The South African Institute for Computer Scientists and Information Technologists

ANNUAL RESEARCH AND DEVELOPMENT SYMPOSIUM

23-24 NOVEMBER 1998
CAPE TOWN
Van Riebeeck hotel in Gordons Bay

Hosted by the University of Cape Town in association with the CSSA,
Potchefstroom University for CHE and
The University of Natal

PROCEEDINGS

EDITED BY
D. PETKOV AND L. VENTER

SPONSORED BY

ABSA Group

The South African Institute for Computer Scientists and Information Technologists

ANNUAL RESEARCH AND DEVELOPMENT SYMPOSIUM

23-24 NOVEMBER 1998
CAPE TOWN
Van Riebeeck hotel in Gordons Bay

Hosted by the University of Cape Town in association with the CSSA,
Potchefstroom University for CHE and
The University of Natal

GENERAL CHAIR : PROF G. HATTINGH, PU CHE

PROGRAMME CO-CHAIRS:
PROF. L VENTER, PU CHE (Vaal Triangle), PROF. D. PETKOV, UN-PMB

LOCAL ORGANISING CHAIR: PROF. P. LICKER, UCT - IS

PROCEEDINGS

EDITED BY
D. PETKOV AND L. VENTER

SYMPOSIUM THEME:

Development of a quality academic CS/IS infrastraucture in South Africa

SPONSORED BY

ABSA Group

Proceedings of the 1998 Annual Research Conference of the South African Institute for Computer Scientists and Information Technologists.
Edited by Prof. D. Petkov and Prof. L. Venter
Van Reebeck Hotel, Gordons Bay, 23-24 November 1998

ISBN: 1-86840-303-3

Keywords: Computer Science, Information Systems, Software Engineering.

The views expressed in this book are those of the individual authors and not of the South African Institute for Computer Scientists and Information Technologists.

Office of SAICSIT: Prof. J.M.Hatting, Department of Computer Science and information Systems, Potchefstroom University for CHE, Private Bag X6001, Potchefstroom, 2520, RSA.

Produced by the Library Copy Centre, University of Natal, Pietermaritzburg.

FOREWORD

The South African Institute for Computer Scientists and Information Technologists (SAICSIT) promotes the cooperation of academics and industry in the area of research and development in Computer Science, Information Systems and Technology and Software Engineering. The culmination of its activities throughout the year is the annual research symposium. This book is a collection of papers presented at the 1998 such event taking place on the 23rd and 24th of November in Gordons Bay, Cape Town. The Conference is hosted by the Department of Information Systems, University of Cape Town in cooperation with the Department of Computer Science, Potchefstroom University for CHE and and Department of Computer Science and Information Systems of the University of Natal, Pietermaritzburg.

There are a total of 46 papers. The speakers represent practitioners and academics from all the major Universities and Technikons in the country. The number of industry based authors has increased compared to previous years.

We would like to express our gratitude to the referees and the paper contributors for their hard work on the papers included in this volume. The Organising and Programme Committees would like to thank the keynote speaker, Prof M.C.Jackson, Dean, University of Lincolshire and Humberside, United Kingdom, President of the International Federation for Systems Research as well as the Computer Society of South Africa and The University of Cape Town for the cooperation as well as the management and staff of the Potchefstroom University for CHE and the University of Natal for their support and for making this event a success.

Giel Hattingh, Paul Licker, Lucas Venter and Don Petkov

Table of Contents Page

A 6-DIMENSIONAL SECURITY CLASSIFICATION FOR INFORMATION

Walter Smuts
Department of Computer Science and Information Systems
University of South Africa, PO Box 392, Pretoria 0003, email smutswb@alpha.unisa.ac.za

Abstract

Most existing information security classification schemes use a **1-dimensional** scale such as [*top secret, secret, employee confidential, company confidential, restricted*]. These classification schemes do not differentiate between the different security properties of information, nor between the *level* and the *scope* of security. In this paper, it is shown that a 1-dimensional classification scheme is inadequate and can result in inappropriate protection, causing increased cost and risk.

A **6-dimensional** security classification scheme for information is proposed and it is shown how this scheme can be used to provide adequate and appropriate levels of security.

Introduction

One of the most important functions of an information security policy, is to classify information according to its sensitivity or importance to the company. Classifying information into discrete security classes simplifies the process of ensuring the security thereof.

