also aims to cut down the associated administrative and security management of printed classified documents. Organization-wide circulars or memorandums are no longer disseminated in a printed form, but are posted on the corporate intranet. Another example is the on-line application of leave through the corporate intranet instead of filling a printed form.

1.5 Scope of Dissertation

The main objective of this dissertation is to suggest an infosecurity model for the classified information held by a typical defence science and technology agency. In order to do this we shall need to survey existing infosecurity models and assess their usefulness. In this thesis, we shall be looking at three security models: the Bell-LaPadula model, the Biba model and the Domain-based Security model. We are concerned with infosecurity models rather than with their implementation. We shall not therefore describe how these models might be implemented, except to the extent that this affects their feasibility. In selecting each model for discussion, consideration was given to the following criteria:

- Ability to fulfill the infosecurity needs of a typical defence science and technology agency
- Ease of adopting or implementing the model
- Ease of understanding the intended capabilities of the models

The weaknesses and strengths of each model would be discussed. The aim is to find the most suitable security model for meeting the security needs of the computer systems of the defence-related organization that is described the previous section. Maybe a security model would not suffice and we might conclude that a composite of models might be more suitable. In summary, the most suitable model should be able to support the following characteristics of the business environment of the organization:

- Domain-based segregation of systems that sometimes need to "talk"
- Control of information flow to allow access to only authorized users on a need-to-know basis
- Access to the internet in the work environment
- "Paperless" work environment

Chapter 2: Bell LaPadula Model

2.1 Introduction

The Bell LaPadula (BLP) model [3] is sometimes known as military access control model or the multi-level model. It deals with the control of information flow and is used for enforcing access control in government and military applications. The model concentrates on the confidentiality aspect in that it states the properties required to prevent information leakage or unauthorized disclosure of information.

2.2 History of Bell LaPadula Model

D. E. Bell and L. J. La Padula first proposed the BLP model in a report titled "Secure Computer System: Unified Exposition and Multics Interpretation" in 1976. The report was for a project in which the United States Air Force, the MITRE Corporation and Honeywell worked cooperatively to develop a design for the Honeywell Multics computer system for the Air Force. For several years preceding the report, there had been ongoing efforts in secure computer system modelling by the Electronic Systems Division of the Air Force and MITRE. As a result of the effort, a mathematical framework and a model with refinements and extensions was produced which reflected a computer system architecture similar to that of Multics. There was a lot of work being done to produce a design for a secure Multics based on the mathematical model. The report summarized the particular version of the mathematical model that was relevant to the development of a Multics security kernel. The report explicitly related the model to the emerging Multics kernel design to help bridge the gap between the mathematical notions of the model and their counterparts in the Multics security kernel.
The BLP model has been the most influential model of security over the last 30 odd years. The policy in the BLP model and some of the elements of the model are embedded within the TCSEC (Trusted Computer System Evaluation Criteria) [4]. TCSEC or the Orange Book was written by the United States Department of Defence to describe the security and assurance requirements necessary for government and military systems. It was used for 17 years as the defacto standard for trusted systems. TCSEC was retired in 1999 in favour of a new criteria and methodology called the Common Criteria.

2.3 Anatomy of the Model

The BLP model supports both mandatory access control and discretionary access control. According to the TCSEC [4], mandatory access control is "a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (for example clearance) subjects to access information of such sensitivity". Discretionary access control is defined as "a means of restricting access to objects based on the identity of subject and / or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) to any other subject". The BLP model supports mandatory access control by determining the access rights from the security levels associated with subjects and objects. It supports discretionary access control by checking access rights from an access matrix. In addition to supporting arbitrary access specifications to the access matrix, the model groups protected objects according to different security labels and decides user privileges by their authorized security clearance levels. This is elaborated in the subsequent section after the definition of certain terms used in the model.

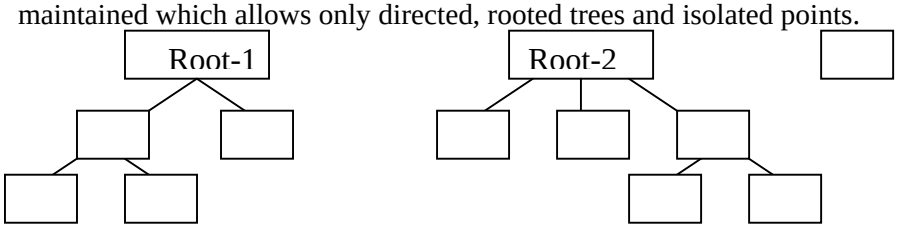
2.3.1 Definitions of Terms in Model:

- **Observation** of object is defined as the extraction of information from the object.
- **Alteration** of the object is defined as the insertion of information from the object.
- Four General Types of Access Attributes:
    - Execute, ***e***: no observation or alteration of object.

- Read, ***r***: observation with no alteration of object.
- Append, ***a***: alteration with no observation of object.
- Write, ***w***: both observation and alteration of object.

The above access attributes form the set **A** of access attributes in the model.

- Four Components of a System State:
  - Current access set, ***b***: current access set by a subject to an object is represented by a triple
    (subject, object, access-attribute).
  - Objects organized in a hierarchy, ***H***, where parent-child relation is maintained which allows only directed, rooted trees and isolated points.



  - Access permission matrix, ***M***.

Subjects	Objects		
		$\mathbf{O_i}$	
$\mathbf{S_i}$		$\mathbf{M_{ij}}$: **r**	

$\mathbf{M_{ij}}$ records the access modes in which subject $\mathbf{S_i}$ is allowed to object $\mathbf{O_j}$. Entries of **M** are subsets of the set of access attributes.

  - Level function, ***f***: represented as a triple of security level assignment functions.

    f = (level ($\mathbf{S_i}$), level ($\mathbf{O_j}$), current-level (**.**)),

    Where ***f*** = level function, level ($\mathbf{S_i}$) refers to the security level of subject and level ($\mathbf{O_j}$) refers to that of the object. The current-level (**.**) identifies the current security level of the subject. It allows a subject to operate at less than its maximum security level. The current security level makes feasible the requirement that high-level information not be put into low-level subjects. A security level of a subject or an object is represented by (classification, set of categories). In a military environment, people and documents are given a classification or clearance (Unclassified, Confidential, Secret, and Top Secret) and also a category of that usually designates the scope of work covered (e.g. Army, Chemical Warfare). In order for a user to access a classified document, it is necessary that his security level, level ($\mathbf{S_i}$), dominates the security level, level ($\mathbf{O_j}$).

    Dominance of $\mathbf{S_i}$: level ($\mathbf{S_i}$) level ($\mathbf{O_j}$)
    (classification of $\mathbf{S_i}$, Category of $\mathbf{S_i}$) (classification of $\mathbf{O_j}$, Category of $\mathbf{O_j}$)
    Classification of $\mathbf{S_i}$ is greater or equal to classification of $\mathbf{O_j}$ and category of $\mathbf{O_j}$ is a subset of the category of $\mathbf{S_i}$.
    A state of the BLP model is a 4-tuple of the form:
    (current access set, access permission matrix, level function, hierarchy)
    represented by the model notation (***b***, ***M***, ***f***, ***H***).

2.3.2 Security Properties to be Adhered:

1. Simple security property (ss – property) stipulates that if (subject, object, observe-attribute) is a current access, then level (subject) dominates level (object) where observe-attribute could be a write or a read access. The ss – property is not sufficient to protect the confidentiality of the information. This is because the expected interpretation of the model anticipates protection of information containers rather than that of the information. A malicious subject might pass classified information

along by putting it into an information container labelled at a lower level than the information itself. This leads to the need for the * - property.

2. * - property is satisfied if in any state, if a subject has simultaneous "observe" access to object-1 and "alter" access to object-2, then level (object-1) is dominated by level (object-2).
   Under this restrictive property:
   level(***a***-accessed-object) dominates level(***w***-accessed-object);
   level(***w***-accessed-object-1) equals level(***w***-accessed-object-2); and
   level(***w***-accessed-object) dominates level(***r***-accessed-object).
   To refine the definition of the * - property in terms of current-level (subject); we have:
   In any state, a current access (subject, object, attribute) implies:
   level (object) dominates current-level (subject) if attribute is ***a***;
   level (object) equals current-level (subject) if attribute is ***w***; and
   level (object) is dominated by current-level (object) if attribute is ***r***.
   Bell and LaPadula included two important comments for the * - property:
   1. It does not apply to trusted subjects.
   2. Both ss – property and * - property are to be enforced.

