Security of Computer Based Information Systems

V.P. Lane

Security of Computer Based Information Systems

V.P. Lane

Principal Lecturer
Department of Systems and Computing
North East London Polytechnic

M
MACMILLAN

First published 1985

Published by
MACMILLAN EDUCATION LTD
Houndmills, Basingstoke, Hampshire RG21 2XS
and London
Companies and representatives
throughout the world

Printed in Great Britain by
Camelot Press Ltd,
Southampton

British Library Cataloguing in Publication Data
Lane, V. P.
Security of computer based information systems.
–(Macmillan computer science series)
1. Electronic data processing departments–
Security measures
I. Title
658.4'78 HF5548.2

ISBN 0–333–36436–8
ISBN 0–333–36437–6 Pbk

Preface

Today, computer based information systems play a critical role and integral part in business operations. Companies and governments are involved each day with the electronic transfer of highly sensitive personal data and of data representing billions of pounds. Irrespective of whether or not a company is involved in electronic funds transfer, it is apparent that information is an important and valuable resource of small and medium sized businesses as well as large ones. These and other factors, such as data protection legislation, have combined to raise the subject of security of computer systems and computer based information systems to its current level of concern.

This book presents methods for engineering security into computer based information systems. It is not a computer security handbook because there are good handbooks already written; nor does it try to use checklists to show how to provide better levels of security. Instead, it attempts to show the underlying general principles of security. For example, checklists that are used extensively throughout the computer security industry are not shown in the book, but are discussed and explained as part of other heuristic methods.

A universal problem with books on computer security is that the subject embraces a vast number of topics, including physical security of buildings and computer facilities, fire protection, privacy, software, hardware, personnel management, financial control and audit and the psychological and sociological behaviour of people. As a result, some topics must be left in the background. Also authors may write on the subject from different viewpoints. For example, one author may concentrate on crime incidents, another on database security and another on hardware. My approach is from the educational needs of students aspiring to be systems analysts – an approach that naturally has its own strengths and weaknesses – but clearly this book can give only a broad insight into an extremely complex subject.

Structure of the book

Chapter 1 defines the basic terminology of security of computer based information systems and argues the importance of the subject. Chapter 2 summarises the basic concepts of physical security. Chapter 3 discusses the security of data within the computer and at the man-machine interface through consideration of access control, information flow, inference control in databases and cryptography. The highly specialised subjects of hardware, system software and communications are introduced in chapter 4 but only in so far as they influence computer applications. Chapter 5 explains the critical part played by people in security – people represent both threats and safeguards. In chapter 6 the steps that must be followed to create and build secure application software are examined. Chapter 7 considers operational aspects of security and shows how operational procedures can ensure that well-designed application software does not deteriorate when in operation. Chapter 8 shows how a security programme can be developed for an organisation and stresses the critical role of people – a theme developed earlier in chapter 5. The historical and international background of the UK Data Protection Act with its management, technical and financial implications is reviewed in chapter 9. In chapter 10 the need for both technical and legal deterrents for proprietary software protection is stressed and detailed consideration is given to copyright, trade secret and patent protection. A number of real-life security breaches are described in chapter 11 to highlight points made in earlier parts of the book. One incident is used for a discussion of data protection legislation and the other incidents highlight the importance of contingency planning, company internal controls, recruitment procedures and policies on the use of computer resources by computer centre personnel. The final chapter refers to the need for a holistic approach to security and looks at the security implications of microcomputers.

Suggestions to readers

I have in mind one major group of readers, namely students who in their future careers will design information systems or advise non-computer personnel of a company about security. For these students the book provides a conceptual framework plus an explanation of useful principles and techniques. However, the book should be useful to any reader with a technical background and a serious interest in computing.

To facilitate its use as a textbook, questions are given at the end of each chapter. Pointers to answers are available from the author in a separate document. The majority of questions can be undertaken by a student studying alone, or they can be used for class discussion. There are a few questions, marked 'group problem', which are best studied by three or four students working together.

