Fourth IFIP TC 11 International Conference on
Computer Security
Monte Carlo, Monaco, 2–4 December, 1986

NORTH-HOLLAND
AMSTERDAM • NEW YORK • OXFORD • TOKYO

SECURITY AND PROTECTION IN INFORMATION SYSTEMS

Proceedings of the Fourth IFIP TC 11 International Conference on
Computer Security, IFIP/Sec '86
Monte Carlo, Monaco, 2–4 December, 1986

edited by

André GRISSONNANCHE
XP Conseil
Paris, France

1989

NORTH-HOLLAND
AMSTERDAM • NEW YORK • OXFORD • TOKYO

No responsibility is assumed by the publisher or by IFIP for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

ISBN: 0 444 87345 7

Published by:

ELSEVIER SCIENCE PUBLISHERS B.V.
P.O. Box 103
1000 AC Amsterdam
The Netherlands

Sole distributors for the U.S.A. and Canada:

ELSEVIER SCIENCE PUBLISHING COMPANY, INC.
655 Avenue of the Americas
New York, N.Y. 10010
U.S.A.

Library of Congress Cataloging-in-Publication Data

IFIP International Conference on Computer Security (4th : 1986 : Monte
-Carlo, Monaco)
Security and protection in information systems : proceedings of
the fourth IFIP International Conference on Computer Security,
IFIP/Sec '86, Monte Carlo, Monaco, 2-4 December, 1986 / edited by
Andre Grissonnanche.
p. cm.
Bibliography: p.
ISBN 0-444-87345-7
1. Computers--Access control--Congresses. 2. Electronic data
processing departments--Security measures--Congresses.
I. Grissonnanche, Andre. II. Title. III. Title: International
Federation for Information Processing.
QA76.9.A25I45 1986
658.4'78--dc19 89-2945
CIP

PRINTED IN THE NETHERLANDS

PREFACE

More and more frequently, information of great commercial, industrial, and financial value, or private information concerning the lives of individuals, is recorded and processed in computers. These systems are more and more often accessible through telecommunications networks, which are generally poorly protected thereby threatening the secrecy, integrity, and availability of information.

Information systems are becoming ideal targets for acts of sabotage, terrorist attacks, redirection of funds, "white collar" computer crime, industrial espionage..., not to mention accidents, such as fire, water damage, breakdown, errors...

The press and public rumour indicate a growing awareness of the financial losses incurred through computer fraud or accidents, and though the reported facts and figures do not yet provide a precise picture of these phenomena, they demonstrate their existence and increasing gravity.

Moreover, new technologies are giving rise to new media and services, such as videotex, teletext, electronic mail, home banking, and remote purchasing. These, in turn, bring up the serious issues of security and legal proof of such transactions.

The additional risks introduced into a company by data processing tools are fundamentally no different than those presented by other manufacturing or business methods, yet some of the characteristics of information systems require particular attention:

– The concentration of vital information in a unique system increases the vulnerability of the company. Distributed systems do not reduce this risk, as long as there are physical or logical links between these systems.

– The immaterial nature of electronic information makes modifications and copying of data extremely hard to detect and trace. Furthermore, the constitution of evidence against the authors of such acts is virtually impossible.

– Legal action in such cases is rendered difficult by the inadequacy of current legislation in this domain.

— The novelty of the phenomenon, in addition to an interest in discretion on the part of the victims, leads to a lack of information which prevents the implementation of appropriate measures. Since reliable information is not available, good investment decisions or insurance policies are not applied.

— These risks are often neglected. The unfortunate result is that many companies today assume risks that are poorly identified and quantified. This situation is, obviously, very dangerous and needs to be remedied as soon as possible.

— Managing information risk requires the implementation of new preventative procedures and systems which, for the most part, have yet to be developed: reliable document authentication, identification of individuals accessing the system, infallible storage media.

— The information risk can also effect the general population, as in the case of sabotage or terrorism aimed at vital information centers, or, in the near future, widespread networks for electronic funds transfer. Accidents, natural catastrophes, and even foreign political pressure regarding delivery of equipment or access to data centers located outside national boundaries must be taken into account in other words, information risk is taken not only by a company or a group of companies, but potentially by the citizens of an entire nation.

Faced with such an imposing and inadequately controlled risk, a realistic approach must be adopted to avoid three principal mistakes:

— indifference or "accidents only happen to other people".

— exaggeration and over dramatisation, creating either panic or disbelief, which generally hinder effective action.