Most existing security classification schemes for information use a 1-dimensional scale such as

- Top secret
- Secret
- Employee confidential
- Company confidential
- Restricted

Although these classification schemes date from a time when information was predominantly stored in a paper format, they are in most cases directly applied to documents in electronic format. We argue that such a 1-dimensional classification scheme is inadequate for information in electronic format. In fact, we even believe that it is inadequate for information in paper format too.

These 1-dimensional classification schemes do not differentiate between the *scope* and the *strength* of protection. As clearly reflected by the labels chosen for the classes, the emphasis is usually on the *scope of confidentiality* only. For example, information which is classified as *company confidential*, may be shared with anyone in the company, but not with people outside the company. No reference is made to how strong the protection against access by outsiders should be, or how well the *availability* of the information should be protected for the insiders.

If the information security policy does specify the level of protection for a certain class of information, it usually only refers to the level of protection for *confidentiality*. In many cases, this enforces completely inadequate protection mechanisms. As an example, for a telephone service provider, the information in the switching centres which control the way in which telephone calls are routed, is extremely sensitive and needs the highest level of protection. If the integrity of this information is affected, telephone calls would not reach their destinations, and the company will loose revenue and may even have to close down. The information in the telephone switches has, on the other hand, no value to anyone outside the company and does not have to be kept secret. In a 1-dimensional classification scheme, the highest level of classification would be the *Top Secret* class. Classifying the information in the telephone switches as *Top Secret*, would impose completely inadequate and unnecessary protection mechanisms onto the information. Inadequate, because the integrity and availability of the information is not protected, and unnecessary, because the secrecy of the information does not have to be protected.

An over-simplified classification scheme enforces the classification of information in inappropriate classes, which again will (through the security policy) enforce inappropriate protection mechanisms on the information source. This will provide inadequate protection and unnecessary inconvenience and cost in those cases where the protection is not needed. The importance of appropriate levels of protection has been emphasized by others [2], [1].

It is within this context that a new security classification scheme for information is proposed.

Information Formats

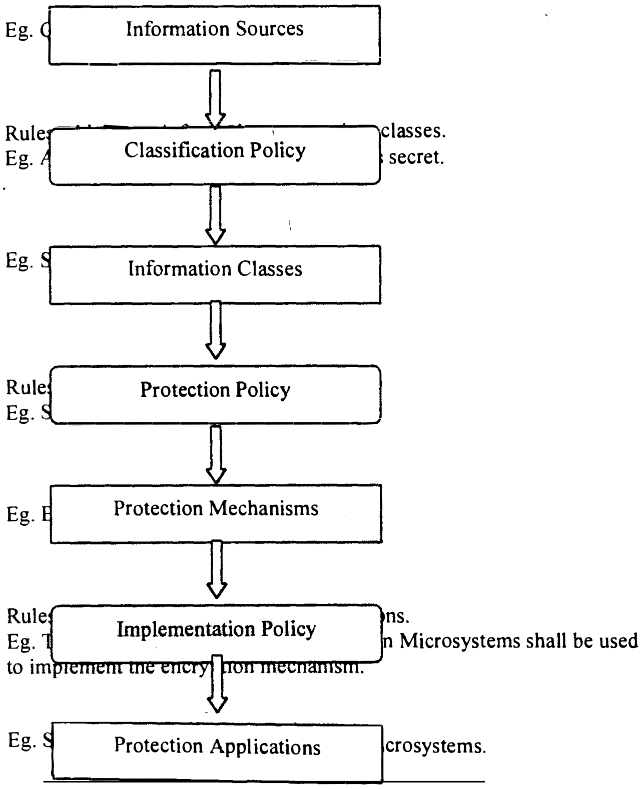
Information basically exists and moves around in companies in three formats:

- paper
- electronic
- intellectual (peoples minds)

This paper focuses on the electronic format of information. The structure and mechanisms can be extended to include information in paper format too. It is definitely not an attempt to address any structures and rules necessary to prevent security breaches when employees share their knowledge.

Information Security Process

For the purposes of this paper, the process of providing information security is modeled as follows:



The Security Process can be explained as follows:

- There are a number of information sources which need to be protected.
- There are a number of applications available, which can be used to protect information.
- The information security process is used to map *sensitive information sources* to *protection applications*.
- The **Classification Policy, Protection Policy** and **Implementation Policy** are needed to ensure that the correct applications are used to provide appropriate protection for every information source.

