Thomas Beth, Withfield Diffie,
Gustavus J. Simmons (editors):

System Security

Dagstuhl-Seminar-Report; 37
30.3.-3.4.92 (9214)

ISSN 0940-1121

Tel.: +49-6871 - 2458
Fax: +49-6871 - 5942

Das Internationale Begegnungs- und Forschungszentrum für Informatik (IBFI) ist eine gemeinnützige GmbH. Sie veranstaltet regelmäßig wissenschaftliche Seminare, welche nach Antrag der Tagungsleiter und Begutachtung durch das wissenschaftliche Direktorium mit persönlich eingeladenen Gästen durchgeführt werden.

Bezugsadresse: Geschäftsstelle Schloß Dagstuhl
Informatik, Bau 36
Universität des Saarlandes
W - 6600 Saarbrücken
Germany
Tel.: +49 -681 - 302 - 4396
Fax: +49 -681 - 302 - 4397
e-mail: office@dag.uni-sb.de

System Security

IBFI Schloß Dagstuhl
March 29 - April 3, 1992

organized by

TH. BETH, H. STRACK
University Karlsruhe

W. DIFFIE
SUN Microsystems

G. J. SIMMONS
Sandia Nat. Labs.

Scope of the meeting

Thomas Beth, E.I.S.S., University Karlsruhe

In March 1982 the first open research meeting in Europe on the then "new" topic Cryptography took place at Burg Feuerstein (Springer LNCS 149). While that workshop is considered to be the first of the EUROCRYPT suite of conferences, it also brought together many researchers in specialist workshops on the topics of the field, primarily at locations like Oberwolfach, Luminy and Cirencester. Meeting the needs of communication security and data integrity in theory and practice, cryptology apparently failed to address the wider system aspects arising from requirements of dependability encompassing security, safety and reliability.

Following an assessment workshop at Ascona in late 1989 and an Oberwolfach Workshop on "Mathematical Concepts of Dependable Systems" in spring 1990, where research problems of secure systems design especially under the aspects of specification and verification has been identified, the present workshop has been convened to address the topics of security and safety of (distributed) systems by emphasizing the points of view of cryptology, information theory, formal methods and system architecture.

System Security Seminar, March 29 - April 3, 1992 - Program:

Monday, March 30, 1992

Chair: *Thomas Beth and Whitfield Diffie*

09.30	Informal Discussion:	Purpose of the meeting, Scope, Goals
10.30	Coffee	
10.45	Whitfield Diffie:	Organizational remarks
11.00	Thomas Beth:	10 years after Burg Feuerstein - comparing Cryptography in 1982 to System Security in 1992
12.15	Lunch, Break	
15.00	Coffee	

Chair: *Roger Needham*

15.30	Andrea Sgarro:	Simmons-Type Bounds for Authentication Codes
16.30	Jeremy Jacob:	Refinement and its Role in Defining, Specifying and Achieving Security
18.00	Dinner	

Tuesday, March 31, 1992

Chair: *Whitfield Diffie*

09.30	Morrie Gasser:	Distributed System Security I
10.30	Coffee	
10.45	Morrie Gasser:	Distributed System Security II
11.30	Hermann Härtig:	Towards a Security Architecture for BirliX
12.15	Lunch, Break	

Chair: *Hermann Strack*

14.30	Sape Mullender:	Operating System Security
15.00	Coffee	
15.30	Jaisook Landauer:	The Trusted Mach Operating System

16.45	Manfred Reitenspieß:	Can Security be adequately implemented ?
18.00	Dinner, Break	

Chair: *Morrie Gasser*

20.00	Evening Discussion:	Security Architectures (until about 22.00)

Wednesday, April 1, 1992

Chair: *Whitfield Diffie*

09.15	Ueli Maurer:	Practical proven communications security
10.00	Ueli Maurer:	Public-key cryptography without interaction
10.30	Coffee	
10.45	Fritz Bauspieß:	Summary on Oberwolfach Workshop on Cryptographic Hash-Functions
11.00	Claus P. Schnorr:	FFT Hash Algorithms
11.45	Thomas Beth:	Digital Signature Standard (DSS)
12.15	Lunch	
Afternoon:		Trip to Trier
After return:	Dinner	

Thursday, April 2, 1992

Chair: *Kaisa Nyberg*

09.30	John Graham Cumming:	Algebraic Laws for Non-Interference
10.15	Roger Needham:	Extensions to the Logic of Authentication
10.45	Coffee	
11.15	Bert den Boer:	A Simple Authentication Scheme
12.15	Lunch, Break	
14.30	Coffee	

Chair: *Morrie Gasser*

15.00	Chris Mitchell:	Standardising Authentication Protocols based on Public Key Technologies
16.00	Break	
16.15	Kwok-yan Lam and Dieter Gollmann:	The Role of Time in Distributed Authentication
17.30	Kaisa Nyberg:	Nonlinearity Criteria
18.00	Dinner	

Chair: *Thomas Beth*

20.00	Evening Brainstorm:	Future Security Research (until about 22.00)

Friday, April 3, 1992

Chair: *Ingrid Schaumüller-Bichl*

09.15	Hermann Strack:	Formal, Informal and Constructive Methods in Development of Secure Systems
09.45	Jean-Jacques Quisquater:	The Login Problem - an Update
10.15	Johannes Buchmann:	Tools for Proving Zero Knowledge
10.45	Coffee	
11.00	Manfred Reitenspieß:	Standards for Secure Distributed Systems
11.30	Whitfield Diffie:	Future Problems of System Security
12.00	End	
12.15	Lunch	

In addition to the scheduled sessions, there were a lot of informal meetings, discussions and walks in the stimulating Schloß Dagstuhl environment to exchange ideas and to discuss current and future work.

