Computer Security & Information Integrity

COMPUTER SECURITY AND INFORMATION INTEGRITY

Proceedings of the Sixth IFIP International Conference on
Computer Security and Information Integrity in our Changing World
IFIP/Sec'90, Espoo (Helsinki), Finland, 23–25 May, 1990

Edited by

KLAUS DITTRICH
Institut für Informatik der
Universität Zürich
Zürich, Switzerland

SEPPO RAUTAKIVI
Finnish Information Processing Association
Espoo, Finland

JUHANI SAARI
International Baseline Security
Helsinki, Finland

1991

NORTH-HOLLAND
AMSTERDAM · NEW YORK · OXFORD · TOKYO

ELSEVIER SCIENCE PUBLISHERS B.V.
Sara Burgerhartstraat 25
P.O. Box 211, 1000 AE Amsterdam, The Netherlands

Distributors for the United States 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 and Information
Integrity in Our Changing World (6th : 1990 : Espoo, Finland)
Computer security and information integrity : proceedings of the
Sixth IFIP International Conference on Computer Security and
Information Integrity in Our Changing World, IFIP/Sec'90, Espoo
(Helsinki), Finland, 23-25 May, 1990 / [edited by] Klaus Dittrich,
Seppo Rautakivi, Juhani Saari.
p. cm.
Includes bibliographical references.
ISBN 0-444-88859-4 (U.S.)
1. Computer security--Congresses. 2. Data protection--Congresses.
I. Dittrich, Klaus. II. Rautakivi, Seppo. III. Saari, Juhani.
IV. Title.
QA76.9.A25I45 1990
005.8'2--dc20

90-26205
CIP

ISBN: 0 444 88859 4

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.

Printed in The Netherlands.

PREFACE

Computer Security and Information Integrity are areas of vital importance whose significance is only just being recognised by the general public. The programme committee for IFP/SEC'90 had an interesting and challenging job selecting papers from among the many submitted, which cover all major aspects of the field and report on the most recent developments. As in several earlier IFIP/Sec conferences, there was a strong emphasis on the practical aspects of providing computer security and information integrity.

IFIP/SEC'90 was the Sixth International Computer Security Conference sponsored by IFIP (International Federation for Information Processing) and under the auspices of Technical Committee, TC 11 (Security and Protection in Information Processing Systems).

We would like to thank all those involved in making IFIP/Sec'90 a success and look forward to meeting next year in Brighton, England.

Klaus Dittrich and Juhani Saari

TABLE OF CONTENTS

Preface v

L. Arnkil and E. Einola
POS Security – State of Art in Finland 1

K. Bauknecht and C. Strauss
Portfolio Techniques to Support Risk Management and Security 9

J.G. Beatson
Security – A Personnel Issue The Importance of Personnel Attitudes and Security Education 29

I. Bentzien
EDP Safety and Usage 39

D. Bonyun and G. Jones
A Knowledge Based Method of Managing Risks in Dynamic Environments 47

K. Brunnstein and S. Fischer-Hübner
Risk Analysis of "Trusted Computer Systems" 71

R.K. Burns
A Relational DBMS Security Policy 89

H. Cnudde
CRYPTEL: The Practical Protection of an Existing Electronic Mail System 107

C. Cresson Wood
Planning as a Means to Achieve Appropriate Data Communications Security 119

R. Dierstein
The Concept of Secure Information Processing Systems and Their Basic Functions 133

J. Dobson
A Methodology for Analysing Human and Computer-Related Issues in Secure Systems 151

W. Fumy and A. Pfau
Asymmetric Authentication Schemes for Smart Cards – Dream or Reality? 171

R. Hackworth
Contingency Planning – Managing the External Impacts of System Security Failures 181

H.J. Highland
Computer Viruses: Factors to Consider Before Purchasing an Anti-Virus Product 189

D.B. Holden
The Digital Distributed System Security Architecture 203

S. Kowalski
Computer Ethics and Computer Abuse: A Longitudinal Study of Swedish University Students 211

M.P.J. Kratz and P.J. Johnston
Managing the Virus Risk 233

K.E. Kristiansen
Information Systems Auditing – A Support to Management 245

K.H. Krueger
Planning for Disaster Recovery in a Multi-Vendor, Networked Computing Environment 255