3. Discretionary security property (ds – property) is in fulfilment of the military / governmental policy of "need-to-know" information sharing. It is mandatory to have the enforcement of classification / clearance matching, and categories (formal need-to-know compartments). The restrictions make up the non-discretionary security policy and are embodied in the model as the ss – property and * - property. An individual must first fulfill the requirements stated in the non-discretionary security policy before anyone can extend discretionary access to classified information. The ds – property is a further restriction on top of the ss- property and * - property for access to information by a subject. Even if the subject has a high security clearance, it does not mean he can access all objects which are below its security level. This is because access requires an additional purposeful act by an authorized subject to extend the access based on need-to-know to certain categories or compartments of information. E.g. an official cleared to Secret level may be allowed access to information regarding Army chemical warfare but not Army biological warfare unless he is authorized to do so because his job requires him to know.

2.3.3 General Mechanisms of the Model:

Basic Security Theorem:
Adhering to the security properties described in the prior section should result in the basic security theorem.
The theorem states that security can be guaranteed systemically when each alteration to the current state does not itself cause a breach of security. Thus, whenever (subject, object, attribute) is added to the current access set ***b***, then:

1. level (subject) dominates level (object) if attribute involves observation to assure ss – property;
2. current-level (subject) and level (object) have an appropriate dominance relation to assure the * - property; and
3. attribute is contained in the (subject, object) component of the access permission matrix ***M*** to assure the ds – property.

All the three conditions stated above must be met in order for a subject to access the targeted object. The basic security theorem establishes the "inductive nature" of security in that the preservation of security from one state to the next guarantees total system security. Consequentially, by maintaining security in each state transition, security may be achieved for the system. Bell and LaPadula went on to describe a general framework for isolating single transitions of state. According to the framework, each class of requests is analysed separately

against a pre-defined rule designed to handle that particular class of requests. Adherence to the rule should result in the desired security properties being achieved, and the preservation of the security of the system. Rules, classes of requests and the system's response to each request are worked out for the whole system. The set of rules do not have overlapping responsibilities and satisfies all the three security properties by not introducing exceptions that violate the properties.
The rule framework breaks down a systemic security problem into smaller, more manageable contained rule-based problems to preserve security from one state transition to the next.

2.3.4 Four Classes of General Functions:

These are the four classes of general functions for changing the Elements of a System State in the Model:

1. Functions to alter current access (the set ***b***);
2. Functions to alter level functions (the values level (subject), level (object), and current-level (subject));
3. Functions to alter the current access permission structure (the matrix ***M***); and
4. Functions to alter the object structure (the hierarchy ***H***).

2.3.5 Operations for Making Changes to the System State:

1. Altering current access:
    - get access (add a triple (subject, object, attribute) to the current access set ***b***). This is used when a subject initiates access to an object like in the case of read, append and execute.
    - release access (to remove an access triple from the current access set ***b***). This is used when a subject gives up an initiated access.
2. Altering level functions:
    - Change object level (to change the value of level (object) for some object)
    - Change current level (to change the value of current-level (subject)). This allows a subject to change its security level (below an initial assigned value).
3. Altering access permission:
    - Give access permission (to add an attribute to some component of the access permission matrix ***M***). This is used when the controller of an object gives a particular access of that object to a subject.
    - Rescind access permission (to delete an attribute from some component of the access permission matrix ***M***). This is used when the creator of an object revokes a designated access of that object from a subject.
4. Altering the hierarchy:
    - Create an object (to attach an object to the current tree structure as a leaf). This allows a subject to activate an inactive object.
    - Delete a group of objects (to detach from the hierarchy an object and all other child objects "beneath" it in the hierarchy). This allows a subject to deactivate an active object.

Certain conditions need to be satisfied before the above operations can be performed. For example, a subject can exercise give and rescind rights to an object provided it has control attributes to that object. A subject can get access to an object provided its security level is equal or above the security level of the object, etc.

Further discussion of the BLP model is in Chapter 5 where its strengths and weaknesses are discussed and its suitability to be used in a typical defence-related organization assessed with the other security models.

Chapter 3: The Biba Model

3.1 Introduction

The Biba Model [5] is the first security model to address integrity in computer systems. It was proposed by Ken Biba of MITRE Corporation in 1975. In studying the two properties of the Bell-LaPadula model, Biba discovered a plausible notion of information integrity, which was the protection against unauthorized modification of information. He observed that a complete approach to information protection should be two-pronged: protection concerning the proper dissemination of information (confidentiality of information) and protection concerning information validity (integrity of information). The Bell-LaPadula model addresses the former effectively and is good in protecting against the compromise of unauthorized observation (dissemination) of information and thus maintaining the confidentiality of the information. In his paper, Biba put forth his idea that, for resource-sharing computer systems in a military environment, it is just as important to protect the integrity of information as it is important to protect the confidentiality of information. His primary concern was the protection of secure computer systems from intentionally malicious attacks: the unprivileged, intentionally malicious modification or sabotage.
To emphasize the importance of implementing integrity protection policies, Biba stressed that despite the apparent initial difficulty often encountered in programming arising from the restrictions imposed by the policies on the behaviour of the programs, the effort to overcome the difficulty is well worth it considering the significant value gained through effective access control. Moreover, the difficulty is transient and would pass once the protection policies become familiar to users.

3.2 Description of Biba Model

The Biba model is an integrity model that deals only with integrity. Subjects and objects in a secure application are assigned integrity levels (similar to the concept of security levels in the Bell-LaPadula model), and the access to modify is determined by comparing the integrity levels of the subjects and objects.

3.2.1 Definition of Terms in Model

- Integrity: a subsystem is considered to possess the property of integrity if it can be trusted to adhere to a well-defined code of behaviour.
- Integrity compartments: partitions imposed on sets of subjects and objects based on functional area. Examples of functional areas include logistics, simulation, real-time command and control and budget control.
- Direct sabotage of information: this kind of threat involves “direct” means where an unauthorized write into a protected database object occurs.
- Indirect sabotage of information: generally refers to improper modifications resulting from the use of data or procedures developed (modified) by a malicious subsystem. By not fulfilling expected requirements, this data or procedure may then sabotage its user’s functions.
- Basic elements in the model:
  - **S**: the set of subjects **s**, the active, information processing elements of a computing system.
  - **O**: the set of objects **o**, the passive information repository elements of a computing system.
  - **I**: the set of integrity levels, which Biba defined as a set of three integrity classes namely TOP SECRET, SECRET and CONFIDENTIAL.

    - TOP SECRET: information whose unauthorized modification could reasonably be expected to cause exceptionally grave damage to national security.
    - SECRET: information whose unauthorized modification could reasonably be expected to cause serious damage to national security.
    - CONFIDENTIAL: information whose unauthorized modification could reasonably be expected to cause damage to national security.
- **il**: **S** ∪ **O** → **I**. A function defining the integrity level of each subject and object; defines a lattice under the relation **leq**. An integrity level for a computer system element is composed of an integrity class and a set of integrity compartments. The integrity level gives an idea of the sensitivity to modification of information. The higher the integrity level, the more confidence one has that a program will execute correctly. The higher the integrity level of data, the more accurate and/ or reliable the data is. An integrity level is assigned on the basis of possible national security damage caused by information sabotage and for the purpose of preventing information sabotage.
- **leq**: a relation (subset of **I** x **I**) defining a partial ordering "less than or equal" on the set of integrity levels **I**.
- **less**: an antisymmetric, transitive relation (subset of **I** x **I**) defining the "less than" relationship on the set of integrity levels **I**.
- **min**: POWERSET (**I**) →, a function returning the greatest lower bound (meet) of the subset of **I** specified.
- **o**: a relation (subset of **S** x **O**) defining the capability of a subject, **s** ∈ **S**, to observe an object, **o** ∈ **O**. If (s,o) ∈ **o,** then s is able to observe o. Observation relates to the viewing of information by a subject. It is the testing of information that results in a choice of distinct states of the observing subject. The observing subject can make a choice based on the observed information, and that choice manifests itself in the resulting state of the observer.
- **m**: a relation (subset of **S** x **O**) defining the capability of a subject, **s** ∈ **S**, to modify an object, **o** ∈ **O**. If (s,o) ∈ m then s can modify o. Modification may be defined in terms of observation. A subject modifies information if its value is changed so that an observation, by a subject results in a different state than previous observations (a discernable change).
- **i**: a relation (subset of **S** x **S**) defining the capability of a subject, $s_1 \in \mathbf{S}$, to invoke another subject, $s_2 \in \mathbf{S}$: s_1 **i** s_2. This operation can be considered a prototype for inter-process communication and procedure call. Invocation is a logical request for service from one subject to another. It is a special case of modification.

