# Safety of Computer Control Systems 1989

# SAFETY OF COMPUTER CONTROL SYSTEMS 1989 (SAFECOMP '89)

*Proceedings of the IFAC/IFIP Workshop,*
*Vienna, Austria, 5–7 December 1989*

Edited by

R. GENSER

*Österreichische Bundesbahnen, Vienna, Austria*

E. SCHOITSCH

*Österreichisches Forschungszentrum Seibersdorf, Seibersdorf, Austria*

and

P. KOPACEK

*Johannes Kepler Universität, Linz, Austria*

Published for the

INTERNATIONAL FEDERATION OF AUTOMATIC CONTROL

by

PERGAMON PRESS

OXFORD · NEW YORK · BEIJING · FRANKFURT
SÃO PAULO · SYDNEY · TOKYO · TORONTO

U.K. Pergamon Press plc, Headington Hill Hall, Oxford OX3 0BW, England

U.S.A. Pergamon Press, Inc., Maxwell House, Fairview Park, Elmsford, New York 10523, U.S.A.

PEOPLE'S REPUBLIC OF CHINA Pergamon Press, Room 4037, Qianmen Hotel, Beijing, People's Republic of China

FEDERAL REPUBLIC OF GERMANY Pergamon Press GmbH, Hammerweg 6, D-6242 Kronberg, Federal Republic of Germany

BRAZIL Pergamon Editora Ltda, Rua Eça de Queiros, 346, CEP 04011, Paraiso, São Paulo, Brazil

AUSTRALIA Pergamon Press Australia Pty Ltd., P.O. Box 544, Potts Point, N.S.W. 2011, Australia

JAPAN Pergamon Press, 5th Floor, Matsuoka Central Building, 1-7-1 Nishishinjuku, Shinjuku-ku,
Tokyo 160, Japan

CANADA Pergamon Press Canada Ltd., Suite No. 271, 253 College Street, Toronto, Ontario, Canada M5T 1R5

First edition 1989

**British Library Cataloguing in Publication Data**

Safety of Computer Control Systems.
1. Process control. Applications of computer systems
I. Title II. Genser, R. (Robert) III. Schoitsch, E.
IV. Kopacek, P. (Peter) V. International Federation of
Automatic Control VI. Series
670.42'7

ISBN 0–08–037535–9

*These proceedings were reproduced by means of the photo-offset process using the manuscripts supplied by the authors of the different papers. The manuscripts have been typed using different typewriters and typefaces. The lay-out, figures and tables of some papers did not agree completely with the standard requirements: consequently the reproduction does not display complete uniformity. To ensure rapid publication this discrepancy could not be changed: nor could the English be checked completely. Therefore, the readers are asked to excuse any deficiencies of this publication which may be due to the above mentioned reasons.*

*The Editors*

*Printed in Great Britain by BPCC Wheatons Ltd, Exeter*

# IFAC/IFIP WORKSHOP ON SAFETY OF COMPUTER CONTROL SYSTEMS (SAFECOMP '89)

*Sponsored by*
IFAC – International Federation of Automatic Control TC on Computers

*Co-sponsored by*
IFIP – International Federation for Information Processing
Working Group WG 5.4 Computerized Process Control
IFAC – TC on Economic and Management Systems (EMSCOM)
IFAC – TC on Systems Engineering (SECOM)
EWICS –European Workshop on Industrial Computer Systems TC7 (Safety, Security and Reliability)
EWICS TC 7 was partly supported by Directorate-General XIII of the European Community
ÖCG – Österreichische Computer-Gesellschaft
ÖVE – Österreichischer Verband für Elektrotechnik

*Organized by*
Austrian Center for Productivity and Efficiency (ÖPWZ), Vienna

*Patronage*
Federal Minister of Public Economy and Transport

*International Programme Committee*
R. Genser, Austria (Chairman)
S. Bologna, Italy
L. Boullart, Belgium
G. Dahll, Norway
B. K. Daniels, UK
W. Ehrenberger, FRG
P. Elzer, FRG
H. Frey, Switzerland
P. Kopacek, Austria
R. Lauber, FRG
N. Leveson, USA
L. Motus, USSR
M. Pelegrin, France
W. J. Quirk, UK
J. M. A. Rata, France
B. Runge, Denmark
G. H. Schildt, Austria
E. Schoitsch, Austria
L. Sintonen, Finland
B. Sterner, Sweden
R. Yunker, USA
J. Zalewski, Poland

*National Organizing Committee*
P. Kopacek (Chairman)
J. Haehnel (Secretary)
H. P. Berger
R. Genser
E. Schoitsch
W. Stejskal

# PREFACE

This seventh SAFECOMP workshop deals with safety related applications of industrial computer systems. Such systems are used in transportation, production industry, power plants, medical and emergency systems.

The objective is to reduce the potential to injure or kill people, lose property or cause hazard to the environment. Methods found for improving safety of systems can fit also for reducing risk in case of product liability.

New aspects have to be considered because of the extension of applications to electronic data interchange for trade and transport (EDI) and to computer integrated manufactoring using distributed systems and wide area telecommunication networks. At SAFECOMP'89 in Vienna therefore a survey on 'means and measures for data security' is given and an invited session on 'electronic business and banking - which security aspects do matter' is arranged.

According to the objectives of the SAFECOMP series the papers in this workshop cover standardization aspects, specification, verification, validation, testing and modelling in safety related systems. The advantages and limits of using diversity are investigated further. A special session is devoted to the application of electronics in safety systems of railways.

