SECURITY, IFIP/Sec'83

Proceedings of the First Security Conference
Stockholm, Sweden, 16-19 May, 1983

edited by

Viiveke FÅK
Linköping University
Sweden

1983

NORTH-HOLLAND PUBLISHING COMPANY
AMSTERDAM • NEW YORK • OXFORD

ISBN: 0 444 86669 8

Published by:
NORTH-HOLLAND PUBLISHING COMPANY – AMSTERDAM • NEW YORK • OXFORD

Sole distributors for the U.S.A. and Canada:
ELSEVIER SCIENCE PUBLISHING COMPANY, INC.
52 Vanderbilt Avenue
New York, N.Y. 10017

Library of Congress Cataloging in Publication Data
Security Conference (1st : 1983 : Stockholm, Sweden)
Security, IFIP/Sec'83.

"Organized by Swedish Society for Information Processing (SSI) under the auspices of the International Federation for Information Processing (IFIP)"--Half t.p.
1. Computers--Access control--Congresses. 2. Electronic data processing departments--Security measures--Congresses. I. Fåk, Viiveke, 1948- . II. Svenska samfundet för informationsbehandling. III. International Federation for Information Processing. IV. Title.
QA76.9.A25S4 1983 658.4'78 83-8042
ISBN 0-444-86669-8 (Elsevier)

PRINTED IN THE NETHERLANDS

FOREWORD

These Proceedings contain the papers presented at IFIP/Sec'83, IFIP's First Security Conference, held at Stockholm, Sweden, May 16-19, 1983. The Conference was sponsored by the Swedish Society for Information Processing (SSI), by the Swedish Agency for Administrative Development, and by Honeywell Bull AB, Sweden. Registration was 325 persons from over 20 countries.

IFIP/Sec'83 was organized in a very short time frame for an international event of its stature - just over one year. It was prompted by the suggestion to IFIP by SSI that a new IFIP Technical Committee (TC) should be formed for EDP Security. The normal sequence of events might have been to form the TC first and then to have it organize a conference. In this case, the need for a conference seemed most urgent and SSI also had offered to host a meeting. Therefore it was decided to stage a conference and thereby provide a forum to attract professionals in the field, and thus assembled discuss the organization of a technical committee.

Both Program and Organizing Committees were quickly assembled in March, 1982. Every attempt was made to achieve international participation and Program Committee members were chosen from Canada, Finland, Sweden and the United States of America. The Call for Papers was issued in the late summer of 1982 with gratifying results though many authors were not able to respond by the deadline of December 1, 1982. In any event, the preliminary program was set by yearend. Invited Speakers included Jon Bing, Norway; Harry DeMaio, U.S.A.; Jan Freese, Sweden; Jerome Lobel, U.S.A.; and Donn Parker, U.S.A.

The technical program for IFIP/Sec'83 was arranged into eleven areas as described in the INTRODUCTION which follows. Forty-sive sessions were scheduled over the three days available from 13:00 hrs. Monday to noon Thursday, May, 19, 1983. Plenary sessions were held on Monday and Wednesday afternoons for the Invited Speakers and on Thursday morning for a Panel Discussion on the subject "Priorities in Computer Security - Immediate Concerns and Long Range Considerations". Otherwise the program was divided into three streams. A visit to a Backup Centre was included in one session and featured a test of a contingency plan by a medium sized computer centre. All Speakers, invited and for submitted papers, showed up to make their presentations.

Arrangements were made with North-Holland Publishing Company for the printing of preprints and the Editor appointed. Though not totally complete with final texts and all speeches, an impressive volume of some 300 pages was produced and distributed to registrants at the Conference.

The Conference was accommodated very well in the Conference Section of the Stockholm International Fairs. Complementing the Program and Exhibition was a fine social program which featured a reception at City Hall, a banquet at the Operakällaren and a steamship tour. In addition, a special program of sightseeing was arranged for accompanying persons.

Early in the planning, it was realized that considerable financing would be needed and also that Honeywell Bull AB, Sweden, planned to hold a "Top Secret" Conference in Stockholm at about the same time. Subsequently, Honeywell Bull discontinued planning for their conference and agreed to assist with IFIP/Sec'83. Their participation in all aspects of the Conference was most appreciated.

These considerations and the objective of organizing an IFIP Technical Committee caused the Organizing Committee to propose the creation of a sponsors' group or

Steering Group. The Steering Group oversaw all aspects of the Conference including financial audit, and the Chairman of the Steering Group headed the windup panel and the plenary discussion of a possible TC. A large audience of nearly 200 participated in this final session during which IFIP's aims and objectives were described.