For the student

The book is intended to serve as a text in computer science or management studies for a senior course at undergraduate level or for postgraduate study. All chapters are appropriate for study but a few chapters – such as those on protection of proprietary software, data protection legislation and the case studies – can be read as separate self-contained studies. The chapters have some overlap but this is intentional because students must appreciate that the many and various security methods complement each other and that no one method can satisfactorily handle the security problems handled by other methods.

The would-be designer needs to appreciate many methods from a number of different chapters. In this sense, the chapters are purely artificial boundaries constructed to help the reader to approach a large subject.

Teaching

Security is not only a fascinating subject in its own right but is also an ideal vehicle to demonstrate the interactions between people and technology in sociotechnical systems. Ideally, the teaching of security should reflect the multidisciplinary nature of information processing and security. Therefore, it presents a perfect opportunity for team teaching.

Although every effort has been made to eliminate errors, some will inevitably remain. Therefore, I would be grateful to receive comments from readers regarding errors of a typographical or a substantive nature.

Acknowledgements

Figures 1.1 and 1.2 are adapted from figure 7 of block II of the Open University course T301 – Complexity, management and change; applying a systems approach, Open University, 1984

Figure 3.2 is adapted with permission from figures 1a and 1b of the paper 'Data security' by Dorothy Denning and Peter Denning, September 1979, *ACM Computing Surveys.* Copyright 1979, Association for Computing Machinery, Inc.

Figure 8.2 and tables 8.2 and 8.3 are reprinted by permission of the publisher from 'Security risk management in electronic data processing systems' by R. H. Courtney presented at the *AFIPS National Conference 1977*

Figure 8.4 is reprinted from *Systems Thinking and Systems Practice* by Peter Checkland. Copyright (1981) reprinted by permission of John Wiley & Sons, Ltd.

Table 10.4 appeared in 'Computing and reform of copyright protection' by D. J. Grover and R. J. Hart, *Computer Bulletin,* March 1982 and is reprinted with permission of the British Computer Society

Tables 11.1, 11.2 and 11.3 appeared in the *Computer Fraud Survey 1985* and are reprinted with permission of the Controller of Her Majesty's Stationery Office.

Ideas for this book started well before I received the assignment to write it. The interest in security started during the late 1960s when I was data processing manager in the Joseph Lucas Group with responsibility for designing and operating secure payroll and other financial systems. The interest developed over the next decade, first through consultancy assignments in many industries including the financial sector, later through experience of project management of major projects in the public sector and finally through my lecturing in security.

Consequently, I have learned a great deal from many people with whom I have worked and am most grateful to those who have helped directly and indirectly with my work in security. In particular, I would like to thank John Corcoran of National Giro Bank, Frank Davies of Littlewood Mail Order computer services, Mark Kahrs of the Computing Science Research Center, AT & T Bell Laboratories, New Jersey, John Step of the Audit Consortium of the Brighton, Tunbridge Wells, Eastbourne and Hastings Health Authorities and Frank Wright of Southern Water Authority for reading parts of the book and providing helpful comments, and Peri Loucopoulos of UMIST for encouragement during the preparation of the manuscript. I have received help from many colleagues at North East London Polytechnic; in particular Allan Cheatham and John Peacham have commented upon parts of the book, Bill Smith helped with the use of word processors, Joan Mouyia assisted in locating publications and Gloria Shayler produced the artwork. Recognition and thanks are due to several talented and helpful members of the staff of Macmillan. In particular I would like to acknowledge the help of Bill Perry and Malcolm Stewart. Finally, and most important, the support and encouragement of my wife Joan was indispensable.

Contents

1 Threats, Safeguards and Security Objectives

Security of computer based information systems is concerned with methods of providing cost effective and operationally effective protection of information systems from undesirable future events. These events, referred to as 'threats', can cause an organisation to suffer a loss and at such times a 'breach of security' is said to have occurred. There are three types of loss, namely (1) loss of integrity, (2) loss of availability of services and (3) loss of confidentiality.