3.2.2 Integrity Problems

It is in the light of the integrity problems to be tackled that integrity policies are devised. So far, there is no "one-size-fits-all" policy that can be used to solve more than the problem it is specifically designed to deal with. Three protection problems were identified in Biba's paper as being relevant to secure computer systems in a military environment. They are:

1) the integrity protection of information vital to national security;
    - The integrity of national security information is of utmost importance for the intended user community. The problem arises when this information has to be made available to many (who are at various different security levels) for observation and yet be allowed to be modified only by a few authorized users to prevent the corruption of critical information. An example given is that of a database defining interstate transportation routes. This information is useful to a large number of non-critical tasks, and yet the sound construction of the database is crucial to the proper operation of logistics programmes in times of national emergency. This information is marked for public dissemination in terms of its security level. This is obviously flawed in terms of protecting the integrity of the

information from the "contamination" or sabotage by users either intentionally or unintentionally. It is vital that only a selected few have "modify" access and these few are assessed to have high integrity level.

2) the integrity protection of information vital to the needs of a particular user; and
   - The owner or creator of a piece of protected information should be able to grant access of this information (for example, a database) to other users. However, when the access is misused, the owner or creator should have the ability to revoke the access. The protection mechanism must support dynamic revocation based on user identity.
3) the integrity protection of the security kernel.
   - A distinct class of protection problems arises from the use of system services. Users (subjects) may invoke service (system-supplied subjects) to perform privileged functions. These services must be protected from their invoker, so that they may not be modified maliciously or unintentionally and their behaviour towards the privileged functions altered. Likewise, the invoking subject also often requires protection from the invoked subject – the "mutually suspicious problem".

3.2.3 Integrity Policies

In his paper, Biba did not just propose one integrity model. In fact, he proposed a few access control policies aiming to provide effective integrity protection for the integrity problems mentioned in the previous sub-section. The most discussed aspects of the Biba model involve two of the integrity policies proposed in the paper. For the purpose of this dissertation, we shall describe these two policies and they are the Low-Water Mark Policy and the Strict Integrity Policy.

The Low-Water Mark Policy

In the low-water mark model the integrity level of a subject is dynamic. It is a function of its previous behaviour. The integrity level of the subject may change or downgrade with each observe access. The low-water mark is the least integrity level of the object accessed for observation by the subject. Note also that a subject can only modify objects whose integrity level is less than or equal to that of the subject. This policy consists of three axioms. (This is the term Biba used. The terms rules or properties are sometimes preferred since they are not strictly axioms in the mathematical sense.).

Three axioms of the Low-Water Mark Policy:

1. **il´(s) = min | il(s), il(o) |**
   The integrity level of **il´ (s)** of the immediate next observe access by a subject **s** is the minimum of the integrity level of its immediate prior access. The result is that **s** can only observe objects of decreasing integrity levels. Satisfaction of this rule insures the indirect sabotage by the use of "contaminated" data or procedure is not possible.
2. **$\forall$ s $\in$ S, o $\in$ O, s m o $\rightarrow$ il(o) leq il(s)**
   s which is an instance of **S**, may modify **o** which is an instance of **O**, if the integrity level of **o** is less than or equal to the integrity level of **s**. This means **s** must be trusted enough to make modification to **o**. Satisfaction of this rule makes sure that indirect malicious modification cannot occur.
3. **$\forall$ s_1, s_2 $\in$S, s_1 i s_2 $\rightarrow$ il(s_2) leq il(s_1)**
   s_1 and **s_2** are two instances of **S**, and **s_1** may invoke **s_2** if its integrity level is higher than or equal to that of **s_2**. Satisfaction of this rule makes sure that lower integrity subjects do not invoke higher integrity subjects, which may have access to higher integrity objects. Indirect damage to objects of higher integrity level is prevented this way.

The result of adhering to the low-water mark policy is that the path of information transfer for a subject starts from a high integrity level (not higher than its own initial integrity level) and progressively downgrades to the low integrity level (to the lowest integrity level of the object accessed by the subject).

Disadvantage of the low-water mark policy

The monotonically non-increasing subject integrity level makes generalized, domain independent programming difficult, because for a given subject, the set of modifiable objects and invocable subjects may keep decreasing with each observation of different objects. A subject might end up sabotaging its own processing when objects necessary for its function are no longer available for modification. This is a serious shortcoming since the only way to recover is to re-initialize the subject.

The Strict Integrity Policy

This policy consists of three axioms, two of which are analogous to the simple-security property and the *-property of the Bell-LaPadula model in that they prevent the direct and indirect sabotage of information.

Three axioms of the Strict Integrity Policy

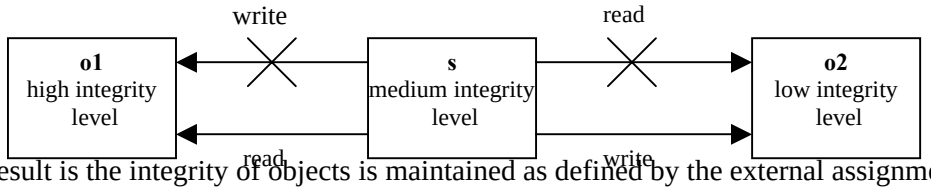
1. $\forall s \in S, o \in O \;\; s \; \underline{o} \; o \rightarrow \underline{il}(s) \; \underline{leq} \; \underline{il}(o)$

   s which is an instance of **S**, may observe **o** which is an instance of **O**, if its integrity level is lower than or equal to that of **o**. This axiom limits the use of data or procedures to those whose non-malicious nature (as indicated by their integrity level) the subject can be sure of. The subject accesses objects whose integrity level is higher than or equal to that of it.

2. $\forall s \in S, o \in O \;\; s \; \underline{m} \; o \rightarrow \underline{il}(o) \; \underline{leq} \; \underline{il}(s)$

   s which is an instance of **S**, may modify **o** which is an instance of **O** if its integrity level is higher than or equal to that of **o**. This axiom is commonly referred to as the si-property (simple-integrity property) of the Biba model, which in essence is "no read down". Satisfaction of this axiom insures that subjects possessing insufficient privilege may not directly modify objects. This is based on the assumption that the modifications made by an authorized subject are all at the explicit direction of a non-malicious program.

   When the above two axioms of the Strict Integrity Policy are adhered, this leads us to the well-known integrity-*-property of the Biba model. The integrity-*-property states that a subject **s** who has read access to an object **o1** may have modify access to an object **o2** if **$\underline{il}$(o2) $\underline{leq}$ il (o1)**. In essence this is "no write up".



   The result is the integrity of objects is maintained as defined by the external assignment of integrity level.

3. $\forall s_1, s_2 \in S \qquad s_1 \; \underline{i} \; s_2 \rightarrow \underline{il}(s_2) \; \underline{leq} \; \underline{il}(s_1)$

   s_1 and s_2 are two instances of **S**, and s_1 may invoke s_2 if its integrity level is higher than or equal to that of s_2. This axiom has the same effect as the third axiom described for the low-water mark policy.

The strict integrity policy is similar to the low-water mark policy in terms of capabilities. They do not allow subjects to modify objects whose integrity levels are higher than that of the subjects, and subjects of lower integrity level cannot invoke subjects of higher integrity level. They are different in the way they prevent indirect sabotage. In the low-water mark policy, the low-water mark changes the integrity level of a subject. This disallows the subject from viewing objects of high integrity level after it has accessed objects of low integrity level. In

the strict integrity policy, the strict integrity policy disallows subjects of high integrity level from observing objects of low integrity level.

Disadvantage of the strict integrity policy
For a given subject, many objects may be unobservable especially if it is a subject of high integrity level, because it can only observe objects of higher integrity levels than itself.

Further discussion of the Biba model is in Chapter 5 where its strengths and weaknesses are discussed and its suitability to be used in a typical defence-related organization assessed with the other security models.

Chapter 4: Domain Based Security

4.1 Introduction

Domain Based Security [6] is an approach to infosecurity that was developed by Defence Evaluation and Research Agency (DERA) for the United Kingdom Ministry of Defence. It is an approach that is designed to meet the demands of modern information systems that supports real business needs through the use of advanced information security technology with maximum use of COTS products as is possible after taking into account security requirements for the transfer of information. IT security is commonly viewed as a stumbling block for effective system operation, when it indeed can be an enabling technology that is vital for core business functions to operate effectively. This is because the confidentiality and integrity of information, and information assurance are frequently essential for effective business operations where decisions are made based on the information. Domain Based Security is an approach to IT security that was developed to meet the infosecurity needs arising from the increasing demand for wide dissemination of information using highly connected computer systems that can be configured in flexible and complex ways.
Domain Based Security is likened to a methodology that places a lot of emphasis on the thoughtful front-end security planning to bring about cost-effective implementation measures to fulfill the security needs of the business through the use of modelling and analysis techniques. The Domain Based Security approach covers all aspects of the development, operation, management and use of the information systems. The security related activities and documents that are required at different stages of a project are identified in order for the eventual successful accreditation of the information systems by security authorities for operational service.

