

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

UNIVERSITÄTSBIBLIOTHEK
HANNOVER
TECHNISCHE
INFORMATIONSBIBLIOTHEK

NORTH-HOLLAND
AMSTERDAM • NEW YORK • OXFORD • TOKYO

CONTENTS

Preface	v
-------------------	---

Jerôme Lobel (speech)	vii
---------------------------------	-----

DATA BASES

“Intelligent” Security System for Relational Data Bases S. Miranda and G. Bonfils	1
--	---

Integrity Lock Prototype K.J. Duffy and J. Sullivan	11
--	----

Disclosure Risk and Disclosure Avoidance for Microdata G. Paass	23
--	----

SECURITY IN ADVANCED APPLICATIONS AND ENVIRONMENTS

Security in Advanced Applications and Environments W.H. Murray	33
---	----

NETWORKS 1

Security Practices for Information Systems Networks L.W. Mehrmann and C.T.H. Amery	45
---	----

Addressing the Telephone Intrusion Threat E.F. Troy	55
--	----

CRYPTOGRAPHY 1

Obtaining the Knapsack Public-key Cryptosystem without Using the Superincreasing Sequence Jun Tang	67
--	----

Cryptographic Requirements for Secure Data Communications J.M. Carroll and S. Martin	71
---	----

Trends in Research and Development J.-O. Brüer	79
AUDIT 1	
The Changing Nature of Systems Reviews by Auditors W. List	81
Questions on EDP Security and Auditing for the Top Management L. Dykert.	89
CRYPTOGRAPHY 2	
Computer Virus Containment in Untrusted Computing Environments M.M. Pozzo and T.E. Gray	95
The Security Processor C.R.I.P.T. J.-C. Pailles and M. Girault	105
AUDIT 2	
Penetration Testing as an Audit Tool L. Jolia-Ferrier	119
SOFTWARE SECURITY	
Administrative Policies, Standards and Procedures for Access Control System R. Coderre	125
Control Elements and Restricted Utilities J.H. Sneep	133
Practical Security Aspects of a Large Operating System R.T. Emery	137
Fuzzy Sets: An Answer to the Evaluation of Security Systems? A. Brignone	143
PRIVACY	
Medical Databanks and Privacy Concern M.-C. Lauzanne.	153

Computerized Medical Data – Privacy and Delinquency Issues I. Grandjean	155
CRYPTOGRAPHY 3	
Secure Exchange of Sensitive Data in a Computer Network S. Muftic	165
A New Key Management Approach for Open Communication Environments J.R. Lemire	177
How to Choose Good Cryptographic Protection V. Fåk	189
SECURITY OF ELECTRONIC FUNDS TRANSFERS 1	
The Integrated Circuit Card, Security Key for Corporated-banking: The Example of the Caisse des Dépôts M. Hermary	193
NETWORKS 2	
Implementation of Security Services in the Teletex Service T. Buffenoir	197
A Layered Architecture for Multi-level Security M.S.J. Baxter	205
Use of Expert Systems in the Analysis of Key Management Systems D. Longley and S. Rigby	213
FINANCIAL TRANSACTIONS SECURITY	
Value Transfer Systems Enabling Security and Unobservability H. Bürk and A. Pfitzmann	225
Highly Secure but Untraceable Transactions D. Chaum	239

SECURITY OF ELECTRONIC FUNDS TRANSFERS 2 TRASEC (TRANsmission SECurity)

A Smartcard Application for the Belgian Banks Ph. van Heurck	243
---	-----

Fraud and Failures: A Proposal to Maintain Data Integrity in Case of Incidents A. Monod-Broca	253
---	-----

ARCHITECTURE

DISCOVERY: An Expert System in the Commercial Data Security Environment W.T. Tener	261
--	-----

A Capability Approach to Multi-level Security S. Wiseman	269
---	-----

Performance Aspects of MVS Access Control R. Paans	277
---	-----

COMPUTER CRIME 1

Computer Crime Investigation – The Lessons Learned from Experience P. Stanley	297
--	-----

Prosecutorial Experience with State Computer Crime Laws in the United States S.H. Nycum and D.B. Parker	307
---	-----

Recent Changes in the Nature of Computer-related Crime R.H. Courtney, Jr. and M.-A. Todd	321
---	-----

PRACTICAL CASES OF APPLICATION OF RISK ANALYSIS AND REDUCTION METHODS

MARION AP: A Method for Measuring and Improving Security in E.D.P. Systems: Two Years of Experience E. Baratte	323
--	-----

DISTRIBUTED SYSTEMS

The Creation and Use of Explicit Rights in a Distributed System R.W. Jones	325
Near-term Computer Security Approaches for Distributed DoD Systems W. Neugent	335
Towards the Development of Secure Distributed Systems V.D. Gligor and C. Sekar Chandrasekaran.	345
A Secure Distributed File System Based on Intrusion Tolerance J.-M. Fray, Y. Deswarte and D. Powell.	357

COMPUTER CRIME 2

Let's Use the Right Code... the Code of Ethics! Program for the Prevention of Computer Abuse D. Poullot	367
Consequential Loss from Computer Crime D.B. Parker	375

ACCESS CONTROL

Dynamic Signature Verification M. Achemlal, M. Mourier, G. Lorette and J.P. Bonnefoy	381
An Intelligent Token for Secure Transactions B.J. Chorley and W.L. Price.	391

RISK MANAGEMENT

Expert Systems for Risk Analysis and Crisis Management R. Pollak	401
Developing Security Awareness: Explicative Concepts for Managers and End-users E. Orlandi	411
Risk Management – A New Approach R. Clark.	421

CONTINGENCY PLANNING 1

Contingency Planning	
H. Macé.	429

SMART CARD

International Standardisation of Security Features of the Application of the Integrated Circuit Card by the Financial Sector	
J. Tunstall and J. Boggio.	431

On the Utilisation of Smart Card Technology in High Security Applications	
R.C. Ferreira and J.J. Quisqater	437

About Software Security with CP8 Card	
M. Dupuy, J.-A. Hernandez, R. Joly and C. Nora.	455

POLICY

Security Requirements on Computers and Operating Systems	
J. Essén.	461

Decentralization of Security – A Viable Alternative	
C.L. Lipsett	469