1.1 Security

The rapid growth and widespread acceptance and approval of information technology by organisations have provided many significant benefits, such as better management control leading to increased efficiency at the organisation level. Unfortunately benefits seldom accrue without corresponding undesirable side effects which are often both unforeseen and costly. In this case, there is evidence that organisations are vulnerable to new dangers. For example, information technology has contributed to centralisation of both data and data processing which has created a corresponding and increased danger in the event of fire; but there has also been a major move to distributed computing which has increased the risk of personnel interfering with input and output data. Many organisations are not willing to recognise these threats and although willing to invest significant sums on information technology are unwilling to incur the relatively small additional expenditure to remove or neutralise the threats.

Threats may be caused by

(1) the information system itself — such as communications failure or employee mistake
(2) malicious acts of people
(3) external disasters, such as flood or lightning.

The first of these threats is a major security concern. It requires examination of the performance of an information system to establish that the system performs fundamental critical functions faithfully without undesirable side effects. This aspect of security encompasses reliability of applications, system software, communications, hardware and personnel. People are at the heart of all security safeguards and threats. On the one hand, users, managers, programmers, analysts, operators and many other people design, maintain and operate the security of the system and their contribution to security cannot be over-emphasised. However on the other hand, these same people who are necessarily involved in the information system are often the most vulnerable components of the system. People pose a threat because of (1) accidental acts and (2) deliberate acts. The possibility of inadvertent mistakes by people is fully recognised by designers but the dangers from malicious and deliberate acts receive less attention, except by designers of highiy sensitive systems such as those for national security. Although externally created disasters are not common occurrences in a computer centre, few sites are completely immune – for example, from the possibility of extreme weather conditions – and the impact of an external event can be horrendous to an organisation. There are no ideal solutions to the majority of security problems.

With infinite resources it is possible to achieve perfect security but in real terms absolute security cannot be guaranteed even in a technology based subject like computing. The impossibility of perfect security is brought into dramatic perspective by the incident in 1982 of a non-professional interloper breaking the security defences of Buckingham Palace to walk into the bedroom of the Queen, by the American teenage boy in 1983 connecting into the Los Alamos computer and by hackers gaining entry in 1984 to the electronic mailbox service of the Prestel system operated by British Telecom and breaking into client files, including that of the Duke of Edinburgh. Although perfection is not attainable, high levels of protection are possible even with limited resources. Generally, significant security improvements are possible at a cost that is trivial compared with the damage or loss that might be otherwise sustained. Nevertheless, cost is always an important factor in selecting security measures.

1.2 An introduction to security of computer based information systems

An organisation can be considered as a system formed by three subsystems; the operations subsystem, the management subsystem and the information subsystem, as shown in figure 1.1. The operations subsystem encompasses all resources, people and activities concerned with the primary functions of the organisation, whereas the management subsystem includes the resources and activities concerned with the planning, decision taking and controlling of operations. Information, fundamental for the effective operation of modern businesses, is provided by the information subsystem which is an assembly of machines, activities and people gathering and processing data to satisfy information requirements of management, as illustrated in figure 1.2. Consequently, the information subsystem is of prime importance to an organisation and it is worthy of consideration as a system in its own right. Information must be provided quickly and accurately and this can often be achieved only by computer based systems. In the past, computer based information systems supported only the control of the basic operational functions with typical applications being stock management, payroll and management accounting, but their use is now being extended into the management decision making function through the development of decision support and knowledge based systems. As a result, the correct behaviour of computers and information systems combined with accuracy and reliability of electronically provided data are fundamental for the day to day effective functioning of organisations.

In an imperfect world it cannot be expected that information systems will be without fault. Faults may appear in many different forms such as unauthorised disclosure of confidential and sensitive data, risk to national security or loss of money. Security safeguards to minimise the dangers or threats are essential. Unfortunately, information systems vary tremendously in the degree of sensitivity that they represent and the possible threats are correspondingly diverse. Therefore safeguards to neutralise the threats cannot be prescribed in any general manner for an organisation but must be designed for each information system.