4.2 Objective of Domain Based Security

The objective of the approach is to provide a means to accomplish the following:

- the definition of information security requirements which is done on the basis of the organizational policy for protection; the operational or business needs for sharing data; and the constraints of available technology;
- the fulfilment of the security requirements at reasonable cost in an operational system; and
- the demonstration that the requirements are met throughout the life of the system.

The approach recognizes that there are different levels of risks, and the levels of protection needed should be commensurate with the levels of risks, so that it does not hamper the way people carry out the business. In addition, the approach allows the maximum use of COTS product with the least likelihood of a compromise in information security. It is good to be able to use COTS products as this reduces the cost of development in terms of time, money and effort. If the product is established in the market, its functionalities, reliability and user-friendliness would be well known to potential users.
The Domain Based Security approach incorporates the use of models and analysis to work out the possible areas of compromise that might arise from two perspectives: the way the business is conducted; and the existing IT infrastructure that has been built to support the business. The models that are drawn up are not only useful in risk management, they can be also very useful in facilitating the discussion among users, developers and security analysts to promote mutual understanding and aid in the resolution of potentially conflicting concerns.

4.3 Infosec Models of Domain Based Security

4.3.1 Reasons for Infosec Models

It is important that the infosecurity properties of particular systems are clearly and precisely defined for a number of reasons [7]:

- to ensure that security requirements are compatible with business requirements and available technology;
- to support early, high level risk assessment;
- to provide a specification for design and development;
- to support accreditation, by providing a key link in the argument relating security objectives to implementation; and
- to support impact assessment when changes to operational systems are planned or become apparent.

The infosecurity properties of particular systems can be expressed effectively through the use of infosec models. The usefulness of the infosec models is not confined to the front-end planning stage of identifying security risks inherent in business processes and the IT infrastructure. They may be used for different purposes at different phases of a project:

- Scoping phase: Infosec Business Model helps to identify the scope of the security problems. Domain boundaries in the model show places where appropriate security measures are needed to manage the risks of an infosec breach.
- Appraisal phase: Infosec Architecture Models, which include the description of the security properties of their respective security options, are used to assess the feasibility of each option in handling the security risks, resulting in the early elimination of unviable ones.
- Provision phase: Security requirements described in the Infosec Architecture Model forms the basis of the design and development of the system, and the production of accreditation evidence.
- Maintenance phase: Models are updated to reflect any changes (such as changes in operating procedures, mode of use and operating environment) to support re-accreditation requirements of the system.

4.3.2 Types of Infosec Models

The infosec models represent two categories of information security risks:

- risks that arise directly from the way information is required to be shared in support of business objectives; and
- risks that arise from the implementation of services to support information sharing.

The former is addressed in an Infosec Business Model whereas the latter is addressed in an Infosec Infrastructure Model. The two categories of risks are combined in the Infosec Architecture Model. Modelling and analysing the way business is being carried out and the IT implementation helps greatly in the risk management where the various ways in which a compromise might occur are considered, and the most appropriate security measures to mitigate the risk selected.
The description of the three models proposed by the methodology, and the definition of some terms used in the models are given in the following sections.

4.3.3 Infosec Business Model (Domain Model)

The Infosec Business Model is used to express security requirements from a business point of view. It is worked out by looking at the core business processes and compartmentalizing these processes into appropriate logical domains. It uses the concept of a “domain” to describe the limits on the way in which people should be able to work together and share their data in fulfilling their business objectives. In the infosec business model, the sort of business data that needs to be shared amongst users, and how the data should be shared are specified. The model highlights how security requirements are influenced by business needs.

Definition of a Domain

A domain describes a logical place where a particular group of people use some shared IT facilities to assist them in the conduct of their business. A domain is represented by an oval in the infosec business model (Figure 1).

People who work in the same domain may share data with relative freedom, but limits are imposed on who are authorized to work in the domain, on what the data is handled there and on what tools and applications they are authorized to use. People who work in different domains may only share data in limited ways, which are clearly defined.

It is important that domains are defined to support the business. People who need to collaborate closely are put in the same domain. In this way, tight security constraints implemented around the boundaries of the domains have the least impact on the ability of users (who are within a domain) to conduct their business. Within a domain, less security constraint can be tolerated.

Definition of an Environment

An environment is a physical place where people work and where electronic media and equipment are located. An environment is represented by an oval with broken lines (Figure 1).

Definition of a Portal

A portal is a means by which domain members may interact with the computer system. It may be implemented by a workstation, operated by a monitor, keyboard and mouse, combined with a set of services that require users to prove their identity to the computer system before access is allowed to interact with application software in the domain. A portal is represented with an arrow (Figure 1).

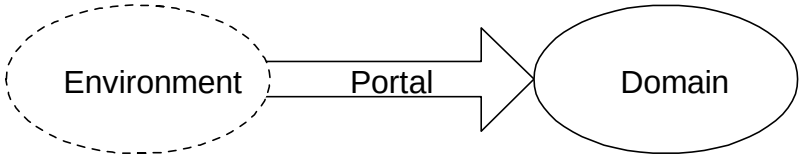


Figure 1: Notation for an environment, portal and a domain.

Definition of a Connection

A connection is a means by which data can be shared or transferred amongst members of different domains. The transfer of information represented by each connection may be unidirectional or bi-directional. When the connections between domains, and hence the transfer of information between domains, are explicitly identified, the security risks that are associated with each connection can be properly identified, assessed and managed.

The types of connections found in an infosec business model and their notations are:

i. Line between a pair of domains: an unspecified connection type.

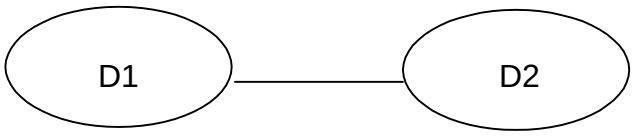


Figure 2: an unspecified connection between D1 (Domain 1) and D2 (Domain 2).

ii. Line with a “diode”: the transfer of business information is unidirectional; only transfer in the direction of the arrow in the diode is allowed.

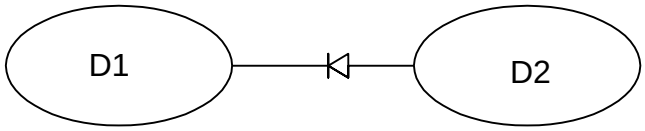


Figure 3: a diode is shown between D1 and D2 denoting a unidirectional data transfer from D2 to D1 only.

iii. Small square: a connection linking more than two domains.

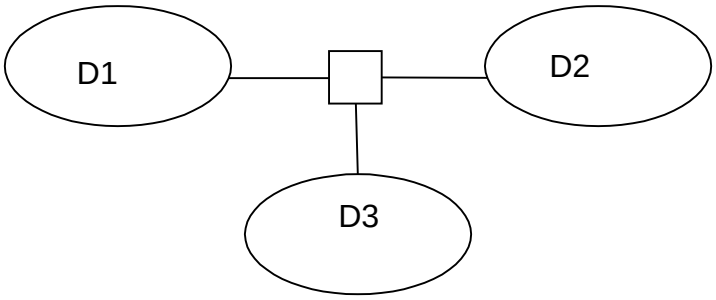


Figure 4: the small square is shown linking three domains D1, D2 and D3 together.

iv. Message connection: transfer of information from a member of a domain to a named member of another domain through the explicit action of the former sending the message.

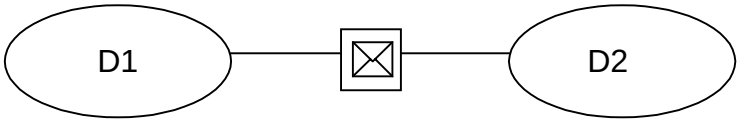


Figure 5: a message connection is shown between D1 and D2. Members of either domain may send messages to named members in the other domain.

v. Shared data repository connection: involves a person of a particular domain publishing data so that others can observe and possibly alter it.

   a. Filestore connection: a traditional means of data sharing which involves a hierarchy of files and file containers. The structure has the advantage of allowing tight control over the sharing of data. Note that there is a special type of filestore connection known as personal file share connection, which permits a member who belongs to more than one domain to transfer data from their “persona” in a domain to their own “persona” in another domain, but not to anyone else.

   b. Web connection: data is shared by publishing on a web server. The advantage is it allows more flexible structures to be created, with unlimited cross-references. The disadvantage is the control over the sharing of data is difficult to administer.

c. Database connection: data from an application specific database is shared to people who have access to the database. The advantage is database structures are well defined. The disadvantage is detailed security requirements must be tailored to the applications concerned.

