Second IFIP International Conference on
Computer Security
Toronto, Ontario, Canada, 10-12 September, 1984

Organized by
the Toronto Section of the
Canadian Information Processing Society
under the auspices of the
International Federation for Information Processing (IFIP)
Technical Committee 11: Security and Protection
in Information Processing Systems

NORTH-HOLLAND
AMSTERDAM • NEW YORK • OXFORD

COMPUTER SECURITY: A Global Challenge

Proceedings of the Second IFIP International Conference
on Computer Security, IFIP/Sec'84
Toronto, Ontario, Canada, 10-12 September, 1984

edited by

James H. FINCH
Cerberus Computer Security Inc.
Canada

and

E. Graham DOUGALL
Comshare Ltd.
Canada

1984

NORTH-HOLLAND
AMSTERDAM • NEW YORK • OXFORD

ISBN: 0 444 87618 9

Published by:
ELSEVIER SCIENCE PUBLISHERS B.V.
P. O. Box 1991
1000 BZ Amsterdam
The Netherlands

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

Library of Congress Cataloging in Publication Data

IFIP International Conference on Computer Security (2nd : 1984 : Toronto, Ont.)
Computer security.

Organized by the Toronto Chapter of the Canadian Information Processing Society under the auspices of the International Federation for Information Processing (IFIP) Technical Committee 11: Security and Protection in Information Processing Systems.
1. Computers--Access control--Congresses. 2. Electronic data processing departments--Security measures--Congresses. I. Finch, James H. II. Dougall, E. Graham. III. International Federation for Information Processing. Technical Committee 11: Security and Protection in Information Processing Systems. IV. Canadian Information Processing Society. Toronto Chapter. V. Title.
QA76.9.A25I45 1984 001.64 84-13802
ISBN 0-444-87618-9

PRINTED IN THE NETHERLANDS

This Volume is dedicated to the memory of
Kristian Beckman of Sweden,
founding Chairman of IFIP Technical Committee 11,
deceased September 16, 1984

PREFACE

This volume contains the 48 papers presented at IFIP/Sec'84 held at the Inn on the Park, Toronto, Canada from September 10 to 12, 1984.

A Global Challenge, theme of the conference, addressed how to confront the increasing problems of computer vulnerability and abuse. Speakers from 10 countries participated and, in addition to the formal plenary and individual sessions, panel discussions were held each day.

IFIP/Sec'84 was the second international computer security conference sponsored by IFIP (the International Federation for Information Processing) — the first having been held in Stockholm in May of 1983. However, it was the first conference held under the auspices of IFIP's new Technical Committee on Security and Protection in Information Processing Systems (TC 11) which was formally established in September, 1983 as a direct result of the Stockholm event.

TC 11 held its first meeting in Toronto immediately prior to IFIP/Sec'84 and was attended by representatives from 13 IFIP member organizations. Plans were discussed for the formation of Working Groups in the areas of security management, office automation security, database security, crypto management and, in addition, during the conference a special meeting was called for all persons interested in computer security in banking.

Dr. Harold J. Highland was appointed Press Relations Officer and North-Holland's journal *Computers & Security* will serve as TC 11's official newsletter. Following a presentation by the Irish Computer Society it was agreed that the third international computer security conference, IFIP/Sec'85, would be held in Dublin from August 12 to 15, 1985.

Regretfully TC 11 Chairman Kristian Beckman, a moving force in IFIP/Sec'83 and in the creation of TC 11, was too ill to attend and subsequently passed away the following weekend. Kristian Beckman will be remembered especially for his tremendous accomplishment in IFIP in a very short time and our deepest sympathy is extended to his family.

We would like to thank all those involved in making IFIP/Sec'84 a success and look forward to meeting next year in Ireland.

James Finch and Graham Dougall

ACKNOWLEDGEMENTS

IFIP/Sec'84 was held under auspices of the International Federation for Information Processing's Technical Committee 11 on Security and Protection in Information Processing Systems through its Canadian member, the Canadian Information Processing Society. The preparatory work was shared among the following volunteers.