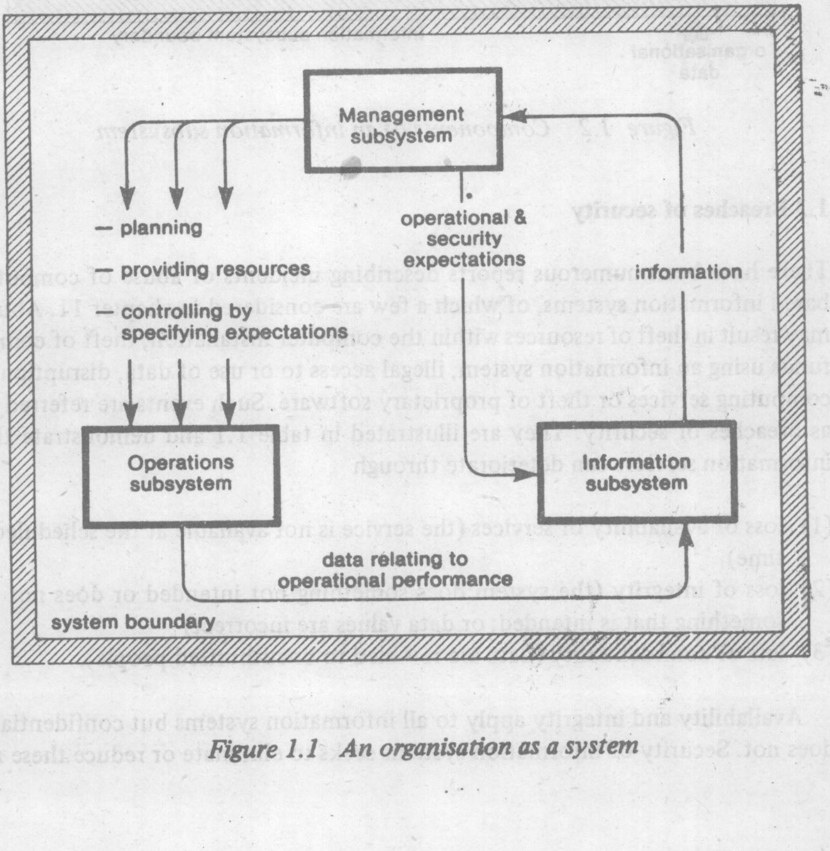

Figure 1.1 An organisation as a system

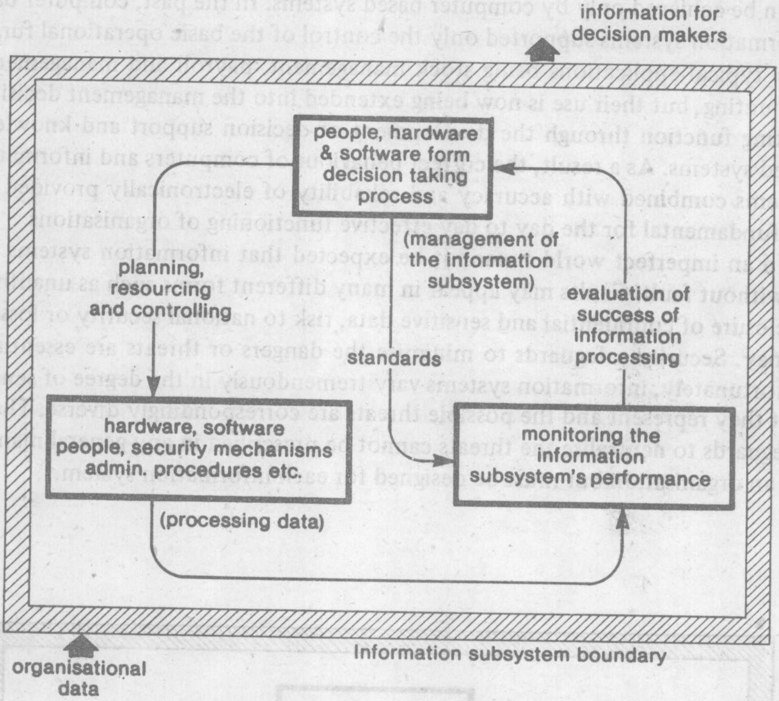
information for decision makers
people, hardware & software form decision taking process
planning, resourcing and controlling
(management of the information subsystem)
evaluation of success of information processing
standards
hardware, software people, security mechanisms admin. procedures etc.
monitoring the information subsystem's performance
(processing data)
organisational data
Information subsystem boundary