It should be pointed out that the spirit of the Purdue Workshop has stimulated the Commission of the European Communities in 1974 to support a development which is now carried out by the Technical Committee on Safety, Security and Reliability (TC7) of the European Workshop on Industrial Computer Systems (EWICS). The emphasis was on the transfer of knowledge to reasonable applications of electronics in safety related systems between researchers and developers, between users and scientists, and between different modes of application areas. The reason for the success of EWICS TC7 was that the experts of different fields had been brought together with the objective to find solutions for problems and not to administer the problems only. The goal to be achieved was the production and evaluation of guidelines and standards for smoothing the transfer of new technologies and solutions to applications, as well as for improving the efficiency of such projects for safety related systems. That this approach is recognized as a need may be realized by the increase of numbers of active TC7 members who have meetings on regular terms four times a year for intensive practical work for 3 to 5 days, and this continues although the external support was reduced.

The editors would like to thank all, who have devoted their work to SAFECOMP'89 and made it possible to prepare this volume.

We have to be aware of the fact that the critical attention,which the public is paying to many technical fields, will turn to information technology in the same manner as fast as more and more safety critical or privacy matters of every day life are affected. May this event be a further valuable contribution to the improvement of safety, which is an urgent need for humans and environment.

Robert Genser
Österreichische Bundesbahnen

Erwin Schoitsch
Österreichisches Forschungszentrum Seibersdorf

Peter Kopacek
Johannes Kepler Universität in Linz

# CONTENTS

## SURVEY SESSION

Chaired by R. Genser

## INVITED SESSION -

Chaired by L. Sintonen

## SESSION 1 - ASPECTS OF STANDARDS

Chaired by J.M.A. Rata

## SESSION 2 - SOFTWARE DELIVERY AND REQUIREMENTS

Chaired by E. Scholtsch

## SESSION 3 - APPROACH IN RAILWAYS

Chaired by B.J. Sterner

## SESSION 4 - VERIFICATION, VALIDATION AND TESTING

Chaired by W. Ehrenberger

## SESSION 5 - MODELS

Chaired by S. Bologna

## SESSION 6 - DIVERSITY AND FAULT TOLERANCE

Chaired by H. Kopetz

# MEANS AND MEASURES FOR DATA SECURITY

**O. J. Horak**

*Armed Forces Data Processing Agency, Stiftgasse 2a, A–1070 Wien, Austria*

Abstract. Information represented by data has become the fourth production factor beside estate, labor and capital. Therefore it needs protection to achieve data security containing the main items data privacy (or data confidentiality), data integrity, data availability and access control. Providing data security demands an overall security concept or security policy based on physical, logical and organizational security measures. Security threats and counteracting by security services, e.g. authentication together with the aforementioned security main items, and security mechanisms especially encipherment are discussed.
Basic ideas on cryptography, important cryptographic algorithms and aspects on management of cryptographic keys are given. Furthermore some fundamentals an data disclosure by unintended but physically caused emanation of signals carrying information known under the term Tempest are dealt with.

Keywords. Data security; data privacy; data confidentiality; data integrity; data availability; access control; authentcation; encipherment; cryptography; Tempest; electromagnetic interference.

## INTRODUCTION

Data are the logical and technical representation of information which has become the fourth production factor beside labor, estate and capital. Therefore today information is as important as the other factors and has to be protected against misuse, distortion, damage, loss etc. That means data, or more exactly spoken information, has to be kept secure. Despite the better term "Information Security" the expression "Data Security", coming from the area of data processing, is used here too, synonymously with information security.

There exist many definitions for "Data Security" with different content but till now no one in standardized form. Analyzing some definitions four main items for it can be found (Price, 1988):

- Data privacy
- Data integrity
- Data availability
- Access control.

To refer to threats data should be protected against and to the just mentioned main items two security attributes are to be observed:

- Secrecy
- Authenticity.

This is especially true for cryptographic security systems where these attributes additionally are independent. Secrecy is fundamental for data privacy and helps by providing data integrity because of difficulties for manipulating data. Secrecy, e.g. obtained by encryption also supports access control. In this case a private cryptographic key has a similar function as a personal identification number (PIN). In equal manner a private cryptographic key contributes to authenticity by corroborating that the source of data received is as claimed (data origin authentication) and that a peer entity in an association is the one claimed (peer-entity authentication). Further details can be found in the OSI "Security Architecture" described in part 2 of the ISO "Basic Reference Model for Open System Interconnection" (ISO 7498-2, 1989).

Providing data security requires measures in the scope of an overall security concept or security policy based on three "Pillars of Security" (Caflisch and Rueppel, 1987):

- Physical security measures, i.e. configuration, position and condition of buildings, design and configuration of equipment, installation of security areas,
- Logical security measures, i.e. cryptological algorithms and protocols for data communications, data storage and personal authentication; security management for logging, authorization and cryptographic keys.
- Organizational security measures, i.e. authorization of users, classification of data, guard and supervision of rooms and equipment.

One of the most important points for a security concept is that all means and measures are well-balanced. A predomination of the one or other part is useless, the chain is as strong as the weakest chain-link!

## SECURITY THREATS

Threats and dangers to data security are manifold and touch often more than one of the four main items simultaneously. Therefore protection measures are necessary out of more than one of the three "Pillars of Security". This will be obvious on the example of access control: Normally a security area (physical security measure) has the same importance as logging (logical security measure) and authorization of legitimate users (organizational security measure).

Concerning security threats is distinguished between intentional and unintentional threats on the one hand and on the other hand between threats against the data itself and the data processing environment consisting of communication and data processing services as well as equipment and facilities. Intentional threats need always an opponent or attacker, aiming at theft, fraud, manipulation or misuse of data etc., usually to achieve an advantage or aiming at circumvention of security measures for getting access to data. All these threats need disclosed data in plain. Disclosure can happen by access from an insider or from an outsider by tampering or interception of communication. Furthermore, attacks against data are done by damaging or distorting to produce negative effects for the data owner as a kind of sabotage. Similarly the data processing environment can be attacked. Therefore in the area of intentional threats between passive and active threats can be distinguished. While the former, if realized, would not result in any modification to any information contained in the system, e.g. passive wiretapping to observe information, active threats to a system involve the alteration of information contained in the system, or changes to the state or operation of the system. An example for the latter is a malicious change to the routing tables of a system by an unauthorized user. Some specific types of attacks are masquerade, replay, modification of messages, denial of services, virus, trapdoor and Trojan Horse.