- A **Classification Policy** is used to simplify the security process. Instead of having a continuum of solutions, a small number of discrete classes are used to provide protection. Every information source is classified into one of these classes. *Secret* is an example of a security class.
- The **Protection Policy** is used to map every information class to a list of mechanisms which must be used to protect all the information sources falling in that class. *Data encryption* is an example of a security mechanism.
- The **Implementation Policy** maps the security mechanisms to real protection applications (products which can be bought and installed). *SKIP* encryption from SUN Microsystems is an example of an application which can implement a data encryption mechanism.

Information Security Properties and Attributes

The one-dimensional security classification mentioned earlier refers to only **one** (confidentiality) of the security properties of information. A more complete model would protect the following three properties [4], [3]:

- **Confidentiality** (secrecy).
  Preventing unauthorized disclosure of information.

- **Integrity** (correctness).
  Preventing unauthorized modification of information.

- **Availability**.
  Preventing denial of authorized access to information.

For every one of these properties there are two attributes:

- **Protection Level**
- **Protection Scope**

The protection level refers to the **strength** of the protection which is provided, while the protection scope refers to the **group of people** for whom the protection is provided. The one-dimensional classification generally indicates the **scope of confidentiality protection** only. A classification system is needed which differentiates between the *level* of protection and the *scope* of protection.

Six-Dimensional Security Classification

Because there is a price to be paid for putting security mechanisms in place, it is important to have appropriate levels of security. In order to express all the subtleties of the security properties of the information, a classification system using six different values, is proposed.

The security classification of each information source is represented by the following six values:

Security_Class: C (C_L,C_S)
I (I_L, I_S)
A $(A_L,A_S)]$

Where

- C: Confidentiality
- C_L: Level of confidentiality protection (values 0 to 3)
- C_S: Scope of confidentiality protection (values reference a security group, eg. IT_Department)

- I: Integrity
- I_L: Level of integrity protection (values 0 to 3)
- I_S: Scope of integrity protection (values reference a security group, eg. IT_Department)

- A: Availability
- A_L: Level of availability protection (values 0 to 3)
- A_S: Scope of availability protection (values reference a security group, eg. IT_Department)

The following three examples show how this classification scheme can be applied to information in a company:

Example 1:

Information: Company Internal Telephone Directory
Classification: **C** (1, company)
I (1, switchboard)
A (1, company)

This classification means that the **confidentiality** of the internal telephone directory will be protected by level 1 confidentiality protection mechanisms. These mechanisms will be used to make sure that the information is not available to people outside the company. The internal telephone numbers should remain inside the company, but this is not so important that it justifies the cost and inconvenience of higher levels of protection.

The **integrity** of the information is also protected by level 1 protection mechanisms, but in this case the scope is restricted to the people working at the switchboard. Only they will have the ability to change the telephone records, and everyone else will be prevented from doing so by level 1 integrity protection mechanisms.

Finally, the **availability** of the information in the internal telephone directory is ensured for everyone in the company by level 1 availability protection mechanisms.

Example 2:

Information: New Business Plans
Classification: **C** (3, Top_Management)
I (2, Top_Management)
A (1, Top_Management)

This classification reflects that fact that the confidentiality of the new business plans should be protected by the highest (level 3) protection mechanisms, and be restricted to the top management only. The integrity of the information is only protected by level 2 mechanisms, again for the top management. The reasoning may be that top management will hopefully notice if the plans were changed maliciously. Lastly, the new business plans definitely do not need to be on-line available for 24 hours per day, and therefore need only be protected by level 1 availability protection mechanisms.

Example 3:

Information:Configuration of Core Business Equipment
Classification: **C** (1, Company)
I (3, Engineering_Department)
A (3, Engineering_Department)

An example of this type of information is the configuration of the computers which control a chemical plant, telephone switching centre or a power station. This information has very little value to anyone else, therefore the level 1 confidentiality protection. The integrity of the information is, however, crucial to the operation of the company. If this information is changed maliciously, it can have devastating effects on the company and is therefore protected by level 3 integrity protection mechansims. 24 Hour on-line availability to manage the processes is again critical and needs to be protected by level 3 availability protection mechanisms.

The next sections show how this classification scheme can be used in the information security process to ensure adequate protection for all information sources.

Information Sources

All critical information sources must be identified. Every critical information source must be classified before it can be protected. All information is by default not protected.