Figure 1.2 Components of an information subsystem

1.3 Breaches of security

There have been numerous reports describing incidents of abuse of computer based information systems, of which a few are considered in chapter 11. Abuse may result in theft of resources within the computer installation, theft of company funds using an information system, illegal access to or use of data, disruption of computing services or theft of proprietary software. Such events are referred to as breaches of security. They are illustrated in table 1.1 and demonstrate that information services can deteriorate through

(1) loss of availability of services (the service is not available at the scheduled time)
(2) loss of integrity (the system does something not intended or does not do something that is intended; or data values are incorrect)
(3) loss of confidentiality (data are revealed to unauthorised people).

Availability and integrity apply to all information systems but confidentiality does not. Security of information systems seeks to eliminate or reduce these risks

Table 1.1 Threats, breaches and countermeasures

Threat	*Loss of*	*Breach of security*	*Countermeasures*
Fire	Availability of computing services	Destruction of data and hardware	Fire and smoke detectors
Insertion of forged input data	Integrity	Financial fraud and corruption of data file	Sound clerical procedures and good administrative practices
Unauthorised perusal of computer reports	Confidentiality	Unauthorised access to sensitive data	Good administrative practices
Unauthorised perusal of terminal screen	Confidentiality	Unauthorised access to sensitive data	Terminal access control
Failure of computer terminal	Availability	Disruption of computing services	A reserve terminal
Noise affecting communications and so data transmission	Integrity and availability	Loss of data	Message sequence numbering
Theft of data file by computer personnel	Availability	Removal and hence non-availability of company data	Vetting of personnel and good operational procedures

of deterioration of services and is a vast subject dealing with hardware, system software, application software, people and organisations. This is not to imply that security has only a technical dimension. It is more than a technical subject and includes the psychological and sociological behaviour of people (Parker, 1981). In fact, the behaviour of people is a major and central factor in security.

1.4 Threats, countermeasures and security functions

A breach of security may be caused by

(1) accidental acts or
(2) deliberate acts.

For example, a fire may be caused by faulty electrics – an accidental act – or by arson – a deliberate act. A good designer attempts to identify such threats to security before they occur as acts, and designs appropriate countermeasures for incorporation within the information system to contain the threats.

Examples of threats, breaches and countermeasures are shown in table 1.1. The steps involved in designing security countermeasures to contain a specific threat are complex and it is a topic that is considered in chapters 2, 3, 4 and 8, but in a more general sense it is the theme of virtually every chapter of this book. For example, the threat of theft of proprietary software and the countermeasures of copyright and patent legislation are evaluated in chapter 10. In all design situations, the analyst must consider the security provided by countermeasures in terms of the following security functions.

(1) Prevention — This is the ideal theoretical concept which can seldom be achieved because of the cost of constructing or operating the countermeasures.

(2) Detection — Prevention and detection features are often combined; for example, in the identification and authentication procedure outlined in figure 3.1 unauthorised access is prevented, but in addition all failed access attempts are logged to detect unauthorised activities.

(3) Deterrence — It is often advantageous to make potential offenders aware of detection and other security procedures because fear of being discovered will prevent intent from becoming violation.

(4) System recovery — In situations in which prevention, detection and deterrence are not completely effective in dealing with a threat, recovery procedures are necessary; recovery examples are check points in jobs that take a long time to process and backup files.

(5) System correction — The weaknesses, which caused the need for recovery, must be corrected immediately after recovery.

(6) Avoidance — It may be the case that in a particular circumstance a specific threat cannot be handled adequately by security countermeasures and therefore the only satisfactory way to proceed is to change the design to remove the threat completely.

In general, accidents caused by human errors and omissions cause more losses than deliberate acts. Therefore, they should be the first to receive attention, especially as a system that accepts a large number of errors provides many opportunities for dishonest activity which can be concealed by the errors. Safeguards that reduce the dangers from accidents contribute to the reduction of opportunities for deliberate acts to abuse systems and to defraud.

1.5 Sensitivity of applications

Information systems are vulnerable to a wide range of hazards (FIPS 65, 1979).