Unintentional or accidental threats are those that exists with no premeditated intent. They occur accidentally or permanent and can be caused by "natural enemies" like power failure, system malfunctions, software bugs, dirt and dust, radiation or generally by force majeure as well as for technological and physical reasons. In the following the latter kind of aspects is emphasized.

As mentioned before disclosure of data is very dangerous because of opponents possibilities. For physical reasons data disclosure occurs automatically in data communication over radio, radio links, satellite links etc. which can be intercepted easily. In some countries (for example Austria) possession and operation of receivers needs approved equipment suitable only for special and limited frequency areas. It is prohibited by the Telecommunication Law (Fernmeldegesetz) to possess and operate equipment for other frequency areas. Though this gives a certain amount of protection against illegal interception, this measure is inefficient outside of the country and especially against offenders.

An other not so obvious and well-known source of data disclosure is the unintended but physically caused emanation of electromagnetic energy from data processing equipment which can be received with slightly modified standard equipment without physical connection to the data source. This phenomenon known under the term TEMPEST will be mentioned in a following chapter.

## SECURITY SERVICES AND SECURITY MECHANISMS

The most elaborated treatise on security for data processing and computer systems is surely the already cited "Security Architecture" for the OSI reference model (ISO 7498-2, 1989) which is an international standard too. With the purpose to allow data communications between different computer systems this reference model proposes a communication architecture with seven layers to make the systems "open" (ISO 7498, 1984):

- Layer 7: Application
- Layer 6: Presentation
- Layer 5: Session
- Layer 4: Transport
- Layer 3: Network
- Layer 2: Data-link
- Layer 1: Physical

Communication between the layers is controlled by interfaces, and between the equivalent layers of open systems by peer protocols. Specially designed for this reference model is the "Security Architecture" which is appended to this ISO-Standard as part 2. Concerning Security in this part 2 it is distinguished between "security services" and "security mechanisms". The security services mentioned in ISO 7498-2 differs slightly from that listed in the introduction. They are:

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Non-repudiation.

The fifth service is rather important for legal or commercial reasons and is not related directly with data security in a narrow sense. The main difference seems to lie in the services "authentication" and "data availability" but looking deeper, both are found implicitly in the other listed three services. Concerning privacy and confidentiality it is only a question of agreement to prefer the one or the other. To fulfill these security services ISO 7498-2 defines eight "Specific Security Mechanisms":

- Encipherment
- Digital signature mechanisms
- Access control mechanisms
- Data integrity mechanisms
- Authentication exchange mechanisms
- Traffic padding mechanisms
- Routing control mechanisms
- Notarization mechanisms

and five "Pervasive Security Mechanisms":

- Trusted functionality
- Security labels
- Event detection
- Security audit control
- Security recovery

Services, mechanisms and layers are standing in defined relationship. ISO 7498-2 shows these relations in two tables and a detailed description for each layer.

## DATA PRIVACY AND DATA INTEGRITY

Data privacy implies the property of preventing disclosure of data or information to unauthorized parties. In principle this can be accomplished with a "locked box" or by making information unreadable by encypherment (encryption). Generally the term data privacy is used for protection of personal data as a task of social policy to protect the personality rights of human beings against consequences of data misuse and total acquisition of his individual data by manual and automatic data processing (Csikai, 1985). Outcomes of this task are Data Privacy Laws (Datenschutzgesetze) enacted already in some countries. In several data privacy laws protection is not limited only to physical persons but include legal personalities like societies or companies. In a broad sense data privacy is sometimes extended to protection for all data where misuse has to be stopped to avoid impairment of foreign and own interests worthy of protection (Kassel and Strnad, 1978). Part of data privacy is "Data Confidentiality", defined as a service for the protection of data from unauthorized disclosure (ISO 7498-2, 1989).

Data integrity implies the prevention of undetected and unauthorized alteration of data. Therefore a data integrity service counter active threats. It is frequently not possible to prevent unauthorized alteration also if cryptographic protection means are used. In this case the opponent only is unable to do alteration aiming at specific changed data, e.g. for the purpose of misuse, fraud etc. But he can achieve disturbance, destruction and occasionally consequential damage. Except the last case where alteration is obvious it is usually possible to take measures ensuring that at least any such alteration is detected. Such measures can be based for example on so called "Hash Functions" which have a similar role as parity bits but are far more complex than these. The results of hash functions are then protected by encryption.

Data integrity is very essential in data communications with a connection between two entities. On a connection, where at the start of the connection a peer entity authentication service and during the life of the connection a data integrity service is used, they jointly provide for the corroboration of the source of all data units transferred on the connection, the integrity of those data units and may additionally provide for the detection of duplication of data units e.g. by the use of sequence numbers. There exist different forms of data integrity depending on the kind of communication system. Mainly it is to distinguish between connection-mode transmission and connectionless-mode transmission. While the meaning of the former mode is clear the latter needs some explanation. In principle in this mode a unit of data is transmitted in a single self-contained operation without establishing, maintaining and releasing a connection. Other terms formerly used in the literature are message mode, datagram, transaction mode and connection-free mode. A practical example for connection-less mode transmission is the communication via a packet switching network e.g. DATEX P according to the CCITT recommendation X.25. Furthermore two sizes of extent for data integrity services can be obtained. The greater one covers all user-data the smaller one only selected fields within the user data (Selective Field Integrity). Additional details can be found in the "Security Architecture" (ISO 7498-2, 1989).