Y. Le Roux
Technical Criteria for Security Evaluation of Information Technology Products 265

J. Lobel
Proactive Network Risk Management 275

W. Madsen
Data Privacy: Legislation and Intelligence Agency Threats 297

R.R. Moeller
Separation of Duties Audit Concerns and the Clark-Wilson Data Integrity Model 319

S. Muftic
Security in Open Distributed Processing (ODP) Systems 333

R. Paans and H. de Lange
Auditing the SNA/SNI Environment 351

D.B. Parker
Seventeen Information Security Myths Debunked 363

H.P. Rieß
Modeling Security in Distributed Systems 371

B. Sarton and P. Capiteijns
Corporate Information Security Policy... A Paper Tiger? 383

P.M. Stanley
Computer Assisted Investigation of Computer Crime 389

M. Tantam
Trouble Ahead: Information Crime and Jurisdiction 403

L.T. Taylor
Case Tools and Security: A Solution or a Problem? 413

Computer Security and Information Integrity
K. Dittrich, S. Rautakivi and J. Saari (Editors)
Elsevier Science Publishers B.V. (North-Holland)

POS Security - State of Art in Finland

Lars Arnkil
SKOPBANK
P.O. Box 400
SF-00101 HELSINKI
Finland

Esa Einola
Instrumentointi Oy
Sarankulmankatu 20
SF-33900 TAMPERE
Finland

Abstract

Card based Point Of Sale (POS) Systems have been used in Finland since 1986. Finnish banks POS Security standardization during 1984-5 was the major impact for the development of Offline POS-terminals, when in most countries Online developments were in sight at the same time. Security features were based mainly on PIN-verification key protection within the equipment and key distribution, without forgetting inspection and approval functions.

The usage of POS-systems has increased dramatically during the last few years. Over 12.000 POS-terminals, including 600 PIN-based self-service and 6.000 simple terminals were in use by the end of 1989. The reliability of Offline POS-termihals has evidently been the major reason for overall acceptance of this system. Transaction amounts are still increasing, leading to decreasing check amounts.

The Key Management and Distribution System has been ideal for banks and other card issuers. Being technically quite sophisticated, it has caused amazingly few problems to POS-manufacturers. The Key Management itself has been under some development to serve also banks for their own key management needs. Old fashioned key envelopes and safes will vanish from EDP-key-management into the history.

We in Finland believe, Offline POS-system with proper security precautions to be ideal for low volume, limited value transaction network. Offline POS-system could easily be upgraded to Online, if feasible from business point of view. Vice versa, use Online POS-system at offline and you are in trouble.

1 Introduction

We have 5 major banking groups (Savings Banks, Co'operational Banks, and commercial banks, SYP, KOP and PSP) covering over 90 % of the market, plus some 5 minor ones (like STS-Bank, ÅAB, etc.). All big banking groups plus two of the small ones form Finnish Banking Association (FBA). EDP-Security Section, which created the POS Security Regulations, works for the first year under FBA.

As you can see, the number of banking groups, competition, nor the changes of cooperation organizations has not prevented EDP-Security cooperation. The development of POS Security Regulations and the overall management of POS system approval process are still major part of the work of the EDP-Security Section.

Finland's Banks Noteprinting Factory (FBNF) has an important role in the POS technical approval, key management, and distribution functions. In fact Finland's Banks Noteprinting Factory also makes plastic cards, mag. stripe and processor cards for the Finnish market.

Instrumentointi Oy, company which developed the Key Management and Distribution equipment (Keyman System) for FBNF, was also the first to develop secure PIN-PAD according to our security regulations. The second approved PIN-PAD was also made by a Finnish company MHH-Sähkö (MHH-Electric).

Other companies, like Nokia (Ericsson), NCR and Ljungmans have also shown their interest to produce PIN-PADs suitable to our standards. EDACOM (Nokia), IBM, Nixdorf and even NCR have at the moment used already approved PIN-PADs for their POS-systems in Finland.