The final session closed with the unanimous approval of the audience that:

- a formal proposal be made to IFIP for the formation of a Technical Committee on Security
- two working groups be established immediately in the areas of "Security Management" and "Office Automation Security"
- two conferences be planned for 1984:
  1. a working conference in The Netherlands in May, 1984
  2. a general conference in Canada in September, 1984

Responsibilities were accepted by individuals for these tasks and events.

These conferences, together with the work awaiting the proposed TC and its WG's, provide ambitious objectives for the future.

For the success of IFIP/Sec'83, we thank all those persons and organizations that contributed and worked so hard to make it an outstanding event.

Per Svenonius
Chairman,
Steering Group

Kristian Beckman
Chairman,
Organizing Committee

James Finch
Chairman,
Program Committee

INTRODUCTION

The first decade of computing on a large scale was characterized by the enthusiasm of pioneers. This meant an overwhelming joy as soon as a system started to do anything similar to what it was specified to do. Errors and mishaps were like death and taxes: Most people accepted them as un-avoidable, while the remaining few were constantly baffled by their appearance. The next decade showed that the field had started maturing. One sign was the awareness that computers should not just execute things. They should function properly and reliably. Moreover, erratic behaviour of all kinds could and should be fought. This applies to computers and their work as such as well as to disturbances in the surroundings and their effect on the computers. The original faith in the infallibility of computer stored data has also slowly faded and changed into an awareness of the quality problems involved in the maintenance and use of data bases. By now security has become established as one of those issues in which a computer professional might specialize, just like database management, data communications, programming languages, etc. A clear sign of this is that IFIP is now arranging its first security conference, IFIP/Sec'83.

The subjects of the conference mirror the relevant areas of interest for computer security analysts and others professionally involved in security work. The contributions to the conference have been grouped under session headings. Although the size of each session mirrors only the number of accepted contributions within that area, the headings could serve as a list of what computer security is about. In the order they appear at the conference, these keywords are:

The opening session gives a survey of the broad problems. Computers have grown to both represent and take care of immense values. There is an urgent need not only for direct security measures but for general awareness of the situation. This is not a problem confined to specific organisations. It is not even just a national problem. The effects are of an international scale, and thus the problems are on the same level. Still the problem has not been left unattended. Much has been accomplished already and much is on the verge of being introduced to the public and professionals. And here the public should not be forgotten. Much will be done which the end-user will never be aware of. You notice what happens, but you seldom think of what might have happened but didn't. Computers and computer professionals are there only to serve the end-user. This service shall include security.

Security management. Proper management is the key to success in all enterprises. This is true for security too. No tool is of any use unless it is used in an effective way in the proper context. Security management is the art of knowing what is in the toolbox and when to apply the different tools. It is also the art of knowing what has actually been done, what the effects are, what should be done next and, last but not least, what should be left as it is. All this is treated with different emphasis in the papers.

EDP security - a public concern. Computers play a very important part in every persons life today. Thus society should be concerned about how all these computers work. Society's vulnerability due to computerization has become a common subject of discussions in most developed countries today. Privacy is another important issue within this area. Since it has been intensively discussed for more than a decade, you might think that good solutions have been found by now. Experience, however, shows that in spite of data acts etc., privacy is still endangered in our modern information society. One example of this is the enormous amount of information gathered by public authorities for the benefit of us all. But misuse of these data is not only a threat against the individual's right to privacy. For organisations in a competitive market dissemination of such data might mean extinction. Thus the

responsibility of the public and public institutions is enormous regarding these different matters of security.

Access control is a term which might encompass both a physical right of entry and a logical one. Papers within the session deal with the logical, computer oriented aspect. Access to data, computational services, etc. can be controlled by different methods attacking different problems. A lot of progress has been made in this important area lately. Still the problem is not completely solved for all situations, as all those responsible for security should know.

Office information systems. The market for personal office computers and for networks connecting them is probably the most dynamic of all the areas within the dynamic field of computing today. But office information systems create new problems concerning security. The distribution of both computers, information, systems development, and responsibility makes it necessary to distribute security measures too. This cannot be done by simply transporting old techniques to new sites. The prerequisites of these new systems are entirely different because there is no central authoritative facility, little possibility to seal off secure rooms, limited storage for data and programs, a different risk pattern, etc. Thus new approaches are neccessary.