## DATA AVAILABILITY AND ACCESS CONTROL

As defined by Price (1988) data availability implies the ability to prevent interference with the data system by third parties designed to deny service to legitimate users. That makes clear that data availability is not identical with system availability but the latter is an unconditional requirement for the former. Generally in data processing the term availability is defined as the degree to which a system or resource is ready when needed to process data (Csikai, 1985). Similar to data security the term data availability is defined in different ways. An other example (Murray, 1988) opposite to that of Price sounds:

> Data may be said to be available when it is in the right place, at the right time and in the right form. This usually requires redundancy of both data and the delivery mechanisms.

While the definition of Price for availability is in a negative form: "*... to prevent interference ... to deny ...*" a third definition contained in the "Security Architecture" (ISO 7498-2, 1989) sounds positive:

> Availability is the property of being accessible and useable upon demand by an authorized entity.

All these definitions show that data availability consists of two different parts:

- Data and services have to be made available to authorized users,
- Data and services have to be protected against denial by other parties.

Denial of service is an attack and is one of the active threats as The following description of such an attack may be found in subchapter A.2.5.4 of ISO 7498-2:

> Denial of service occurs when an entity fails to perform its proper function or acts in a way that prevents other entities from performing their proper function. The attack may be general, as when an entity suppresses all messages, or there may be a specific target, as when an entity suppresses all messages directed to a particular destination, such as the security audit service. The attack may involve suppressing traffic as described in this example or it may generate extra traffic. It is also possible to generate messages intended to disrupt the operation of the network, especially if the network has relay entities that make routing decisions based upon status reports received from other relay entities.

The example shows clearly that data availability fails if the service "data traffic" is disturbed. It shows further that data availability can not succeed with only one security mechanism as for example data privacy can where already encryption covers nearly all requirements. The protection part of data availability described in the ISO-example demands at least traffic confidentiality, access control and data encryption to avoid such attacks. In principle there is no general or all-round solution for data availability. Adaptation of the security mechanisms to the special realities and requirements is necessary and can be realized only after detailed studies.

Access control was one of the very first security mechanisms in data processing, allowing access by authorized parties and denying it to others. Access control is obviously relevant to achievement of data privacy, data integrity and data availability and is itself of great importance. ISO 7498-2 defines it as "The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner", complemented with a definition for an access control list: "A list of entities, together with their access rights, which are authorized to have access to a resource" and furthermore with a detailed description of access control mechanisms.

Access control affects physical and logical access to data, data processing resources and services as well as data processing equipment and data processing areas. Concerning security mechanisms mentioned here, logical measures of access control are to discuss. Like data availability access control shows two parts:

- A permission part: an authorized user gets the possibility for access to data or resources, limited to that users security profile,
- A supervision part: any access is protocoled in a log and checked on admissibility.

Access control as a security mechanism can be part of a complete system e.g. as proposed in the "Security Architecture" of OSI or as a add-on solution offered as software product like RACF, TOP SECRET, ACF-2 etc. for mainframes and many products for personal computers. All activities of access control mechanisms together provide for the demanded access control service.

## CRYPTOGRAPHY

From the beginning of human culture where human beings have started to record something with characters what the memory could not keep but should be kept — unintelligible for others — beginning of secret writing can be observed. Writing itself originally known only to some insiders offered protection as long as the rest of people were ignorant of this art. With growing culture and education new means and ways for protection have to be found. Starting with stipulated secret signs secret writing followed by *concatenating them*. Next step was the use of normal letters of the alphabet in changed arrangement (transposition or permutation of letters) or substitution of letters by others. In that way first ciphers have been developed and the art of enciphering or encryption was founded. David Kahn mentioned this phase of development very detailed in the chapter titled "The First 3,000 Years" of his famous book "The Codebreakers" (Kahn, 1967). There he showed as an early example for transposition ciphers the first system of military cryptography and earliest known cryptographic apparatus the "Skýtala" ($\Sigma\kappa\acute{\upsilon}\vartheta\alpha\lambda\alpha$) employed about in the fifth century B.C. by the Spartans, the most warlike of the Greeks. It consists of a wooden rod with an agreed diameter wound round with a tape of parchment where the message was written in axial direction. The meaning of the letters on the unwound tape could be reconstructed only with knowledge of the principle and the diameter of the rod. Examples for *substitution ciphers* also described by Kahn (1967) are the Caesar-cipher used by Gallius Julius Caesar (100-44 B.C.) consisting of a alphabet shift of three places so that stands D for a, E for b, ..., B for y and C for z, using the modern 26-letter alphabet. Furthermore he described the Polybius Square (Polybius; $\Pi o\lambda\acute{\upsilon}\beta\iota o\varsigma$; 200-120 B.C.) where a 25-letter alphabet (e.g. a modern alphabet with i and j as one character) is arranged in a 5 × 5 square e.g. starting in the upper left corner and filling row by row from left to right, each row and column numbered from 1 to 5. Any of the 25 letters are then substituted by a two digit number for example 11 for a, 12 for b, ..., 21 for f, 22 for g, and so on.

Development of secret writing proceeds. In the 16th century first printed books describing cryptographic methods and supporting cipher equipment came up for example Trithemius (1518), Bellaso (1555), Porta (1563) and Viginère (1586). Means and Measures improved, refined and supplemented step by step till to the 19th and 20th century where enciphering and deciphering became automated first by mechanical and later by electromechanical cipher machines. In the middle of this century first electronic cipher equipment appeared followed by encryption means as part of electronic systems in hardware as integrated circuits or as software algorithms.

Investigating cryptographic means and measures any of them includes two principal elements:

- An algorithm, generally defined as a finite set of well-defined rules for the solution of a problem in a finite number of steps, and
- A secret element, called the cryptographic key.