— multiplying technical protection methods which ignore the fundamental aspects of information security distribution or responsibilities and user training.

Companies should consider the security of information management systems as an integral part of their general policy, taking it into account when planning information management strategy. As a prerequisite to information risk management, both the company's managers and personnel should be convinced of the importance of information security. Security issues are too often perceived as restricted to technological, procedures, methods, and equipment designed to protect the organisation.

It should be a state of mind not only for all the employees of a company, but also for its clients, who are equally implicated. This message must be spread throughout the company, using modern communication and training methods. Information security should be presented not as an end in itself, but as a necessary step toward the realisation of the company's objectives.

Companies which have truly confronted these issues generally appoint a Data Security Officer (D.S.O.), whose job it is to advise data processing management on investment choices. However, the final responsibility for these decisions and policies rests with top management, who alone can settle inevitable conflicts between users, system designers, and especially financial management.

The objective of the IFIP/Sec'86 Conference is to present state of the art technology at the international level and to provide examples of real life experiences in the implementation of security systems. Information security techniques, such as cryptography, the Smart card (integrated circuit card), identification techniques, audit methods, risk analysis, and access control, figure among the presentations on the state of the art. Presentation of real life cases and videos have also been programmed to give participants a maximum of support material to sell the concept of information security.

Information security: a challenge? Indeed, but solutions and motivation are certainly not lacking to confront this challenge. The wish of the organisers of this conference is that it provides the necessary practical references for top managers who are determined to act.

André GRISSONNANCHE

Jerôme LOBEL
Honeywell Systems

Good afternoon, Ladies and Gentlemen; and thank you André for inviting me to attend the most important meeting on computer security held in the world this year. I believe that the diversity of subject matter and the fact that there are over 27 countries and 550 participants represented at this meeting automatically accord this degree of importance to this conference.

Although my primary mission here today is to talk about the future for computer security technology in the next five years extracted from my book "Failing the System breakers", I feel compelled to say a few introductory words about why I think that conferences like this one are so important.

First, I am convinced that these meetings focus on a critical international problem, and that is how to bring about an ever more responsible use of computer technology. In other words, conferences like this one should help to assure that the social benefits of computer technology will always exceed the harm that can be caused by its abuse.

This is the third IFIP Security Congress I have attended in the past four years. It is also the third major conference I have attended in less than five weeks in three different parts of the world. I think the statistics alone that come from just these three conferences have a pertinent story to tell and in a way, forecast the future, which as I mentioned is the basic theme of my talk today.

Consider this: in less than 5 weeks almost 2000 computer security professionals have gathered together in three different parts of the world – Stockholm, Sweden; Atlanta, Georgia; Monte Carlo – to discuss their mutual concerns about the increasing problem of computer abuse.

Consider that altogether over 150 different manufacturers, vendors and consultants have displayed their computer security protection products and services at these three meetings.

Even if the number of computer security products and services do not impress you, I would hope that the advances represented in the technology displayed at the meetings do. I know that the technical advances impressed me.

Two weeks ago, I was able to personally test four biometric personal identification systems in less than one hour at one exhibition. More importantly, they all worked, they all satisfied their type 1 and type 2 error capabilities, they were all priced within reason and they all could be ordered for short delivery cycles or were off the shelf products.

It was really a fascinating experience to log on a personal computer first with a system that verified my signature, next with a system that identified my voice, next with a device that validated my fingerprints, and finally with a scanner that authenticated the retinal image of my left eye.

Personal positive identification finally arrived in November 1986. My forecast is that the next five years should be very exciting ones for security providers and users in this area.

At this point, I would like to be more specific about my forecast for computer security for the next five years...

It has always been challenging to me to speculate about the future for computer security technology. For those of us that have been directly involved in this field in some cases for as long as 20 years, I think that there are at least three major trends that have remained consistent during all of this time.

The first trend is that *computer abuse* and crime seem to increase at a rate that is somewhat faster than the rate at which cost-effective solutions come into the market place. The second trend is that the *perceived need* for solutions to computer abuse problems by computer security technologists seems to grow at a faster rate than the perceived need for solutions by most computer users. The third trend is that the payout or profit potential to those organizations that invest in computer security technology always seems to be next year or just around the corner.

So, I have a question for you. What do you think the odds are that these trends will change very much during the next five years? (Or put another way, what do you think are the options?) Who here would be willing to gamble their own money that these trends will reverse themselves or change dramatically during the next half decade. In other words; would you be willing to invest your own friends in researching solutions and developing new products for a market that contains this much uncertainty?