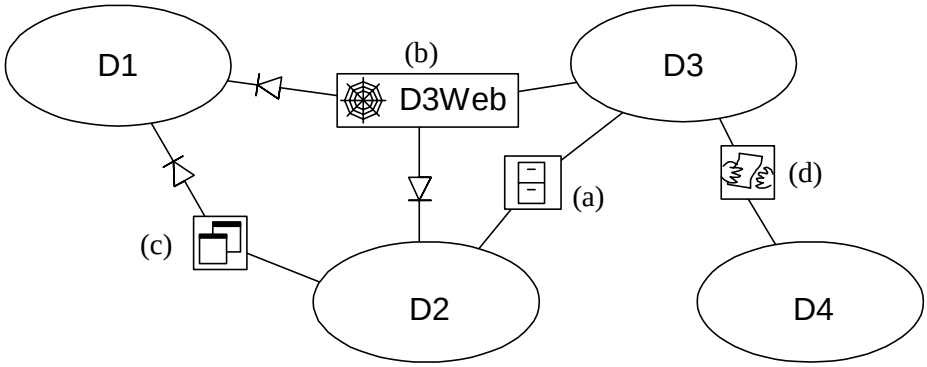


Figure 6: a simple model with the various shared data repository connection types.

(a) D2 and D3 share the file repository and members of the domains may share files in this repository.

(b) A member of D3 publishes data on the D3 web. Data from the D3 web may be transferred to D1 and D2, but not the other way round because of the data diodes.

(c) Both D1 and D2 use the database repository. D2 may transfer data into and out of the database. D1 may have data from the database transferred into its domain, but no data can be transferred out of its domain into the database.

(d) Some members of D3 who are also members of D4 may transfer data from their “persona” in one domain to their own “persona” in another domain, but not to anyone else.

vi. Conferencing connection: consists of a range of services that allow people to interact with each other in a real-time, conversational manner. This type of connection is very convenient but it is very difficult to control and limit the information exchanged. When control is necessary, strong security controls are placed outside the scope of the conversation itself. The types of conferencing connections are listed below:

(a) Video-conferencing connection

(b) White-boarding connection

(c) Telephone: only relevant where applications within an information system that handles sensitive information requiring protection are used to implement the connection. The conventional telephone systems between two physical environments are not included.

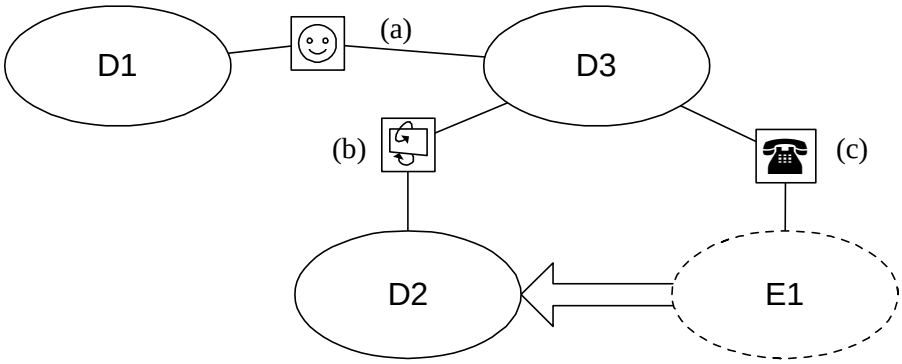


Figure 7: a simple model with the three types of conferencing connections.

(a) Members of D1 and D3 may interact real-time via video-conferencing connection.

(b) Members of D2 and D3 may interact real-time via the white-boarding connection.

(c) D3 has application(s) that is/are required to provide a telephone connection to people in E1 (Environment 1), and these people are members of D2 who can enter D2.

vii. Printing and static display connections: transfer of information for printing or for static display of images. File printing and fax are services included in this category of connection.

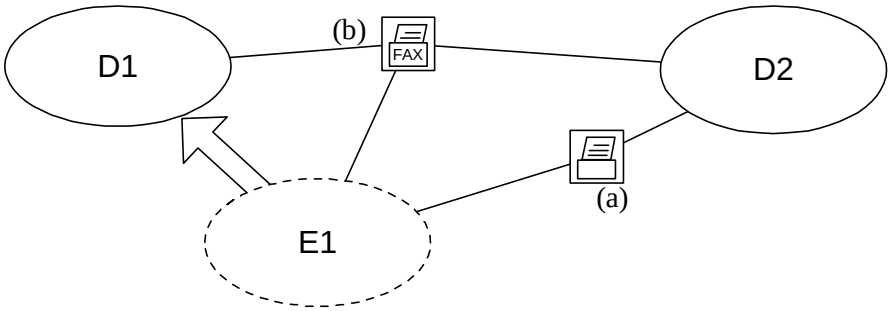


Figure 8: a simple model with printing and fax connections.

(a) D2 has application(s) that is/are required to provide the printing connection to people in E1, and these people are members of D1 who can enter D1.

(b) D1 and D2 have application(s) that is/are required to provide a fax connection to people in E1.

4.3.4 Infosec Infrastructure Model

The Infosec Infrastructure Model is important for it shows how the business model is implemented by IT infrastructure. When assessing the risks posed by the possibilities of compromises that occur because of certain undesirable or unwanted IT infrastructure implementation detail, it is important to place bounds on the assessment. This can be done by specifying an architectural requirement for impenetrable boundaries around certain elements of the business. The concept of “islands” and “causeways” are used in this model. “Islands” of infrastructure provide the impenetrable boundaries of a system and the “causeways” provide the sole means of transferring data between islands.

Definition of an Island
In isolation, an island is a computer system that is separated from all other computer systems by an “impenetrable” boundary. A boundary is regarded as “impenetrable”, if it is so strong that, for the purpose of a particular risk assessment, the people outside the boundary can be ignored. For any model, the strength of separation that is required for a boundary to be considered “impenetrable” must be stated. ” The island is represented by a rectangle with rounded corners in the model.
Definition of a Causeway
A “causeway” is defined as the only means by which exchange of information between islands (that are joined by the causeway) can occur. The flow of information between islands in terms of the nature and degree of information exchange can be closely regulated at the “entry” and “exit” of each causeway. The causeway may be represented by a small rectangle with rounded corners or the symbol of a diode if allows only unidirectional data transfer.

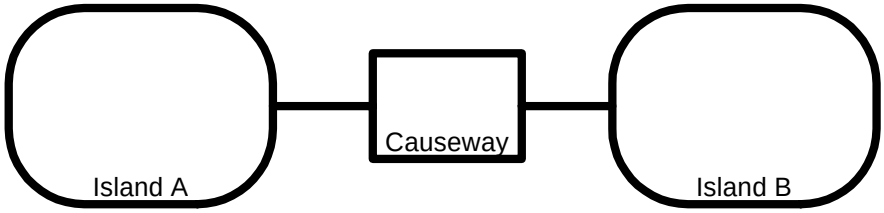


Figure 9: A simple infrastructure model that shows Island A and Island B joined by a causeway.

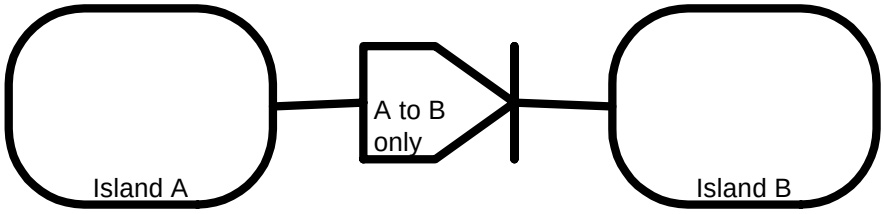


Figure 10: A simple infrastructure model that shows two islands joined by a one-way causeway. Data can only flow from Island A to Island B and not the other way round.

The Infosec Infrastructure Model is used to abstract the essential structure of systems that are required to implement the business requirements for connectivity. It highlights the points at which strong security controls can and must be provided to regulate information flow. Constraints such as the business requirements for security (and it is important that it does not hamper the way business is conducted) and the limits of available technology determine the positioning of the security controls. The Infosec Infrastructure Model forms the basis for analysing the risks arising from the implementation that are not inherent from the way business is conducted.