This fact has been postulated already by Kerckhoffs (1883) who stated as the second of his six deduced specific requirements for cryptographic systems that the algorithm (or the "system" as he called it) must not be secret. Adapted to the technological advances of today this requirement is as true as at his time and is now known as the "basic assumption of (military) cryptography". Especially in cases where an algorithm is used by many subscribers it must not be secret because of problems in providing confidentiality for the algorithm if it would be secret.

The art of secret writing has gone through a transformation during the centuries and has changed from an art to a science called cryptology with its branches cryptography and cryptanalysis. G.J. Simmons (1987) has given the following definition and explanation for this terms which implicitly also contains Kerckhoffs' second specific requirement:

> "Cryptology" (from the Greek *κϱυπτός* [kryptós], "hidden", and *λόγος* [lógos], "word") is the science of secure (generally secret) communications. This security obtains from legitimate users, the transmitter and the receiver, being able to transform information into a cipher by virtue of a key i.e., a piece of information known only to them. Although the cipher is inscrutable and often unforgeable to anyone without this secret key, the authorized receiver can either decrypt the cipher to recover the hidden information or verify that is was sent in all likelihood by someone posessing the key. "Cryptography" (from the Greek kryptós and *γϱαφεῖν* [grapheĩn], "to write") is the study of the principles and techniques by which information can be concealed in ciphers and later revealed by legitimate users employing the secret key, but in which it is either impossible or computationally infeasible for an unauthorized person to do so. "Cryptanalysis" (from the Greek kryptós and *αναλυεῖν* [analyeĩn], "to loosen" or "to untie") is the science (and art) of recovering information from ciphers without knowledge of the key. Cryptology is often - and mistakenly - considered a synonym for cryptography and occasionally for cryptanalysis, as in the popular solution of cryptograms or ciphers, but specialists in the field have for years adopted the convention that cryptology is the more inclusive term encompassing both cryptography and cryptanalysis.
>
> Cryptography was concerned initially with providing secrecy for written messages. Its principles apply equally well, however, to securing data flow between computers, to digitized speech, and to encrypting facsimile and television signals. Most communications satellites, for example, routinely encrypt the data flow to and from ground stations to provide both privacy and security for their subscribers. Because of this broadened interpretation of cryptography, the field of cryptanalysis has also been enlarged to include the recovery of information from ciphers concealing any form of data.

Knowing now what cryptology, cryptography, cryptanalysis and the difference between them is, cryptography has to be discussed in some details. Concerning the cryptographic key two different types of systems are possible:

- Symmetrical or secret-key systems: enciphering and deciphering take place with identical keys which have to be kept absolutely secret,
- Asymmetrical or public-key systems: enciphering and deciphering is accomplished with different keys. Normally the former is published, the latter is kept secret as a personal private key.

Concerning the ciphering technique also two kinds of systems exists:

- Stream cipher systems: a continuous data stream is processed sequentially bit by bit,
- Block cipher systems: data blocks of defined length are processed as single units one after the other, all bits of each block at the same time in parallel.

Concerning basic ciphering methods three types occurs. The first two have been already mentioned:

- Substitution cipher systems,
- Transposition or permutation cipher systems,
- Product cipher systems: they combine in one algorithm substitutions and permutations.

Substitution cipher systems use frequently the Vernam principle (Vernam, 1926). With this method each bit of plain information or plaintext is "mixed" with one bit of key sequence to get the ciphered information or ciphertext. Mixing is done by addition modulo 2, realized by an ex-or function (EXOR). If the key sequence is absolutely random and used only once such a system is unbreakable. For technical and organizational reasons instead of random, only pseudo-random key sequences are used. Consequence of this limitation is an "only" computational secure system with calculated security of up to many thousand of years.

Secret key systems can be constructed as stream or as block cipher systems. They have the advantage of nearly unlimited processing speed. Throughput in the size of megabits per second is no problem. Stream cipher systems with Vernam's principle need a key sequence in the length of the plaintext identically for sender and receiver. Vernam solved this problem for teletype machines with pairs of randomly punched paper tapes. Today pairs of hard-disks, diskettes or tape cassettes with random bitstreams are used for top-secret applications. These carrier of key sequence have to be distributed to the autorized receiver in secure manner to keep it secret (key distribution). The length of plaintext to be ciphered is therefore limited to the length of key sequence available. To overcome this limit pseudo-random bitstreams are produced identically on both sides with a key generator, containing a complex generation algorithm and controlled by the (much shorter) secret key (key extension). The strength of the system depends now on the quality of the generator algorithm , the quality of the produced key sequence and also on the length of the cryptographic key.

Block cipher systems are common in data processing environment because of the block-like structure of processed data. The most well-known block cipher algorithm is the Data Encryption Standard (DES), standardized in the USA (NBS, 1977). It is a product cipher algorithm with 16 rounds and a combination of substitutions and permutations of 64-bit blocks. Key length is 56 bit (plus 8 parity bits). DES with its published algorithm is a typical example for Kerckhoffs' second specific requirement! Realizations of DES are available both as integrated circuits and as software products with different categories of performance and processing speed.

The most complex task with secret key systems is the key management, i.e. the secure generation, distribution, storage and deletion of cryptographic keys. Complexity grows with the increasing number of subscribers and the size of the network. Different examples can be found in the literature on this subject like Konheim (1981) or Meyer and

Matyas (1982). Many key management schemes have been proposed but none of them satisfied totally. Therefore cryptologists and scientists were looking for better solutions or new cryptographic systems without the need of key distribution. An answer to this effort seems to be found with invention of asymmetrical or public-key systems. Base of them are mathematical one-way functions defined as follows: $f(x)$ is a *One-way Function* if

(1) $f(x)$ is ***easy to compute*** for all $x$ in the domain of $f$.