2 Security Standardization, Approval Process and Key Loading in general

Security regulations for POS System, the result of standardization co-operation, was approved by Joint Delegation of Banks at March 1985.
The development of these regulations was somewhat rapid at the beginning, but stabilized within the first year. Now, after five years, we are planning additions and clarifications to get POS Security regulations version number 4 issued. Upgrading the regulations has, and shall always be made to cause minimum change needs for old equipment, for the delight of manufacturers, shops and even banks.

Main ideas on standardization:

- Customer Identification	PIN, Key Mgmt, Authenticity
- Problem Card Handling	Black lists
- Manipulation Protection	Grey lists, Tx protection, Sigill, MAC
- Offline Risk Minimizing	Value limits, Authoriz. & Online Services
- Physical Security	Security Prom & Protection of keys
- Secure Key Distribution	Standardized key distribution (sec proms)

Regulations are written to give more or less idea what should be secured and protected, leaving the solutions themselves as open as possible.
This could lead into a mess if we wouldn't have official Approval Process with all the negotiations with manufacturers.

Approval Process:

1. Approval of Specifications	by EDP-Sec. Section of FBA
2. Physical Inspection	by FBNF
3. Agreement of Keyman System	by "
4. Final Approval of POS	by EDP-Sec. Section of FBA
5. Key Loading Permissions	from banks directly
6. Key Loading	by Key Guns & stand. proced.

Key Loading:
The manufacturer must first send all the security proms he needs to FBNF for Master Key and Security Prom software loading. FBNF sends loaded proms to manufacturer for building up the POS equipment. When POS equipment is installed physically, the keys for PIN validation are loaded by special Key Guns. Key loading is recorded for auditing purposes. Nowadays we prefer test key loadings, and equipment tests at site, before live keys are loaded. The structure of key loading seems to be ideal.

3 Usage of Cards and POS Systems in Finland

In Finland we have about 3 million cards at use and delivered by banks, which is quite high compared to our population (almost 5 million).
Last ten years has been our plastic card decade. The first Automatic Teller Machines (ATM's) we got 1980 or so. The amount of ATM's increased slowly for some 7 years, but then very rapidly being now over 2.000. One of the highest numbers per population, ATM saturation point cannot be far away.
POS-equipment seems to have even more rapid increase curve than ATM's. First POS installations were made August 1985, and the first installation with PIN-PAD November 1985. By the end of 1989 the amount of PIN-based POS terminals was near 600.
Total amount of POS terminals by the end of 1989 was 12.000 (in 10.000 shops). The trend seems to be, integrated POS systems are used by bigger shops and stores, POS systems based on PC-technology are used by special shops and the most simple ones (even from security point of view) by small shops. POS system saturation point doesn't even seem to be close at all.

Card based transaction amounts were 1988 close to 100 mill/y, of which 16 mill POS transactions. The original estimation for year 1989 was 20 million, but it was 35 million. Best shops have reached 15.000 tx's per month, which seems reasonably high.

Here, as in many other countries, shops and shopkeepers have been blaming banks for the need of POS terminals. Mainly, even in this case, the question has been money. Of course, if the POS system means separate, extra equipment, which doesn't comply to the needs of shopkeepers, the situation could be very difficult. Our POS systems are mainly designed to serve shopkeepers as well. The system itself also guarantees quick and reliable money transfer even between banking groups from customers to shopkeepers accounts. The benefits of this kind of system are evident. The benefits, reliability and standardization of money transfer has been the main reason for good acceptance of POS systems in Finland. Presumably prices have been reasonable too.

The number of customers that are active card users is still growing which means a large potential for POS systems. The development of POS systems, specialized equipment for ticket sale and so on seems to be very interesting and useful for customers.