Frankly, I do not have a crystal ball that I can peer into and see what the future holds any more than you do. However, my best guess is that 1987 to 1992 can well be the years during which we will see a reversal of these negative trends.

Why, you might ask am I so optimistic? My answer is simple. Look around you at how many people are in this room right now. Our numbers added to the many other conferences and meetings on this subject held this year alone actually run into the tens of thousands. But even more important than mentioned earlier are the quality and variety of good solutions to computer security that we are seeing in the exhibits. I believe that for the most part, these are really good products, and that during the next five years we will see still more and better product solutions offered.

My primary thought today is that I think we are going to see a much closer alignment of supply and demand for computer security services and products during the next five years. I grant you that the market size and profit potential for suppliers of these services and products might still leave something to be desired — but overall I think — and in fact I am willing to forecast — that the negative trends of the past that have curtailed the purchase and implementation of computer security product solutions — will improve significantly during the next five years. And here, as an example are 3 reports that support my reasons for saying this.

Electronic Security Equipment Demand will Grow

The US market for electronic monitoring and detection equipment totalled almost $1.5 billion in 1985, while consumption of electronic deterrent and the protection equipment was over $700 million. This is one of the conclusions reached in a new report titled: "Recent Developments in Electronic Security Equipment" published by Worltech Reports Inc.

According to the report, many segments of the electronic security equipment market will grow dramatically between 1985 and 1990. Included in this group are biometric access control devices, public key encryption equipment, infrared intrusion sensors, and secure telephones.

Data encryption equipment sales will rise from $76 million in 1985 to $162 million by 1990. The market for dial-up access security devices is estimated to be $91 million by 1990, up from $50 million in 1985 says the report.

Users for Smart Cards to be Studied

New opportunities for users, manufacturers, and suppliers of memory cards will be identified in a study to be sponsored by a number of companies interested in obtaining information that will help them identify, develop, and evaluate market opportunities in memory card systems — devices that combine data processing and information storage within a portable unit such as a plastic credit card.

Memory cards – also called "smart cards" – make it possible to carry large amounts of data easily and conduct electronic transactions in isolated locations without the need for on line computer support. They can be packaged in many forms, including tags, keys, or modules embedded within other products.

While major applications for memory cards have focused on the financial sector, new applications have surfaced in inventory control, medical, security, and telecommunications areas.

Information about these new uses must be coordinated if corporate planners are to make effective business decisions and understand current and future market forces. There are now more than 1 million memory cards of all types in use worldwide, and by 1990 that figure is expected to jump to 50 million.

Access Control Market in Europe

A new *Frost & Sullivan* study forecasts that the total market for access control and identification products in Europe will grow to $1.47 billion by 1995, representing a very healthy increase over 1985's $828.97 million market.

According to the "Access Control & Identification Products Market in Western Europe" (E803), this growth trend is not at odds with the recent market behaviour. The authors note that the steady rise of the dollar relative to European currencies between 1980 and 1985 has made the European market, when viewed in dollars, appear to grow less slowly or even contract, than when viewed in local currencies. In fact the security market as a whole stayed fairly healthy through the recession and will continue to expand as well.

Overall, I believe that these reports are accurate and I personally agree with these directions and conclusions.

The future for computer security during the next five years should be very bright.

I would again like to thank you for the invitation to be your luncheon speaker today, and I will look forward to seeing you all again at the next IFIP Security Conference in Australia in 1988.

CONTENTS

DATA BASES

SECURITY IN ADVANCED APPLICATIONS AND ENVIRONMENTS

NETWORKS 1

CRYPTOGRAPHY 1

AUDIT 1

CRYPTOGRAPHY 2

AUDIT 2

SOFTWARE SECURITY

PRIVACY

CRYPTOGRAPHY 3

SECURITY OF ELECTRONIC FUNDS TRANSFERS 1

NETWORKS 2

FINANCIAL TRANSACTIONS SECURITY

SECURITY OF ELECTRONIC FUNDS TRANSFERS 2
TRASEC (TRAnsmission SECurity)

ARCHITECTURE

COMPUTER CRIME 1

PRACTICAL CASES OF APPLICATION OF RISK ANALYSIS AND REDUCTION METHODS

DISTRIBUTED SYSTEMS

COMPUTER CRIME 2

ACCESS CONTROL

RISK MANAGEMENT

CONTINGENCY PLANNING 1

SMART CARD

POLICY