(2) For almost all $y$ in the range of f it is *very hard to find* an $x$ such that $f(x) = y$ .

There exists some mathematical operations in finite fields able to serve as one-way functions. Examples are:

- Exponentiation versus logarithm,
- The "Knapsack problem": In a knapsack are some goods of defined weight out of a known set of different goods. Given is the total weight of the full knapsack, asked is which goods are the content.
- The factoring problem: Prime factors of a given number are to be found.

To fulfill requirement (2) of the above definition all shown examples need to work with great numbers consisting of some hundred digits to provide for the demanded security. To make a one-way function useful for cryptographic purposes additionally a "trapdoor" is necessary, i.e. an additional amount of information (the secret key) makes the reverse operation also easy to compute. The public key in such systems consists of the publicly known information necessary to compute the chosen one-way function in the easy direction. Great numbers as a paramount security requirement for public-key systems lead to long computing time what makes practical realizations of public-key algoritms rather slow.

Examples for public-key systems based on the above listed one-way functions are:

- DH-System: algorithm for key exchange based on exponentiation, proposed by Diffie and Hellman (Diffie and Hellman, 1976),
- MH-System: ciphering algorithm for blocks of information based on the knapsack problem, proposed by Merkle and Hellman (Merkle and Hellman, 1978). This kind of algorithms together with all proposed enhancements as well as all derivates of that principle rates as already broken.
- RSA-System: ciphering algorithm for blocks of information based on the factoring problem additionally using exponentiation, proposed by Rivest, Shamir and Adleman (Rivest, Shamir and Adleman, 1978). It could not be broken until now if it is used with prime numbers of more than twohundred digits. Technical realizations exist for bit-rates up to some hundred kilobits per second.

In the introduction it has been pointed out that security systems have two attributes: secrecy and authenticity, which are independent in cryptographic security systems. That means it is possible to have either one or the other. To have both each of them needs its own security mechanism. Before an example is given, the influence of both attributes has to be clarified: secrecy concerns content and confidentiality of messages and transactions, authenticity concerns sender, receiver and content to be as claimed. Independence of this attributes can be shown easily on the example of public-key systems. The encipher key is public, the decipher key is privat and secret. Secrecy is accomplished by the system with enciphering but for the receiver of an enciphered message it is impossible to proof if the content is authentical and what the identity of the sender is. A solution to cover both attributes is double encipherment, first with secret "decipher key" of the sender followed by encipherment with the public key of the receiver. Decription is done in same order but with adjoined secret and public keys. Only if both pairs of keys are belonging together the receiver can get the plaintext knowing at the same time the identity of the sender. This procedure (or protocol) combined with a hash function is used also as an electronic or digital signature. In secret-key systems the basic assumption is made that the owner of a secret key is an authorized user. With secret keys used only in pairs authentication of sender and receiver is therefore given. In this case secure distribution of the key and encipherment are the two security mechanisms to cover both security attributes.

## TEMPEST

Tempest as word with the meaning of thunderstorm used as an acronym has produced a real newspaper thunderstorm for a short time in the middle of the eighties. The acronym TEMPEST beside other interpretations explained as T*ransient* E*lectro*M*agnetic* P*ulse* E*mantion* ST*andard* comes from the Tempest project started in the USA some 30 years ago by DoD's National Security Agency (NSA). It concerns a special area of electromagnetic interference (EMI) and there especially electromagnetic emanations from components of computer systems (and some other electronic systems). Elementary physics shows that electricity flowing through conducting material propagates an electromagnetic field which leaves the conducting area as more as frequency increases. Data processing equipment are working with very high frequencies and some ten up to some hundred MHz (Megahertz, million cycles per second) can be observed. This unwanted but physically caused radiation of electromagnetic energy can be intercepted and evaluated. The Tempest project, classified for about 20 years, has been disclosed to the public in the spring 1985 by a feature on "Tomorrow's World" of the british TV-company BBC with a five-minute demonstration of this kind of eavesdropping. One of the next steps of disclosure was a presentation of Wim van Eck (Van Eck, 1985) at the SECURICOM '85 conference. He showed that anyone can put together a primitive eavesdropping unit for somewhat over $ 100 and a portable television set, effective to a limited range between 20 and 40 feet (6 and 12 meters).One of the most radiating and therefore most dangerous part of a computer system is the video display unit ("Terminal") and in it especially the deviation unit because it contains all information shown at the screen and is working with high frequency and energy. Enciphering does not help in this case: displayed information has to be in plain what needs decipherment at least before entering the display part of the terminal. Some of the most effective measures to avoid this security threat are:

- for equipment to be constructed new a design with minimized emanation together with proper shielding to avoid or reduce outside radiation,
- for existing equipment installation in special shielding boxes or cabinets, filtering of all conducting lines from and to the equipment, defining security areas around the equipment great enough to avoid eavesdropping, accessible only for authorized employees.

A comprehensive overview on the problems with leaking computers is given in a paper from Highland (1988).

## CONCLUSION

Means and measures for data protection are as manifold as security threats are. Irrespective the missing of a strong definition for data security about four main items are to observe: data privacy or *confidentiality*, data integrity, data availability, access control and explicitly or implicitly authentication. Opposite to security threats security services and security mechanisms are available which are the substance to achieve data security. One of the most effective security mechanism is encipherment which can provide for both security attributes "secrecy" and "authenticity". Secrecy is endangered by disclosure of information in different ways. Some are well-known and obvious, some have become aware in public just since some years like Tempest. Summarizing it can be seen that data security is not the result of one or the other single protection mean or measure, it needs a well-balanced arrangement of many of them in the scope of global security concept or security policy respectively.

## REFERENCES

Bellaso, G.B. (1555). Novi et singulari modi di ciffrare. ...con le sue regole et essempi. Brescia.