4 Extracts of POS Security Regulations

Regulations are aimed to ensure that in a POS system:
- the card used meets given standards and that prohibition of use is not imposed upon it
- the person using the card is its legitimate holder
- the sales transaction does not exceed the restrictions defined by the card issuer and the organization responsible for the POS system
- the data contents of the transaction will be transferred to the card issuer/bank in its complete, original form
- it is possible afterwards to reconstruct from the transaction that it has been accepted by the customer either with his/her signature or PIN

Regulations are mandatory for all PIN-based POS systems, but they direct the development of all card based POS systems as well. Next we concentrate on some PIN-based regulation areas, from the security point of view, areas like customer identification, key mgmt, warning registers etc.

POS Security Regulations are underlined here to show you the briefness of the standardization, leaving the security solutions as open as possible, even for the future developments.

Each card reader has its own separate PIN-unit (= PIN-PAD)
By all means, this is important to customers, but it also makes security testing and approval of the system much easier.

Eavesdropping of the PIN-keyboard must be prevented
Easy to say, but the solutions and even the level to aim at is still somewhat unstable.

The card reader sends a request for PIN-check to PIN-unit (PIN-PAD). This request is encrypted with DES-algorithm so that the transaction will include variable information for each transaction.
Here remember, our POS equipment must have Offline PIN-verification capabilities. Same rule stands for the answer from PIN-unit and for Online PIN-verification, if used. Amazingly often POS equipments do not have this feature as standard.

The amount of false PIN-attempts allowed is saved in the PIN-unit as a card issuer parameter.
Finnish POS Key Management System has capability of handling this information by card issuers, and the parameters are loaded with keys. For card issuers this gives even possibilities to vary PIN-attempts by card type.

If the PIN-check gives negative result, the card number will be added into the local warning register (grey register) and the transaction will be transferred to the card issuer with other, normal transactions.
Quite convenient way of keeping control and protecting the lost or stolen cards against criminal PIN-attempts.

No key will be processed unencrypted outside the security module. Exceptions are the CK-Master key and the CK key, which are stored unencrypted during the run of the data communications security program.
Security modules have vital part in the security. Losing keys used for PIN verification could cause enormous expenses for card issuers. Good thing here is, that no person has to handle the keys - they are loaded into security modules from secure Key Guns after appropriate hand shaking procedures. Key Guns are built to meet the POS security regulations and technically are based on same security modules as POS terminals themselves.

Acceptable security modules are; Intel 8751H, -8752H and AMD 9761H and ideally all security proms based on same technique and security level.
Development of security proms during last decade has been very interesting and only this has made it possible to create secure Offline POS-systems. The security of these proms is based on security bit technique, which prevents reading of the contents of the prom very much in the same way as within chip-cards. Of course one must remember, what is now secure and protected, might not be that in the future. That is one good reason not to keep direct PIN keys in POS systems.

Warning register (black list) has a hierarchic structure. Thus all cards of a certain issuer or type can be added in the register with only one update transaction.
This is more or less to make life easier under catastrophe-times.

Warning register has an online connection to the card reader and the warning register-check precedes the local grey register check and the PIN-check.
It is important to do the customer identification in correct order and guarantee the presence of black list at the same time.

The Warning register must have the capacity of saving a minimum of 0.1 percent of the cards accepted by the system.
In practice this has been difficult for the shops and POS-equipment manufacturers, but for other reasons. Shops having their own cards, would like to use bigger share of this black list capacity. Reason for that is (normally) they do not put so much effort on the integrity of their card registers as banks do. POS-manufacturers problems are mainly in the technical (capacity) side.

A card is added to the grey register in two occasions:
1 If the PIN-entries exceed the card type based limit, or
2 If the processing of the transaction is terminated after a minimum of one false PIN-entry.
This guarantees the card PIN-test to be under control, and as also transaction to card issuer is generated, the level of security is rather high.

The card number storage capacity of the grey register must be 1 percent of the system average of daily terminal transactions. The absolute minimum is 10 numbers.
Grey register functions on daily bases, balancing card usability and security needs. During these years we have not had any reason to change this regulation at all.

The transactions are registered in the local log file. This is mandatory at Offline type of systems. The loss of data would be more or less on shopkeepers own responsibility.