Program Committee

Chairman
Jerome Lobel
Honeywell Information Systems, U.S.A.

Kristian Beckman, Beckman & Beckman, Sweden
William Bound, CSC UK Computer Sciences Ltd., U.K.
Richard Koenig, Union Carbide Corp., U.S.A.
Colin C. Rous, Cerberus Computer Security Inc., Canada
Michael B. Wood, The National Computing Centre Ltd., U.K.

Organizing Committee

Chairman
Carol Lipsett
Canadian Imperial Bank of Commerce

Vice-Chairmen

Peter Kingston
Kingston, Goulbourn & Associates Ltd.

E. Graham Dougall
Comshare Limited

Dough Berry, Workers' Compensation Board
Dave Church, Stelco Inc.
Jo-Anne Doyle Knysh, Clarkson Gordon
Marc Duez, Canadian Imperial Bank of Commerce
Bill Eadie, Bank of Montreal
James Finch, Cerberus Computer Security Inc.
Pat Finch, James Finch & Associates Limited
David Greenaway, New York Life Insurance
Tim Haist, Canada Systems Group
Ben Hollander, Gulf Canada Ltd.
Beth Kendall, Ontario Ministry of Labour
Sheila Parsons, Data Security Limited
Francine Pouliot, ADP Dealer Services Ltd.
Steve Tower, Arthur Andersen & Co.
Sally Woodhead, Cerberus Computer Security Inc.

Financial support was provided by the Canadian Information Processing Society's Sections in Toronto and Victoria and by its National Computer Security Special Interest Group.

EDITORS' NOTES

The papers contained in this volume are those actually presented during the Congress. The following changes to papers in the preprints are included in this edition.

Revised Papers

Professional Responsibility for Information Privacy, Isaac L. Auerbach

Implementation Issues for Master Key Distribution and Protected Keyload Procedures, Göran Pagels Fick

Corrections

Formal Verification: Its Purpose and Practice, David A. Bonyun
This paper appeared out of sequence in the preprints. The correct page ordering for the preprints is 159, 163, 160, 161, 162, 164 and 165.

An Application of the Chinese Remainder Theorem to Multiple-Key Encription in Data Base Systems, R.H. Cooper, William Hyslop and Wayne Patterson.

The formula on page 365 of the preprints in step 5 should be as follows:

$$A(x) = T_k(x) \bmod (p, I_k(x))$$

TABLE OF CONTENTS

INTRODUCTION

The stated objective of IFIP/Sec'84 was to address the global challenge of confronting the increasing problems of computer vulnerability and abuse. More specifically, the proliferation of computers and data communication networks is causing major social, economic and political controversy which could have severe long-term consequences worldwide.

It was this theme that provided the intellectually stimulating forum for the distinguished speakers from ten countries and the three hundred and thirty participants from twenty-four countries.

The dramatic official opening of IFIP/Sec'84 by the Right Honourable John B. Aird, Lieutenant-Governor of Ontario, and his accompanying fife and drum corps was followed by greetings from Jim Finch on behalf of the Congress sponsor TC 11 and Jerome Lobel, the Program Chairman. From the Keynote Address by Mr. Isaac Auerbach on 'Professional Responsibility for Information Privacy' to the closing presentation by Martin E. Hellmann on 'Beyond War: Implications for Computer Security and Encryption' the Congress was dynamic, thought-provoking and definitely encompassed perspectives on computer security from around the world.

Similarly, the receptions and social activities provided both the opportunity and the ambiance for all participants to freely exchange ideas and philosophies. IFIP/Sec'84 was truly an enlightening and exciting experience.

As a Canadian, I considered the opportunity to welcome a Congress of this stature to the North American continent for the first time both an honour and a privilege. It was very timely that this event took place in Canada when issues such as computer security and abuse, transborder data flow, and privacy are undergoing extensive examination at all levels of government and industry. Canada and the United States are two countries probably unique in the world in that the physical border is so extensive (approximately 6400 kilometers) and yet basically open in nature. In terms of industry, trade, and technology it is a constant challenge to assure that data, from both the private and public sectors, can be maintained in a secure fashion while simultaneously business requirements are creating communication networks that transform the world into a few millionths of a second. Hence, the *Global Challenge*.