Caflisch, M. and R.A. Rueppel (1987). Datensicherheit — ist Kryptologie genug? *E und M*, 104, 529-532.

Csikai, K. (Wörterbuchredaktion) (1985). Fachausdrücke der Informationsverarbeitung. In *Wörterbuch und Glossar, Englisch-Deutsch und Deutsch-Englisch*, IBM Deutschland GmbH., Stuttgart.

Diffie, W. and M.E. Hellman (1976). New directions in cryptography. *IEEE Trans. on Inform. Theory*, IT-22, 644-654.

Highland, H.J. (1988). The tempest over leaking computers. *Abacus*, 5, No. 2, 10-18, 53.

ISO 7498 (1984). Information processing systems — Open systems interconnection — Basic reference model. *International standard*, 7498 (E), International Organization for Standardization, Geneva.

ISO 7498-2 (1989). Information processing systems — Open systems interconnection — Basic reference model — Part 2: Security architecture. *International standard*, 7498-2 (E), International Organization for Standardization, Geneva.

Kahn, D. (1967). The Codebreakers — The story of secret writing. Macmillan Publishing Co. Inc., New York.

Kassel, H. and P. Strnad (1978). Lexikon Datenschutz und Datensicherung. Siemens Aktiengesellschaft, München.

Kerckhoffs, A. (1883). La Cryptographie militaire. *Journal des science militaires*, 1883, Jan., Feb., 5-38, 161-191.

Konheim, A.G. (1981). Cryptography — A primer. John Wiley & Sons, New York.

Merkle, R.C. and M.E. Hellman (1978). Hiding information and signatures in trappdor knapsacks. *IEEE Trans. on Inform. Theory*, IT-24, 525-530.

Meyer, C.H. and S.M. Matyas (1982). Cryptography: A new direction in data security. John Wiley & Sons, New York.

Murray, W.H. ("Bill") (1988). Security in open systems. Paper given at COMPSEC '88, October 11-13, 1988, Organisers: Elsevier Seminars, London.

NBS (1977). Data Encryption Standard. *FIPS Pub.*, 46. National Bureau of Standards, Washington, DC.

Porta, G.B. (1563). De furtivis literarum notis, volgo de ziferis libri IIII. Mariam Scotum, Neapoli.

Price, W.L. (1988). Standards for data security. Paper given at COMPSEC '88, October 11-13, 1988, Organisers: Elsevier Seminars, London.

Rivest, R.L, A. Shamir and L. Adleman (1978). A method for obtaining digital signatures and public key cryptosystems. *Comm. of the ACM*, 21, 120-126.

Simmons, G.J. (1987) Cryptology. In *Encyclopædia Britannica*, 5, 16th Ed., 913-924B, Encyclopædia Brtannica, Inc., Chicago.

Trithemius (Tritheim), J. (1518). Poligraphiae libri sex .... Bibliopolae Joannis Haselbergi de Aia Constantiensis.

Van Eck, W. (1985). Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4, 269-286.

Vernam, G.S. (1926). Cipher printing telegraph system for secret wire and radio telegraphic communications. *Americ. Inst. of Electrical Engineers Journal*, 45, 109-115.

Viginère, B. de (1586). Traicté des chiffres, ou secretes manieres d'escrire. Abel L'Angelier, Paris.

INVITED

# ELECTRONIC BUSINESS AND BANKING— WHICH SECURITY ASPECTS DO MATTER?

**W. J. Jaburek**

*GABE Geldausgabeautomaten-Service GmbH, Vienna, Austria*

Abstract. Business life is undergoing a profound change as our paper-based system of communicating is gradually replaced by electronic means. The new standards on Message Handling Systems X.400 (CCITT 1988) and EDIFACT (Electronic Data Interchange for Administration Commerce and Trade, UN ECE/ ISO 1988 and later) create a unified framework for such applications.

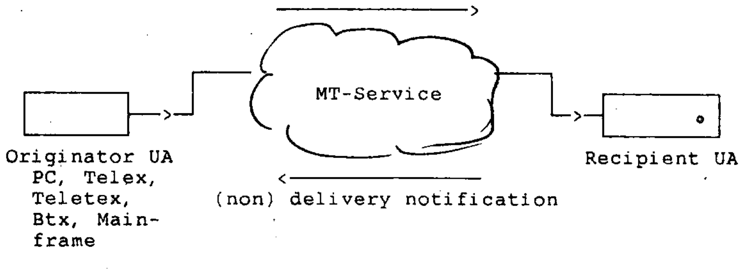
After giving examples of legally relevant communication possible security problems of using electronic mail or message handling systems (MHS) for banking, contracting, invoicing, and communication with administrations are discussed. Security in the context of the paper is defined to include legal and social as well as technical aspects. Results of a study done by the author comparing functional reliability and security of evidence of a typical MHS of today with paper-based conventional mail and Eurocheque are given.

Keywords. Security; Reliability; message handling systems; EDIFACT; data security; data privacy.

## THE FUNCTIONALITY OF MHS

Message Handling Systems (MHS) manage the forwarding of messages, mostly text documents, from the originator's computer or application Software (user agent) to a receiver's computer. Only one of the communication partners must establich an online connection to the service provider's system (MHS) at a time or they can communicate directly with one another. The user agents may be located in a PC and linked to the MHS via telephone or can be located in a companies mainframe, that is linked to a packet switched network, e.g. Datex-P in Austria.

After creation in the user agent, e.g. by using a wordprocessing system, the messages are transferred to the Message Transfer System (MTS) together with the name of the recipient's mailbox. The MTS stores the message and forwards it to the recipient's user agent, where it is kept until the recipient decides to read it. In case the message is undeliverable or in case the originator wanted it, the system generates a (non) delivery notice and sends it to the originator's user agent.