4.3.5 Infosec Architecture Model

The above two models are combined to give the Infosec Architecture Model (Figure 10). The Infosec Architecture Model represents the information security requirements of the systems at different levels of detail, and in a user-friendly form that can be easily understood by a wide range of people. The infosec requirements are based in the need to protect sensitive data and services, combined with the need to share data in pursuit of operational or business objectives. This model also puts down the consideration of the constraints imposed by legacy systems and the available technology (including the limits on technical feasibility) in meeting security requirements. With the business model superimposed on the infrastructure model, islands implement the domains. When more than one domain is found on the same island, the island implements the connections joining the domains. Through the combination of the models, the Infosec Architecture Model enables the description of all the different means by

which data may be compromised. This includes compromises that arise from the exploitation of the required business connections and implementation flaws.

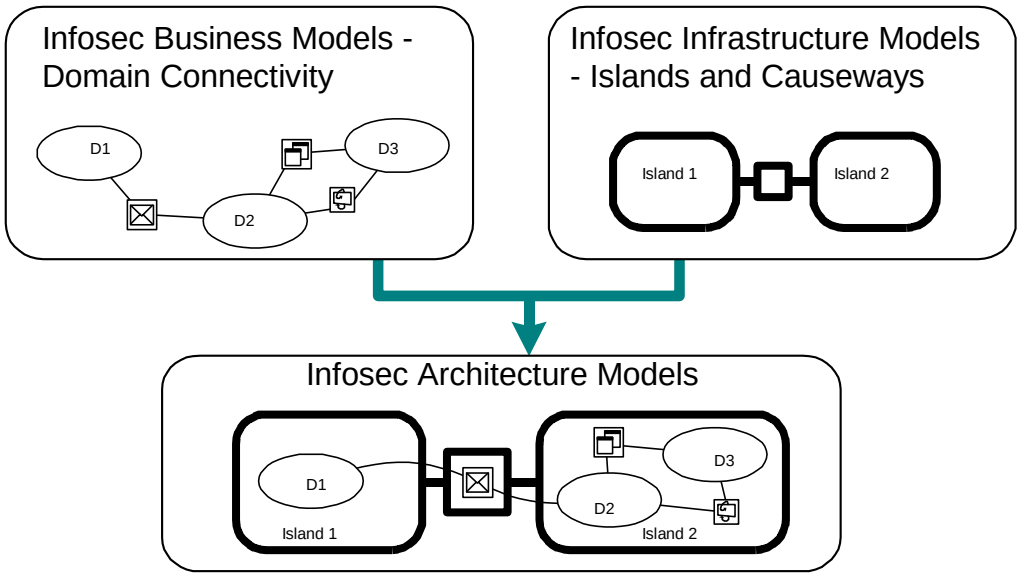


Figure 11: The Infosec Business Model is superimposed on the Infosec Infrastructure Model to give the Infosec Architecture Model.

Further discussion of the Domain Based Security is in Chapter 5 where its strengths and weaknesses are discussed and its suitability to be used in a typical defence-related organization assessed with the other security models.

Chapter 5: Strengths and Weaknesses of the Models

5.1 Introduction

All the three security models described were developed to address valid infosecurity concerns for the computer systems of a military-based organization. This chapter discusses the strengths and weaknesses of the models. At the end of the chapter, the models are gauged for their suitability to be used in a defence-related organization.

5.2 Strengths of the Models:

5.2.1 Bell LaPadula Model (BLP model):

This is the best-known example of a security policy model. It was formulated in the context of classification of the military and intelligence data, and it was proposed by Bell and LaPadula in response to the United States Air Force's concerns over the security of time-sharing mainframe systems [2]. The concern over the vulnerability of military operational systems to attacks by people using malicious and buggy codes such as Trojan Horses was also growing. The *-property was a critical innovation in the model which could effectively protect the computer systems from attacks that could cause information leakage.
When it was first described, the BLP model created some excitement because it was a relatively straightforward security policy that could verify claims mathematically about the protection provided by a design [2]. Although it was clear to the intuitive understanding, it allows people to prove theorems. From the simple security property and the *-property, various results can be proved about the machine states that can be reached from a given initial state, and this simplifies formal analysis. Despite its strengths, the model was a failure in leading to the development of useful and cost-effective systems, though the theory has had lasting effects on system design [1].

5.2.2 Biba Model:

The Biba model was the first formal model of integrity. It deals with the integrity considerations for secure computer systems [5], which the BLP model totally ignores. Information integrity is an important issue in computer security and if ignored could lead to highly undesirable consequences. An example that illustrates this point is the importance of ensuring information integrity in the drug dosage database in a hospital [1]. If the information is not protected from modifications (including malicious and accidental types), this could lead to patient(s) being given the wrong dosage that could be life threatening. Another example relevant to a defence-related organization is the database that stores performance figures of weapons. It is important that these figures are not modified or falsified because these are information that are important to tactical decisions that are made which involves life-and-death matters.
In a digital age where a lot of information is stored in the computer systems, and sometimes with no backup of hard copies, ensuring the integrity of the information is very important. Without appropriate security measures, the authenticity of digitised information can be difficult to discern, since it is easier to falsify or modify data without being detected easily. With the trend of many organizations taking up the initiative of creating a "paperless" work environment, information integrity as addressed by the Biba model is a valid security concern, especially for a defence-related organization that is vulnerable to attacks from its adversaries in order to undermine its operational readiness and effectiveness.

5.2.3 Domain Based Security:

The first strength of the Domain Based Security approach [8] is that it enables the organization to assess the risks and define its priorities for security. Infosec Business models, Infosec Infrastructure Models and Infosec Architecture Models are produced to aid in the

systematic identification of infosecurity risks from the way business is carried out and the IT infrastructure. Through the approach, security solutions that are proposed can commensurate with the risks confronting the information assets. This can help keep the cost of acquisition down.
The approach is commendable for striving to meet real needs and optimising the use of advanced appropriate security technology in a cost-effective way. Effort is put in to understand the business processes, and not having the security analysts jumping into conclusion the security measures the organization needs. The focus when searching for security solutions is on fulfilling security objectives which reflect an operational necessity. Appropriate security solutions are put in places where necessary, while offering minimal disruption of the conduct of necessary business activity. The approach takes into serious consideration the need for security solutions to complement or enhance, and not to hamper the way users conduct their business. This is because ignoring this need would most likely result in users bypassing the security measures and thus defeating the purpose and effort of implementing the security measures. The proposed security measures are implemented after considerable effort in the planning and discussion with stakeholders, instead of the haphazard assembling of the most trendy, or the most attractively marketed security technologies or products at the time of acquisition, some of which might not even be suitable to the infosecurity needs of the organization.
The Domain Based Security is a comprehensive approach that provides the methods and tools for the organization to create its own infosecurity strategy, especially to tackle the threats of the "application level" attack kind. It is entirely generic, independent of any particular security product and the concept of protection offered by the approach is fairly easy to understand. Being easy to understand is an advantage when promoting the approach to the executive management and even the rest of the staff for adoption in the organization.
In the Domain Based Security, domains and islands are used to segregate different groups of users in the organization. The groups may differ in terms of the nature of their work (for example, Weapon Acquisition and Research for the Airforce Department, Biological Weapon Research and Development Department, and Human Resource Department), or they may differ in terms of security classification. The concept can be used to satisfy the need for multilevel security in a defence-related organization. For example, if there is no requirement to do business with people except those that can be completed trusted, the conduct of this business can be isolated from the rest of the world using domains and islands effected through a combination of physical separation and cryptography.

5.3 Weaknesses of the Models:

5.3.1 Bell LaPadula Model:

John McLean raised one of the first criticisms on the BLP model. In 1987, he wrote a paper that discussed a contradiction of the Basic Security Theory: the "System Z" [9, 10]. "System Z" is like a BLP system that a user can ask the system administrator to temporarily declassify any file from high to low level, hence allowing users from low security levels to access or read high security files without violating the rules of BLP model [2]. McLean noted that no adequate definition of access security could be based entirely on the notion of a secure state. In response to this criticism, a tranquillity principle was introduced into the model to counter the contradiction raised by "System Z". The strong tranquillity principle states that security labels do not change during system operation, while the weak tranquillity principle states that the security labels do not change in such a way as to violate a defined security policy. However, the problem with the tranquillity principle is that a lot of software needs to be re-written or modified to run on multilevel platform, and this is one of the serious complexities of multilevel security.
McLean brought up another weakness of the model: the model has little to say about systems in which users may change security levels of themselves or their files [9]. These changes are often necessary in real-world systems. The strong tranquillity principle of the BLP model

does not allow changes in the security levels and access rights. The weak tranquillity property allows changes, but subject to adherence of the other two properties of the model, such that classified information can only flow from low security level to high security level with the security labels being upgraded appropriately when it happens. This lead to the following problems [11]:

i. According to the *-property (no write-down), an authorized subject accessing a piece of information at a high level of security classification cannot pass the same piece of information to objects at low level of security classification. In the real world, this is very restrictive and impractical if subjects with access to highly classified objects may never pass information to lower level objects to fulfil legitimate business objectives. Bell and LaPadula then introduced the concept of trusted subjects, who are not constrained by the *-property and are trusted not to consummate an information flow transfer resulting in a security breach, even though it is possible for them to do so [10].
ii. The *-property may be too simple to be practical. In an example of a printer spooling, problems arise when subjects from different security levels request to print. If the printer spooler has processed a print request from a high security level subject, the printer spooler becomes a subject with security level (tranquillity property at work) and would reject subsequent print requests from lower security level subjects due to the simple security property of “no read up”. The solution to this kind of scenario is to make the printer spooler a trusted subject, which is allowed to make changes in its security levels in order to handle print requests from multilevel subjects.