Data transfer must be protected using one or more of following methods:

1 Data is transferred in encrypted form

2 A check field, which is verified in the receiving end of the line, is calculated from data with a cryptographic algorithm. Method can be: check field calculated from the file with the Electronic Seal, or using DEA-1 algorithm based ISO DIS 8731, or using authentication fields total sum technique.

3 File transferred in an unencrypted mode by identifying the sender with the user-id (with passwords) and the transfer is verified by return call or equivalent system.

When written 1985, this regulation caused lots of problems. The meaning of this rule has been also to guide future developments into more secure solutions and practice. The upgrading of these regulations shall eventually mean history to the third method in near future. But remember, this regulation concerned only the transfer of transactions, the whole file.

For each payment transaction accepted with a PIN an authentication field is calculated with AUK (authentication key). The algorithm used in the authentication field calculus is the ISO standard proposal DIS 8731 (Banking-Approved Algorithms for Message Authentication, Part 1: DEA-1 Algorithm) All PIN-verified transactions have Message Authentication (MAC) field, which can be verified and authenticated by card issuer.

5 Secure POS System Architecture - Transaction and Key Management

An example of secure POS system architecture is shown in the picture. On the right hand side there is the description of user system, the participants (banks, oil companies etc.) and systems (banking systems, retail shop systems etc.) involved in the transaction management. The left hand side shows the Key Management and Distribution System and the interfaces to the transaction management and equipment.

In fact it is an example of our POS System with terminals and necessary security equipment for self service stands outside and inside petrol station. Pin verification and transaction message authentication is handled by PIN-units. PIN is verified by using PVV-technique and the authentication code is calculated (MAC). Transaction messages are transferred via the systems of Oil companies to card issuer bank. The authenticity of transaction can be verified by using special Authentication Units in banks.

The KEYMAN System is the heart of Key Management and Distribution. Today the application keys are loaded into the security equipment by secure Key Guns. MASTER-keys are loaded into the security processors in a secure environment (FBNF) and shipped to the manufacturer to be assembled into the PIN-unit equipment.

Security software, which handles the MASTER keys and application keys is validated by FBNF loaded into the security processors within KEYMAN environment.

We, by our experience, feel this architecture to be secure, flexible and maintainable for POS systems.

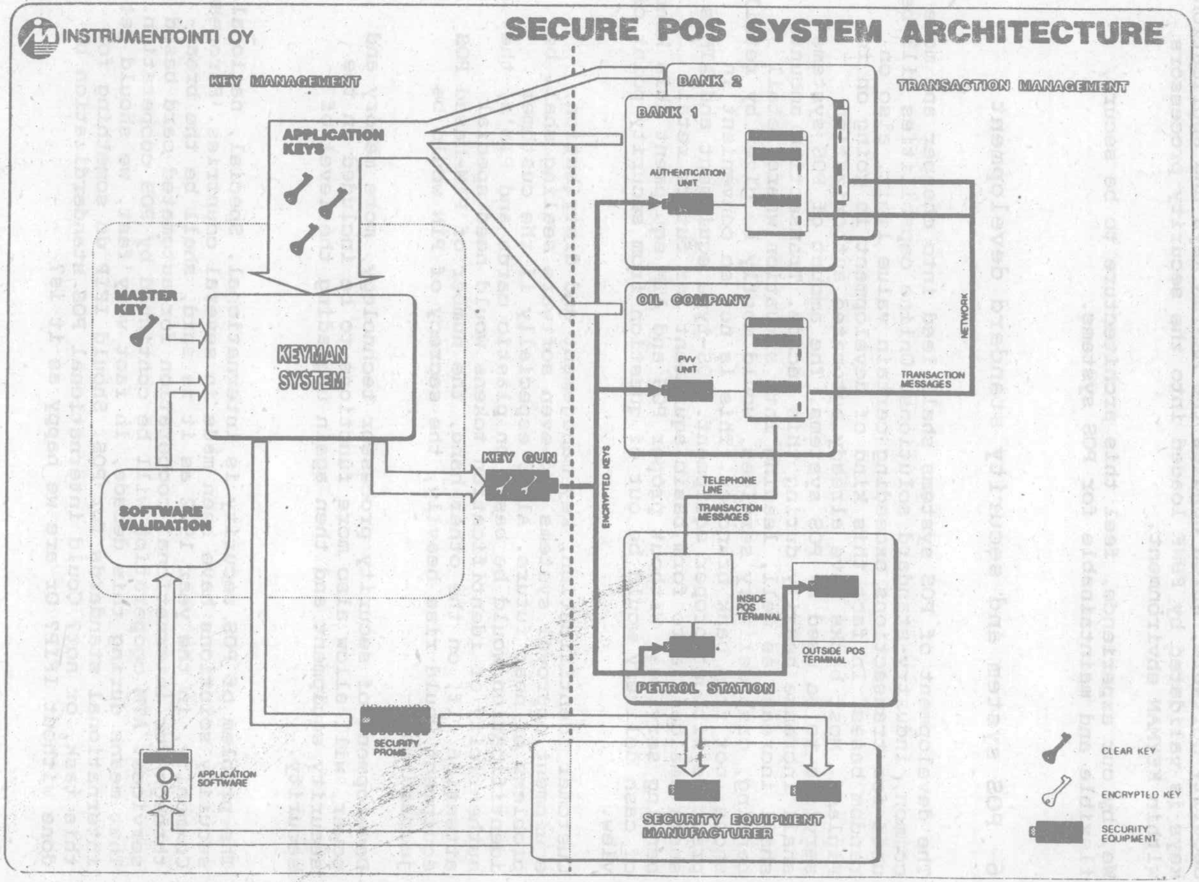
6 POS system and security standard development