## USAGE OF MHS

Today systems like Telebox Austria or IBM's INS are used for communicating orders, invoices, for negotiating contracts or having them translated to foreign languages by people working as professionals in the foreign country. The ordering system of the Austrian Booksellers, KÖBU-Data, is working via Telebox. The banking community is operating its own MHS based on standards of its own. The international MHS of SWIFT (Society for Worldwide International Financial Telecommunication) links 3.000 connection points in 60 countries and switches about one million messages per day. The Austrian System EBK (Elektronische Banken und Kunden Kommunikation) begins to replace money transfer orders by telephone within Austria and provides information services between banks and the Oesterreichische Nationalbank. EFT-Networks for ATM and POS-Apllications in fact are specialised MHS. EAN-Austria is operating the general ordering system ECODEX on basis of a MHS.

## THREATS TO MHS-SERVICES

In order to be useful, MHS for real life usage in commerce and banking must

* be available and work reliable (<u>Reliablity</u>)

* protect data against unauthorized disclosure (<u>Data Protection</u>)

* protect data against unauthorized alteration by technical errors or "the enemy" (whoever that might be) (<u>Message Integrity</u>)

* provide means to send legally recognized and provable messages for contracting (<u>Juridical Threats</u>).

## THREATS TO AVAILABILITY

Along the path of a message the following components of the system must be available for transferring a message:

(* the originator's secretary)
* the originator's and the recipient's terminal (PC, telex, mainframe)
* the subscriber lines from the terminals and the MHS-host to the telecommunications network
* the telecommunications network (exchanges, trunk lines)
* the MHS-hardware and software
* operating personnel

Threats in this respect are:

- failure of central components: CPU, magnetic media, telecommunication lines (mean time between failure mostly being about 10.000 working hours or about one year in 24 hour service)
- overloaded parts of the system cause traffic congestions

  Here continous gathered statistics and Erlang theory of telecommunications traffic patterns help to forecast the number of lines, ports and server processes to be used.
- damage by fire, water, overvoltage (thunderstorm)
- terrorist attack, war (NEMP), other catastrophic events
- destroyed telecommunication lines or switching nodes
- power outage
- failure of air conditioning
- software errors, computer virus
- no spare parts, no maintenance available
- strike of personnel, all personnel leaving the company

One of the most common countermeasures in that area of concern is reduplication and decentralization (failure tolerant hard- and software) of hardware, telecommunication lines and personnel.

## THREATS TO DATA PROTECTION

There seem to be three major points in the path of a message, where it may be observed without much work:

* Using the electromagnetic radiation of the subscriber's terminal,

  All kind of CRT-equipped terminals work as radiotransmitter, too. Using cheap equipment (radio receiver, old black and white TV-set) it is possible to observe the contents of other people's CRTs up to some 100 metres. That seems to be enough to work in larger urban areas.

* tapping the subscriber's link to the first telecommunications exchange,

  The subscriber's lines in Austria all through houses and along the streets are marked "ÖPT" and are easily accessible, the only major difficulty being the search for the right pair of wires. Implanting a tiny bug powered by the links base current will hardly be detected and even in that case nobody knows, where the receiver is and who uses it.

* at the telecommunication exchanges themselves.

Telecommunication exchanges at night mostly are unmanned buildings without alarm system. All lines are readily accessible. Equipment for line surveillance is here, too. And for those, who do not like to work themselves, there seem to be ways to get information via people working there anyway.

More difficult or risky possibilities include

* Tapping a trunk line

needs some more technical equipment and therefore will be done only by secret services, the main advantage for the enemy being the fact, that much traffic is sent via directed radio links that always have a certain spill-over beyond their prime direction.

* Stealing data, e.g. on tape out of the MHS-Provider's building

* Hacking

* Bribing MHS personnel to get access to (selected) messages

The primary countermeasures against that types of attack ar of cryptographic nature. Especially public key cryptosystems and the Standards on Directory Services (CCITT X.500) seem to be suitable for keeping information secret in large networks.

One purely technical reason may render some messages readable to unauthorized users:

- misrouting of messages due to hard- and software errors

THREATS TO MESSAGE INTEGRITY

The integrity of messages may be endangered by purely technical risks:

* hardware and software failures

* transmission errors

Here the theory of error correcting codes provides countermeasures. CCITT X.25, the standard for packet switching networks all over the world, uses Cyclic Redundancy Checks (CRCs) for discovering transmission errors.

But the main threat seems to be intentional misuse of the system after having gained access to authorisation and authentication data. That mostly means: passwords. Those at least play three roles in today's MHS: They are
- the stamp for using the system,
- the pencil for signing a message, and
- the key to one's personal mailbox for the messages received.

Passwords can be observed at every part of the transmission path, as they are sent unaltered many times from the user's terminal to the central system. That is:

* User

Users not only tend to handle carelessly their Bankomat-PIN, e.g. in writing it on their ec-card, but tend to have a notice at their terminal containing their passwords. Even in banking applications that behaviour is observed and in the famous Rifkin case [2] led to the unauthorised telex funds transfer of more than 10 Mio $.

* Terminal, personal computer

As most users of MHS have their PC-dealer install the passwords in the PC so that they can access the system by pressing one button, PC dealers know and sometimes misuse them. The first case of that kind led to a Criminal Court Procedure right now in the second ?Instanz?

* On the way from the terminal to the central system passwords may be acquired by tapping lines, eg at the subscriber's line, in the exchange or at the trunk line.

* Another very promising way to find passwords is simple hacking combined with an attack to the system's password-file.

That was confirmed by the very successful attack against the NASA-SPANET [1] and in most systems is made easy due to users choosing simple passwords. A survey done by the author in an Austrian MHS exposed that 0,5% of the subscribers using their user-id as the password. About 40 to 80% of the passwords tend to be guessable by PC-hacking software.

* Last but not least it should be mentioned that passwords might be sold by MHS personnel.