

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

UNIVERSITÄTSBIBLIOTHEK
HANNOVER
TECHNISCHE
INFORMATIONSBIBLIOTHEK



1984

NORTH-HOLLAND
AMSTERDAM • NEW YORK • OXFORD

AD 1077 (2)
July 1984

TABLE OF CONTENTS

Preface	vii
Acknowledgements	viii
Editors' Notes	ix
Introduction	xv
Program Chairman's Address	xvii

KEYNOTE SPEAKER

Professional Responsibility for Information Privacy Isaac L. Auerbach (U.S.A.)	3
--	---

INVITED SPEAKERS

The Use of Digital Signatures in Banking Donald W. Davies (U.K.)	13
What about your Legal Parachute when your Data Security Crashes? Jan Freese (Sweden)	23
Equity in Access to Information Calvin C. Gotlieb (Canada)	29
Beyond War: Implications for Computer Security and Encryption Martin E. Hellman (U.S.A.)	41
Some Legal Aspects of Computer Security Susan H. Nycum (U.S.A.)	49
The Future of Trusted Computer Systems Roger R. Schell (U.S.A.)	55
Security Guidelines for the Management of Personal Computing Systems Dennis D. Steinauer (U.S.A.)	69

ACCEPTED PAPERS

SECURITY MANAGEMENT

Safeguards Selection Principles Donn B. Parker (U.S.A.)	83
---	----

Problem Definition : An Essential Prerequisite to the Implementation of Security Measures Robert H. Courtney, Jr. and Mary Anne Todd (U.S.A.)	97
Security and Productivity Edwin M. Jaehne (U.S.A.)	107

ACCESS CONTROL

A Proposal for an Automated Logical Access Control Standard Charles R. Symons (U.K.) and James A. Schweitzer (U.S.A.)	115
Computer System Access Control Using Passwords R. Leonard Brown (U.S.A.)	129
Computer Viruses Fred Cohen (U.S.A.)	143
Selection Process for Security Packages Jan H.P. Eloff (R.S.A.)	159
Incorporating Access Control in Forms Systems Gee Kin Yeo (Singapore)	169
Characteristics of Good One-Way Encryption Functions for Passwords – Some Rules for Creators and Evaluators Viiveke Fåk (Sweden)	189

OPERATING SYSTEMS SECURITY

A Topology for Secure MVS Systems Ronald Paans and I.S. Herschberg (The Netherlands)	195
Measuring Computer System Security Using Software Security Metrics Gerald E. Murine and C.L. (Skip) Carpenter, Jr. (U.S.A.)	207
Formal Verification – Its Purpose and Practice David A. Bonyun (Canada)	217
An Overview of Multics Security Benson I. Margulies (U.S.A.)	225

DATA BASE SECURITY

Some Security Aspects of Decision Support Systems Daniel I. Lawrence (Canada)	239
The Integrity Lock Support Environment Richard D. Graubart and Steve Kramer (U.S.A.)	249

EDP AUDITING

- Integrity Analysis – A Methodology for EDP Audit and Data
Quality Assurance
Maija I. Svanks (Canada) 271
- Retrofitting the EDP Auditor – EDP Security Skill Needs and
Requirements
Robert R. Moeller (U.S.A.) 283

RISK ANALYSIS

- Towards an Expert System for Computer-Facility Certification
John M. Carroll and W.R. Mac Iver (Canada) 293
- A Composite Cost/Benefit/Risk Analysis Methodology
John Miguel (U.S.A.) 307
- The SBA Method – A Method for Testing Vulnerability
Rabbe Wrede (Sweden) 313
- An Automated Method for Assessing the Effectiveness of Computer
Security Safeguards
Suzanne T. Smith and Judy J. Lim (U.S.A.) 321

PHYSICAL SECURITY

- Security Threats and Planning of Computer Centers
Antero Mustonen (Finland) 331
- Data Processing Security and Terrorism – How to Safely Pass Through
the Plumb Years and Inherit a Trade Union Problem: The Italian
Experience
Eugenio Orlandi (Italy) 377

CONTINGENCY PLANNING

- General Electric – An Approach to Disaster Recovery
Douglas D. Walker (U.S.A.) 387
- Industrial Relations and Contingency Planning
J.F. Donovan (Eire) 401

COMPUTER CRIME

- The Programmer's Threat: Cases and Causes
I.S. Herschberg and Ronald Paans (The Netherlands) 409

Introduction to Computer Crime Jay Bloombecker (U.S.A.)	423
Deviancy by Bits and Bytes: Computer Abusers and Control Measures Detman W. Straub Jr. and Cathy Spatz Widon (U.S.A.)	431
Characteristics of the Computer Environment that Provide Opportunities for Crime James E. Miller (U.S.A.)	443
COMMUNICATIONS AND NETWORK SECURITY	
EFT – Systems and Security, Practical Co-Operation between Banks in Finland Lars Arnkil and Juhani Saari (Finland)	451
Security and Privacy in Cellular Telephone Systems Roy Masrani and Thomas P. Keenan (Canada)	457
OFFICE INFORMATION SECURITY	
Access Control Models and Office Structures Giorgio Montini and Franco Sirovich (Italy)	473
Security Management in Office Information Systems Mariagrazia Fugini and Giancarlo Martella (Italy)	487
MICRO, SMALL SYSTEMS AND PERSONAL COMPUTER SECURITY	
Security Considerations in the Small Systems Environment Hal B. Becker (U.S.A.)	501
Data Protection in a Microcomputer Environment Harold J. Highland (U.S.A.)	517
Cause-and-Effect Model for Personal Computers Leroy A. Wickstrom (U.S.A.)	533
The Software Sieve Michael H. Darling (U.S.A.)	539
ENCRYPTION	
An Application of the Chinese Remainder Theorem to Multiple-Key Encryption in Data Base Systems Rodney H. Cooper, William Hyslop and Wayne Patterson (Canada)	553

A High Performance Encryption Algorithm W.E. Madryga (Canada)	557
Implementation Issues for Master Key Distribution and Protected Keyload Procedures Göran Pagels Fick (Sweden)	571