The development of POS systems shall lead into cheaper and more common, industry-standard solutions. Online capabilities will be used for transactions exceeding certain value limit, also on random bases. In fact this kind of development is going on in Finland. Most banks have already automated authorization services to be used by POS systems. The amount of POS systems shall increase heavily during this decade. Transaction amounts shall increase as well, leading into situation where retail banking, cash delivery services, would mostly be given by retail shops, not from bank branches. This is not so convenient in practice without proper equipment. POS-type equipment and ATM's shall amalgamate to form basic equipment for future retail banking services. Without proper POS and ATM equipment this kind of cash delivery would be out of question from security point of view.

Customer identification, key management and distribution, equipment approval systems and even software sealing shall be problems of near future. Also, especially if the customer identification would be based on plastic cards and PIN's, the authenticity of identification tokens would need special attention. If, on the other hand, the number of PIN-based POS equipment would rise heavily, the secrecy of PIN would be jeopardized.

Development of security processor technology, more memory and power, will allow also more functions to be included in the security equipment and then again upgrading the level of security.

The problem of POS security is international. Special, national security solutions have been made in several countries. European Community, in the year 1992 as it is said, shall be the breakthrough for international cooperation for automated card based services. ATM cooperation will be continued by POS cooperation. That means during this decade, in fact very fast, we should get international standards for POS. Should IFIP do something for this task, or not? Could international POS standardization be done without IFIP? Or are we happy as it is?


INSTRUMENTOINTI OY
SECURE POS SYSTEM ARCHITECTURE
KEY MANAGEMENT
TRANSACTION MANAGEMENT
APPLICATION KEYS
MASTER KEY
KEYMAN SYSTEM
SOFTWARE VALIDATION
APPLICATION SOFTWARE
SECURITY PROMS
KEY GUN
ENCRYPTED KEYS
BANK 2
BANK 1
AUTHENTICATION UNIT
OIL COMPANY
PVV UNIT
NETWORK
TRANSACTION MESSAGES
TELEPHONE LINE
TRANSACTION MESSAGES
INSIDE POS TERMINAL
OUTSIDE POS TERMINAL
PETROL STATION
SECURITY EQUIPMENT MANUFACTURER
CLEAR KEY
ENCRYPTED KEY
SECURITY EQUIPMENT

Computer Security and Information Integrity
K. Dittrich, S. Rautakivi and J. Saari (Editors)
Elsevier Science Publishers B.V. (North-Holland)
© IFIP, 1991

Portfolio Techniques to Support Risk Management and Security

Kurt Bauknecht
Christine Strauss

Institut für Informatik, Universität Zürich-Irchel
Winterthurerstrasse 190, CH-8057 Zürich
e-mail: bauknecht@ifi.unizh.ch, strauss@ifi.unizh.ch

Abstract

Decisions concerning corporate-wide security levels and activities are frequently taken ad-hoc, as a result of actual damage, sales conversations or a seminar attendance. Resulting strategies and actions therefore are often local, people-dependent and they sometimes provide just low overall security.