Another weakness of the model is that it does not address the problem of information being passed by covert channels. A covert channel is any communication channel that can be exploited by a process to transfer information in a manner that violates the system’s security policy. This channel is a private information flow that is not controlled by a security mechanism. For instance, even filenames (object names) can be a kind of covert channel if everyone on the system can see them. Sometimes, it is necessary not only to conceal the contents of the objects, but also their existence. There are two types of covert channels and the TCSEC defines them as [4]:

i. Covert storage channels: all vehicles that would allow the direct or indirect reading of writing of a storage location by one process and the direct or indirect reading of it by another.
ii. Covert timing channels: all vehicles that would allow one process to signal information to another process by modulating its own use of system resources in such a way that the change in response time observed by the second process would provide information.

In order to minimize the risk of security compromise existing in any multilevel computer system which contains classified information, the system should not contain covert channels with high bandwidths. However, it may be impractical to eliminate all covert channels with higher bandwidths sometimes in order to maintain an acceptable system performance. An audit capability is required to provide system administration with the ability to detect significant compromises. The failure to address covert channels can be a significant weakness of the BLP model because as advances in hardware architectures occur, it results in more computing resources available to exploit covert channels in vulnerable modern BLP-compliant systems [12]. This weakness is made worse if the use of COTS is incorporated into the computer system of the organization, because codes provided by people outside the organization could lead to Trojan Horses being implanted into secure systems, and unwittingly allowing unauthorized users to exploit the fast speed of the hardware activities in modern systems to transfer information over covert channels.

The fourth weakness of the model is that it does not address the management of access control. Due to the tranquillity property, access permissions or access rights of objects cannot change. In the real world, access rights of different objects may change over time. For example, logistical information during the Transition-To-War period, when stockpiles of supplies and equipment occur, could be highly classified information and its access rights

being such that only “write-ups” (for instance, to report current levels of supplies) and “no read-downs” (for instance, operation plan) are allowed to maintain secrecy. However, at the start of war, this piece of information would have to be made available to lower echelons of the armed forces to execute the operation plan. The access rights to this information therefore have to be changed such that “read-down” access can be given. The inability of a security model to allow this change can handicap the effectiveness of the intended operational capability of the computer systems.
The last weakness of the model discussed is that it does not address information integrity. In 1987, Ken Biba wrote a paper that pointed out this weakness [5]. For example, a low security level user could over-write highly classified documents unless an integrity policy exists to prevent that. The model does not discuss the ways legitimate modifications can be made by authorized users and what would be the security classification as a result of this modification (which could change after modification). Sometimes, a document with modification(s) made may end up having sections with different security classification labels. The way the BLP model handles this is to classify the document at the highest security level from aggregate of the security labels of the sections. Adhering to the *-property, the only modification (write) allowed is from lower to higher levels. This might lead to the problem where all documents or information move gradually from low to the highest security levels over time.

5.3.2 Biba Model:

The main weakness to the Biba model that is commonly discussed amongst the computer security community arises from the Strict Integrity Policy and it is the problem of proper assignment of integrity labels to documents and users [13]. For the BLP model, the security levels and categories correspond to the government classification system. Established criteria or guidelines exist that help determine which disclosure levels and categories should be given to both personnel (subjects) and documents (objects). This is not the case for the integrity levels of the Biba model. It is difficult to nail down the criteria to justify the assignment of different integrity levels to users and data. Up till now, there are still no criteria for determining integrity levels and categories. For this reason, it is thought that the Biba model is not the best approach for dealing with integrity. Until a classification similar to the established governmental classification system is worked out and tested to work well, hierarchical levels will not be very useful for computer system integrity. It does not seem to be practical or easily implemented where the determination of integrity labels for specific data and the subsequent labelling operations of data items seem extremely difficult and of a much higher cost than the value returned.

5.3.3 Domain Based Security:

One of the weaknesses of the model is that the success of the implementation of Domain Based Security is dependent on the presence of an influential “champion” who can lead the project to completion. This “champion” should come from the executive management and he or she needs to believe in the value of the work involved in the model. The “champion” has to garner the support of the rest of the executive management to gain cooperation by all levels of employees in the organization in sharing their corporate knowledge. In the process of creating the Infosec Business Models, Infosec Infrastructure Models and the Infosec Architecture Models, the security analysts need to talk to people to gather the necessary information. The project team is likely to encounter resistance from people of some domains who jealously guard their information and are reluctant to share information. This problem is especially apparent for projects that involve large-scale modelling of the organization’s business processes and computer systems which can involve a lot of people from different domains. In addition, large-scale projects in a defence-related organization commonly take more than one year to complete. The composition of the project team may change and there might even be a change of the “champion”. This is not good for the continuity of the project.
Another weakness concerns the risk of a small group of people having access to a lot of classified information. Sufficient clearance is required of the personnel who are modelling

and analysing the business processes and the IT infrastructure of the organization. This is especially so for an organization dealing with defence science for whom the Ministry of Defence is a major client. It is a risk from the perspective of the organization and its client for a single person or a group of people to have access to a large amount of sensitive information spanning different domains.
The model recommends the use of COTS, and the last weakness of the model arises from this recommendation. Attacks on the computer systems resulting in a computer security breach might occur from the exploitation of known vulnerabilities in COTS products by people with ill intent (disgruntled employees or adversaries). In addition, the use of COTS might unwittingly introduce Trojan Horses or some other codes designed for ill intent and thus jeopardize the infosecurity of the computer systems.

5.4 Selection of a Model for a Defence-Related Organization:

The discussion for this section starts by first looking at how each security model meets the following criteria for use in a defence-related organization (as given in Chapter 1:Section 1.5):

- Ability to fulfil the infosecurity needs of a typical defence-related organization:
  The infosecurity needs include multilevel security, confidentiality of information, integrity of information, authentication and availability of information. Being a confidentiality model that is built in the context of governmental classification of information [2], the BLP model is apt in addressing multilevel security and information confidentiality, though it does not deal with the other infosecurity needs listed above. The Biba model is commonly categorized as an integrity model with hierarchical classification of integrity, and it deals only with multilevel security and information integrity at the exclusion of other infosecurity needs. The Domain Based Security is an approach that seeks to identify security objectives by looking at all the relevant infosecurity risks relevant to the organization, and then implementing security measures in response to the risks identified. Being an encompassing and generic methodology that covers identification and mitigation of infosecurity risks from front-end planning to maintenance, it could handle most of the infosecurity needs mentioned above. However, it is most obvious that the needs of multilevel security, information confidentiality and information availability are fulfilled by the use of domains and islands in the approach.

- Ease of adopting or implementing the model:
  In the previous sub-section discussing the weaknesses of the models, it can be observed that the BLP model and Biba model are not easy to handle in terms of system design and implementation. For example, a lot of software needs to be rewritten or modified to run on multilevel platform of a BLP-compliant system [2]. For the Biba model, it does not seem to be practical or easily implemented because the determination of integrity labels for specific data and the subsequent labeling operation of data items seem extremely difficult and of a much higher cost than the value returned [13]. In comparison these two security models, the Domain Based Security suffers less technical difficulty, and the weaknesses lie more in the human aspect of implementation (Section 5.3.3 for details). The opinion of whether this model is easier or more difficult to handle due to these weaknesses could be subjective. Some may find it more difficult to iron out problems arising from human behavior than technical hitches.

- Ease of understanding the intended capabilities of the model:
  There are a lot of publicly available papers discussing the theories and implementation of the BLP Model and the Biba model. In terms of the availability of information and experts (especially among the academics of computer security), there is no lack of information and advice for someone eager to understand the intended capabilities of these two models. However the ease of getting information and advice

does not necessarily equate to the ease of understanding them. The availability of information on Domain Based Security is more limited because the White paper that proposed this approach was only written recently in 2002. There is not much other information available regarding this methodology. The experts in this area may also not be easy to find.