Classification Policy

A classification policy is a set of rules which spells out **how** information should be classified. The 6-Dimensional Information Classification Scheme simply defines the classes. It does not specify which type of information should be classified in which class. The following statements illustrate the type rules which can be found in a classification policy:

1. All information which can cause a loss of revenue if the confidentiality is compromised, must have a **$C(3,C_s)$** classification where the scope **C_s** is chosen to be the smallest group necessary to perform the work.
2. All information which can cause the company embarrassment if the confidentiality is compromised, must have a **C(1,Company)** classification.
3. All information which can cause a loss of revenue if the integrity is compromised, must have a **$I(3,I_s)$** classification where the scope **I_s** is chosen to be the smallest group necessary to perform the work.

Information Classes

The information classes are those defined in the 6-Dimensional Information Classification Scheme. The scale used in each dimension can differ from company to company.

Levels of Protection

> The scale using 4 different levels of protection with a value of **"0"** meaning **"no protection"** and a value of **"3"** meaning the **"highest level of protection"**, seems to be a practical choice.

Scope of Protection

> The scope of protection will reflect the organigram of the company and may have values such as:
> - Top Management
> - Finance_Department
> - Engineering_Department
> - Y2K_Project
> - Company

Protection Mechanisms

Security protection mechanisms are abstract concepts (algorithms, transformations, etc.) which can be used to protect the security properties of information.

Every company needs a list of security protection mechanisms which it needs and can support. The following are examples:

- Strong end-to-end encryption.
- Weak end-to-end encryption.
- Link encryption.
- Strong password protection.
- Weak password protection.
- Firewall protection.
- Dual redundant communication links with a hot take-over ability.
- Dual redundant communication links.
- Dual redundant servers with a hot take-over ability.

- Double backup.
- Automatic daily/weekly backup.
- Regular user-initiated backup.

Protection Policy

The Protection Policy maps the **security classes** to **security protection mechanisms**. It states that if an information source is classified in a specific security class, then it must at all times be protected by the mechanisms specified for that class. The following table shows an example of how the security policy can map protection mechanisms to specific security classes:

Table 1: Protection Policy

Protection Level	Confidentiality	Integrity	Availability
3: High	• Strong end-to-end encryption of data for all communication. • Strong encryption of data on disk. • Strong password protection for all users of the equipment. • Fire wall protection.	• Weak end-to-end encryption of data for all communication to equipment. • Strong encryption of data on disk or • Strong password protection for all users on equipment. • Fire wall protection.	• Automatic double backup every 24h. • Dual redundant communication links for all communication paths with a hot take-over ability. • Dual redundant servers with a hot take-over ability.
2: Medium	• Weak end-to-end encryption of data for all communication. • Fire wall protection.	• Strong password protection for all users on equipment. • Fire wall protection.	• Automatic weekly backup. • Dual redundant communication links. • Dual redundant servers.
1: Low	• Weak password protection for all users of the equipment. • Fire Wall Protection • Weak link encryption over public networks.	• Weak password protection for all users of the equipment. • Fire Wall Protection • Weak link encryption over public networks.	• Regular user initiated backup.
0: None	• None	• None	• None

Protection Applications

Protection applications are product which can be bought (or in-house developed) to implement the protection mechanisms. The following are examples of protection applications:

- SSH Secure Shell from Data Fellows.
- Skip and SunScreen EFS from Sun Microsystems.
- Firewall-1 from Check Point.
- Windows NT Domain login from Microsoft Corporation.
- SecurID from Security Dynamics.

Implementation Policy

The implementation policy maps the security mechanisms to specific security applications.
The following mappings may, for example, be used:

- Strong Encryption: SSH from Data Fellows.
- Weak Encryption: Skip From Sun Microsystems, Link encryption from Cisco.
- Weak Password Protection: NT Login from Microsoft.
- Strong Password Protection: SecurID Tokens from Security Dynamics.
- Firewall:Firewall 1 from Check Point.

Conclusion

A 1-dimensional security classification cannot be used to provide appropriate protection for all types of information in a technology-based company. It causes many information sources to be either inadequately or unnecessarily protected. This increases both the security risk and the cost of ensuring security.

A 6-dimensional classification scheme can reflect more of the subtleties between different information sources and can be used to both reduce the risk and the cost in providing information security.

References

1. Z. Ciechanowicz. "Risk analysis: requirements, conflicts and problems", *Computers & Security*, Vol 16 no 3, p 223-232, (1997).

2. W.F. de Koning. "A Methodology for the design of security plans", *Computers & Security,* Vol 14 no 7, p 633-643 (1995).

3. J. Olnes. "Development of Security Policies", *Computers & Security*, Vol 13 no 8, p 628-636, (1994).

4 C.P. Pfleeger. *Security in Computing.* Second edition, Prentice Hall, Upper Saddle River, NJ, 1997.