The intention of this paper is to introduce and discuss methods and procedures which support and help people involved in decision-making to establish security policies and make relevant provision.

1 Goals

As companies have come to depend increasingly on reliable information technology for their business, aspects of security have become centrally important. In many companies, security policy is limited to implementing measures to limit the damage after a relevant event. Comprehensive security measures seem to be limited to certain particularly sensitive domains such as banks, civil administration, and the military. In many companies there is no security consciousness at all, or there is no concept of what would be adequate and efficient security procedures [Stol 88]. We will try to outline possible strategies for a suitable risk policy and for a practical concept to realize security measures under the aspects of business management. The method chosen will consist in the adaptation and operationalization of Markowitz' portfolio management.

The use of information technology has led to a massive increase in the potential threat to companies: On the one hand new types of threats have developed (malfunctioning hardware, faulty programs), but on the other hand conventional types of threats have become much more important ever since systems have been linked in networks and the number of potential attackers has drastically risen, in parallel with the number of users. In addition, in order to get access to a system, a traditional attacker had to overcome physical obstacles (he had to copy keys or break locks), and he had to be physically present to do so. Today's technical possibilities put much larger amounts of information at risk: An attacker need no longer be physically present, and he has to overcome logical obstacles only. Furthermore, while there are clear legal sanctions against traditional offences, the legal system has not yet caught up entirely with offences touching upon the value of information. The barriers that moral and ethics raise against such offences are low. It is difficult and, in many cases, impossible to actually prove a breach of security, and an attacker often stands good chances to remain anonymous.

Although the scenarios we will use are limited to the domain of information technology, the methods we have designed can be applied to the entire range of security problems.

2 Framework

2.1 The Notion "Risk management"

The notion "risk management" goes back to the institutionalization of central departments whose job it was to deal with organizational aspects of assessing and limiting risks. The notion can mean either the activity itself or the organization performing it. Risk management in the narrow sense means that sector of a company which is concerned exclusively with so-called "pure risks" [Imbo 83]. Pure risks threaten assets, labour potential, or financial potential of a company and are the result of accidental and probable events. Pure risks are limited to events with detrimental consequences to a company, in contradistinction to speculative risks[1] which involve the possibility of both gain and loss[2].

2.2 "Risk" and "Uncertainty"

F.H. Knight draws the distinction between risk and uncertainty on the basis of whether the occurrence of an event in the future can be predicted by means of objective or statistical probabilities (risk), or whether this is not possible (uncertainty) [Knig 57]. This definition of risk assumes that the clusters of conditions, as derived from past experience, will remain valid in the future. Uncertainty can be present only in the case of unique and non-repeatable decisions or, possibly, in the case of degrees of subjective conviction. On the scale of states of knowledge, risk and uncertainty lie between the two extremes "ignorance" and "perfect knowledge"[3] (fig. 1).

[1] H. Griesshaber, Risiko-Management und die Versicherung des Betriebes, Pöching 1977, pp. 33, attributes this distinction to Hellauer, Zwei Fragen aus dem Risikoproblem, in: ZfB, 1928, p.19

[2] Examples for speculative risks are risks of investment, market risks and risks related to the rate of exchange, while examples for pure risks are fire, liability, and loss of information.

[3] A similar approach is taken by [Hert 83]: "A risk situation is argued as one in which a probability distribution for outcomes is made on a meaningful basis, agreed upon by the set of relevant experts, and is, therefore, ´known´. Uncertainty situations arise, therefore, when a consensus agreement amongst the set of experts cannot be achieved, i.e. there is an unknown, undefine probability distribution on the set of outcomes."