Facility protection. There is one obvious prerequisite for the maintenance of proper computer service: The existence of a working computer. Thus facility protection is at the very heart of computer security. Some knowledge in this field can be directly taken over from successful protection schemes for any valuable machines. But computers also cause problems which are very different from other fields. Computers are valuable in themselves, vital to the organization, climate sensitive, dependent on constant power supply, fairly likely targets for terrorists, keepers of both secrets and "electronic money", etc. This mixture of characteristics calls for very special skills in those supplying real facility protection.

Education. Without education there will be no security. Security analysts must learn to do their job properly. Managers, auditors, and others must learn enough about computer security to supervise and evaluate what is done within their fields of responsibility. Computer professionals and end users must know their responsibilities and they must be motivated to keep up security. Developments in this field are very recent. Thus there is a great need for massive educational efforts in the field of computer security.

Risk management. The analysis of risk and the evaluation of measures to contain them are very important in any attempt to reach a reasonable level of security. This calls for both evaluation of the existing situation and proper analysis of projects. Conscientious managers have always tried to achieve the desired effect. The tools have, however, been conspiciously lacking. Now risk management and quality assurance are developing as a natural and necessary help in this area.

Audit. Auditors have always been a security resource and this is no less true in the computer age. The changing world puts a constant pressure on auditors to learn about new things. Yet even in our dynamic society the impact of computers is outstanding. The problems facing auditors are immense. Still an auditor who knows the new parts of his trade is an invaluable asset in security work. Close cooperation between auditors and security analysts is neccessary to get the desired results.

Cryptography. Cryptography is an old security technique for information. Nowadays it is closely connected to computers. It offers the only protection against wiretapping, changes of data in transfer and other similar threats. Its use in computer systems has created both new problems and new ideas in the field. Thus the demands of file encryption are very different from those of communications encryption. Asserting that data have not been changed is very different from asserting that they cannot be read by unauthorized persons. Algorithms have to be optimized for the environments where they should serve. Key exchanges must be adjusted to the

demands of the specific system, and the algorithm must be fitted into protocols and other parts of an environmet. The need for computer security has created a lot of acitivity concerning cryptography and its use, and still this seems to be just the beginning.

Contingency planning. When everything has been said and done concerning security, something may still go wrong. There is no such thing as absolute security. Thus there must be a contingency plan in order to ensure the survival of all vital activities as far as possible even when the impossible happens. This is the last but very far from the least important link in the long chain that creates computer security.

Computers and the law. Criminal activity is the classical security threat. Much can be learned from studies of all kinds of crimes which have some connection to computers. But crime, computers and the law interact in ways that are sometimes very strange to the layman. The computers have created such enormous changes in our world that laws are no longer applicable where they should be, or they mean something different from the original intent, or they just cover a situation which has changed completely. Thus the present laws and their interpretation must be adjusted to our computerized world, and those responsible for computer systems must learn what demands law puts on their work.

In this changing world computer security must evolve to support the formal and informal societal framework which we together have created. All professionals in every society must take the responsibility for their part. This is valid for computer security professionals too.

IFIP/Sec'83 has been arranged as a forum for all those who are interested in computer security. Its aim has been to cover all relevant issues. This conference documentation is a unique collection of the latest results from specialists in this new and very active branch of computer science.

ACKNOWLEDGEMENTS

This conference is held under the auspices of IFIP through its Swedish member society SSI. The preparatory work has been shared among the following volunteers.

Steering Group

Per Svenonius, Statskontoret/SAFAD, Chairman
Knut Hernaes, SSI
Anders Rönn, Honeywell Bull AB, Sweden
Kristian Beckman, Organizing Committee Chairman
Johan Essén, Local Arrangements Subcommittee Chairman
James Finch, Program Committee Chairman

Program Committee

James Finch, Cerberus Computer Security, IFIP Trustee, Chairman
Jerome Lobel, Computer Security
Jan Freese, Data Inspection Board, Sweden
Juhani Saari, Savings Banks Inspection of Finland
Viiveke Fåk, University of Linköping, Sweden
Bengt Rudfeldt, The Swedish State Power Board, Sweden

Organizing Committee

Kristian Beckman, SPADAB, Chairman
Birgitta Olsson, SSI
Johan Essén, AB Bofors
Per Hoving, Saab-Scania AB
Bengt Nordqvist, Värnpliktsverket
Jöran Wester, Honeywell Bull AB, Sweden
Rolf Åstrand, Honeywell Bull AB, Sweden

External financial support to the conference has been given by Statskontoret/SAFAD - the Swedish Agency for Administrative Development - and Honeywell Bull AB, Sweden. In addition, Honeywell Bull has discontinued its advanced plans to organize an international EDP Security Conference of its own in favour of this IFIP event.

TABLE OF CONTENTS