IFIP/Sec'84 was not possible without the support of many people and organizations. I would like to personally thank all the members of the Organizing and Program Committees, the Corporate Sponsors and Congress Exhibitors and in particular our hosts, the Canadian Information Processing Society (CIPS) and the International Federation for Information Processing. Lastly, I would like to wish every success to IFIP/Sec'85 which will be held in Dublin, Ireland in August, 1985.

Carol Lipsett
Chairman, Organizing Committee

PROGRAM'S CHAIRMAN'S ADDRESS

Good morning ladies and gentlemen. It is my pleasure to greet you on behalf of the Program Committee. I would like to initiate our formal program this morning by briefly discussing the Congress objectives with you.

To begin with, I would like to set the stage for a successful conference by describing the main objectives of our meeting.

Basically, there are three:

- First, this conference should be receptive to all insight on how to prevent further abuses of modern information and communications technology.
- Second, this meeting should be a co-operative effort, where ideas and experiences will be shared, so that the end result will be the creation of an international community of interest in computer security.
- And third, our meeting must come to grips with one of the most powerful and permanent forces of all – the force of change.

  For example, it has been said that modern computer security and privacy problems are technology driven. It has been inferred that our new electronic and computer oriented tools may be the cause of the new social, industrial and financial problems.

  Personally, I do not agree with this thesis, and I hope that this will be one of the major issues to be covered by our guest speakers during the meeting.

Before leaving the subject of our meeting objectives, I would like to add a few comments about the first IFIP Computer Security Congress held in Stockholm, Sweden a little over a year ago. Actually that Congress set the pattern for this meeting. It had as its primary objectives:

To arrange "a forum for all those who are interested in computer security";

and second

"To form a new IFIP Technical Committee for EDP security".

It may sound strange that a conference was held before the Committee that normally should sponsor such an activity was formed. Actually, sound reasoning went into

the decision. It was decided that the immediate need for an international congress exceeded the need for an operating Technical Committee.

Technical Committees as you know, normally discuss technical issues or problems, and recommend new guidelines or standards as solutions.

In the case of computer security, the problem that was recognized, was that we were witnessing a world-wide explosion of new computer users as a result of great cost reductions and performance improvements in personal computers and data communications.

Of course, almost all of the old problems of host or mainframe computer abuse are still with us. Unfortunately, the security compromises of hosts today are more serious and more frequent as a result of the increasingly large numbers of personal and other computers that are now capable of communicating with the mainframes.

If you doubt this reality, simply look at the numbers:

> In the U.S. alone, last year we estimated we had 2,230,000 people that had access to over 140,000 main frame computers.

This is about 10% of our population. Also, one out of every ten homes in the U.S. has a home or personal computer installed right now. By 1990, or maybe sooner, over 50% of our population will have some form of computer access.

Obviously, the phenomena I am talking about is not just a U.S. experience. Sooner or later, it will be a world-wide experience. It is just a matter of time.

Why is this so important to computer security professionals? Well, for the same reason that it is important to most computer users:

Computer system functionality without computer security is generally acceptable!

Most of us know that there are normal procedures and automated safeguards available to prevent most computer abuses. The problem as I see it is largely an educational one. After all, would not adequate file back up, a carefully managed encryption system, or a call-up answer back device have prevented many of the abuses that we know about? The big question is why were these known abuse prevention methods not used? And furthermore, what is it going to take to convince computer users that functionality without security is not acceptable?

In a very general way therefore, I think these are the real issues that need to be addressed during our meeting. We are here therefore to share our ideas regarding

ways to prevent the abuse of computer technology. We are also here to learn how to better communicate the importance of implementing safeguards to computer users – regardless of their system size, or country of residence.

I wish to thank you for letting me express my personal desires for this Congress.

Jerome Lobel