Table 5.1 below shows in summary the extent each security model meet the criteria for being the most suitable model for a typical defence-related organization.

Selection Criterion **Security Model**	**Ability to fulfill infosec needs for a typical defence-related organization**	**Ease of adopting or implementing the model**	**Ease of understanding the intended capabilities of the model**
Bell LaPadula model	Infosec needs of multilevel security and information confidentiality are met.	Difficult.	May be easy due to abundant resources available to research the model.
Biba model	Infosec needs of multilevel security and information integrity are met.	Difficult.	May be easy due to abundant resources available to research the model.
Domain Based Security	May be able to meet all the infosec needs, though multilevel security, information confidentiality and availability are the needs most obviously met.	May be considered difficult.	May not be easy because of the lack of resources to research on the model.

Table 5.1: Comparison of Models Against the Selection Criteria for the Security Model of a Typical Defence-Related Organization

Next, the discussion on the suitability of the security models continue by looking at how well each security model complements to the characteristics of the organization. A list of the characteristics for the business environment is given as follows:

- Domain-based segregation of systems that sometimes need to "talk":
  In this context, "talk" means the flow of information between systems. The BLP model and the Biba models were designed to suit a military environment where information and users are categorized into domains such as Chemical Warfare and Army Logistics. Systems are allowed to "talk" subject to the respective rules of the models. For Domain Based Security, systems and users are segregated into logical domains in which inter-domain flow of information can occur in a tightly controlled manner. Hence all the three security models can complement this characteristic well.

- Control of information flow to allow access to only authorized users on a need-to-know basis:
  In the BLP model, there is control of information flow such that users must have sufficient security clearance in order to access classified information. The model further restricts the access of these users by granting access to information that is required by their work (i.e. on a need-to-know basis). The Domain Base Security also controls the information flow between defined domains. Users can have relatively easy access to information within their domain (which can be assumed to be directly relevant to their work), but the information in and out of their domains is tightly controlled. The Biba model does not really discuss the control of information flow, rather it is about the control of modifications that can be made on information in the

secure systems. Hence the BLP model and the Domain Based Security can complement this characteristic well.

- Access to the internet in the work environment:
  It is possible to have workstations in the work environment to be connected to the Internet. However, in the interest of protecting secure systems from the myriad of infosecurity attacks that could occur from the Internet, it is best that these workstations are isolated from these systems. The BLP model and the Biba model do not address the threats of the Internet to secure systems. The Domain Based Security would probably treat the workstations with Internet connection to pose high security risk and appropriate security measures need to be in place to handle the threats. Hence out of the three security models, the Domain Based Security may be the only one that can complement this characteristic well.
- "Paperless" work environment:
  In a "paperless" work environment, it is important that the information would be available to the users when requested. It is also important that the integrity of the information is upheld because the digitised information may be the only form of the information stored. The concerns addressed in the Biba model are very appropriate for such an environment. In a way, all the three security models could support the set-up of a "paperless" work environment in the sense that information may be stored in the systems whatever the security models are implemented. However, it is prudent to have full backup of these systems just in case system failures occur.

Table 5.2 below shows in summary the extent each security model caters to the characteristics of the business environment typical of a defence-related organization.

Characteristics / **Security Model**	**Domain-based segregation of systems**	**Control of information flow**	**Internet access in the work environment**	**"Paperless" work environment**
Bell LaPadula model	√	√		
Biba model	√			√
Domain Based Security	√	√	√	

Table 5.2: Extent of models In Catering to the Characteristics of a Typical Business Environment in a Defence-Related Organization.

Chapter 6: Conclusion

There are a myriad of digital threats that the computer systems of a defence-related organization is vulnerable to, and it is important that the organization is able to find a suitable security model that it may adopt to protect itself against most of the threats. Some of the major digital threats include unauthorized access, malicious damage, impersonation, and denial-of-service. In many sense the infosec needs of a defence-related organization are similar to that of a military organization. These infosec needs include multilevel security, information confidentiality, information integrity, authentication and information availability. In this thesis, the three security models that are studied are the Bell LaPadula (BLP) model, the Biba model and the Domain Based Security. They are chosen for their apparent relevance to a defence-related organization, being themselves developed for use by military organizations. The intended capabilities, the strengths and the weaknesses of each model are discussed. Each of the security models is able to meet at least a particular area of infosec needs for the organization. Being developed in the context of the United States governmental classification of military and intelligence data, the BLP model is able to address multilevel security well. The other need that is addressed by the model is information confidentiality. However, the BLP model does not address other infosec needs that are as important as those included in the model, and it suffers many implementation setbacks. The Biba model is good in pointing out valid issues concerning information integrity of secure systems, which are glaringly lacking in the BLP model. However the Biba model suffers implementation setbacks too. This is because the hierarchical integrity classification is not easily implementable or practical at the moment. The Domain Based Security is a useful methodology that provides a framework that guide security analysts in performing a comprehensive risk assessment. The assessment helps identify the security objectives by assessing the risks arising from the way business is conducted and the IT infrastructure, and deciding the various types of protection required by information assets. Being a generic methodology, the Domain Based Security can help in the identification of most infosec risks, and suggest security solutions to mitigate these risks.

After looking at the strengths and weaknesses of the models, the extent to which each fits the criteria for use in a defence-related organization, and the extent to which each complements the characteristics of the business environment in such an organization, the Domain Based Security approach seems to be a practical and relatively easily implemented security model that can offer the most help in protecting the information assets of a typical defence-related organization.

Critical Appraisal:

By the time the description of the three security models was completed, I realized that Domain Based Security is not a typical security model, and comparing its capabilities to the other two models can be difficult. It is really an approach or methodology that tackles the infosec needs of a military organization (it was developed for the United Kingdom Ministry of Defence). Nevertheless, I focus on how each model satisfy the infosec needs that are relevant to a defence-related organization, and hopefully manage to compare the merits and demerits of each model in a fair way.

It would be good to include in this thesis the discussion of the infosec threats and infosec needs arising from the use of the email system in a defence-related organization. The use of emails has become an essential communication tool for many organizations. Classified information may be exchanged in emails, and classified documents may be attached to emails. In addition, the email system is a means by which many malicious codes are introduced into the computer systems of organizations. The management of the infosecurity risks arising from the email system is important to the holistic management of digital threats in many organizations.

Bibliography

[1] Schneier, B (2000) *Secrets & Lies Digital Security in a Networked World*. Wiley, New York.

[2] Anderson, R (2001) *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, New York.

[3] Bell, D. E. and LaPadula, L. J. *Secure Computer System: Unified Exposition and Multics Interpretation*. Technical Report MTR-2997, Mitre Corporation, Massachusetts.

[4] United States Department of Defense (1985) *Trusted Computer System Evaluation Criteria*. DoD 5200.28-STD, National Computer Security Center, Fort Meade.

[5] Biba, K. (1975) *Integrity Considerations For Secure Computer Systems*. Technical Report MTR-3153, Mitre Corporation, Massachusetts.

[6] Defence Evaluation and Research Agency (2000) *Overview Of Domain Based Security*. Report DERA/KIS/SEB/TR000807/v1.0, Hampshire, United Kingdom.

[7] Hughes, K. J. (2000) *Domain Based Security Modeling And Analysis Techniques: Introduction To Infosec Architecture Models*. Report DERA/KIS/SEB/CR000nnn/1.0, Defence Evaluation and Research Agency United Kingdom, Hampshire.

[8] Hughes, K. J. (2002) *Domain Based Security: Enabling Security At The Level Of Applications And Business Processes*. White Paper. QinetiQ Ltd, Hampshire.

[9] McLean, J. D. (1990) *The Specification and Modeling Of Computer Security*. Computer, 23(1). Institute of Electrical and Electronics Engineers, Inc., New Jersey.

[10] Sullivan, E. C./ Oregon Health & Science University (2003) *Security Policy Models The Bell- LaPadula Model*. http://www.cse.ogi.edu/~crispin/527/cse527%20Policy%20and%20BLP2.ppt

[11] Chan, Eddy/ Imperial College London (2003) *Computer Security Models*. http://infoeng.ee.ic.ac.uk/~malikz/surprise2001/spc99e/article1/

[12] Sibley, E. H., Michael, J. B. and Sandhu, R. S. (1991) A case-study of security policy for manual and automated systems. *Proceedings Of 6th Annual Conference on Computer Assurance (COMPASS 91)*, **June 1991**, 63-68. Gaithersburg, MD.

[13] Mayfield, T., Roskos, J. E., Welke, S. R. and Boone, J. M. (1991) *Integrity In Automated Information Systems*. Technical Report 79-91, Institute of Defense Analysis, Virginia.