Acknowledgement: We would like to thank everybody who made this workshop possible, interesting and enjoyable, the IBFI Scientific Board of Directors, the participants and everybody who supported us in running the workshop so smoothly, especially Dietmar Kunzler, Angelika Mueller, Kathrin Schrader, Josefine Schneider, Melanie Spang, all other of the Dagstuhl staff and Verena Kölmel (E.I.S.S.).

10 years after Burg Feuerstein:
Comparing 1982 Cryptology to 1992 System Security

Thomas Beth, E.I.S.S., University Karlsruhe

Starting from the "hot" topics of 10 years ago, an assessment of the state of the art of cryptology and its development to system security is given:
Illustrated by the history of the areas

- Cryptanalysis of classical machines
- Stream Ciphers
- Block Ciphers
- Public Key Cryptography

of the last 10 years including most recent results and announcements, the two areas

- Modern cryptology and
- System Security

have been described in presenting their features and research topics in an encompassing manner. Cryptology based on algebra, information theory and complexity with many new paradigms of evaluating system security and performance is connected to formal methods, which allow the specification and evaluation of security and safety of application w.r.t. their semantics by developing a concept of "trust" as a security primitive and in view of its "dual", "risk", which forms the basic notion of safety evaluation.

Simmons-type bounds for authentication codes

Andrea Sgarro, University of Trieste

We deal with the theoretical model of authentication coding introduced by G.J. Simmons. We make use of two "abstract" observations to present in an very compact way a whole set of information-theoretic lower bounds to fraud probabilities. (1st: many properties of authentication coding, including the definition of impersonation and the corresponding fraud probability, depend on a much weaker mathematical structure than the one originally given; 2nd: many fraud probabilities - e.g. substitution of the legimate codeword by a fake codeword for codes with and without splitting - can be taken back soon to fraudolent impersonation probabilities).

The key-role in the lower bounds is played by the rete-distortion function R(Z,X); Z being

the random key [encoding rule] and X being the binary complement of the authentication matrix [distortion level = 0]; the intrigueing appearance of rate-distortion theory (an important branch of source coding) in authentication coding is commented upon.

Practical provable communications security

Ueli Maurer, ETH Zürich

Key distribution protocols are presented that allow two parties Alice and Bob to generate a common secret key S about which an enemy Eve cannot obtain more than a non-negligible amount of information (in Shannon's sense), regardless of her computing power. As opposed to previous approaches to provable security in cryptography, which are either impractical or based on generally unrealistic assumptions about the enemy's obtainable information as on an unproven hypothesis about the computational difficulty of a certain problem, the new approach suffers from none of these disadvantages. The security of the proposed protocols rests solely on realistic assumptions about the noise on the involved communication channels.

The Role of Time in Distributed Authentication

Kwok-Yan Lam and Dieter Gollmann, Royal Holloway and Bedford New College,
London University

In this talk we discuss the notion of time in distributed authentication. In the context of authentication, we identify the place where the concept of time is needed, and describe the ways that timeliness of authentication protocol can be achieved.

Public-key cryptography without interaction

Ueli Maurer, ETH Zürich,
Yacov Yacobi, Bellcore

Presently - used public-key cryptosystems require that the sender of a message knows the (certified) public key of the intended receiver of the message. This means that the sender must interact with the receiver or with a certified public-key server prior to sending the encrypted message. In many applications such as electronic mail, such an interaction is impractical or impossible. We present the first public-key system in which a user's public key is equal to his universally known identity (e.g. e-mail address), which neither needs to be authenticated (certified) nor transmitted. A trusted authority provides a user's secret key corresponding to his identity when a user joins the network. The trusted authority is not needed for operating the system.

Formal Methods and Security

Jeremy Jacob, Oxford University Computing Laboratory & Saint Peters College, Oxford

The common model of formal developent of systems does not guarantee to preserve confidentiality properties present in a specification. Such a development only preserves (what I term, for want of a better word) functionality properties. A new set of proof rules is needed to guarantee that an implementation has every confidentiality property present in a specification. The different proof rules can be abstracted as pre-orders (reflexive & transitive relations). It is then possible to reason about the methods efficiently.

Nonlinearity Criteria

Kaisa Nyberg, University of Helsinki and Finnish Defence Forces (on leave)

The study of the design criteria of DES S-boxes has led to a number of nonlinearity criteria for Boolean functions. In this talk we discussed correlation immunity, distance from linear structures, propagation criteria and low shifted autocorrelation and further, interrelations between these criteria. It has recently been shown that partially bent functions are in certain sense optimal. This motivates a construction method for permutations with partially bent

coordinate functions to be presented at Eurocrypt '92.

Can Security be Adequately Implemented ?

Manfred Reitenspieß, SIEMENS NIXDORF Informationssysteme, Munich

The increased demand for security in information technology systems affects both the development as well as the operation of such systems.

All aspects of computer system development like problem analysis, requirements engineering, specification and implementation have to be addressed to increase security. During computer system operation, services and mechanisms have to be provided to assure the expected level of security. The security measures provided and applied are dependent on the target system architectures and their intended use.

Although considerable progress could be achieved in the last 20 years, in particular in operating system security and cryptosystems, much remains to be done. The following seems to be most important to work on:
- security in distributed or complex application systems
- understanding and implementing end user security requirements
- standardizing security mechanisms and functions.

Trusted Mach operating Systems

Sue Landauer, Trusted Information Systems Inc., USA

TMach is an object-oriented message-passing communications operating system, designed to be secure in the military usage secure & usable.

The approach used to gain the necessary assurances is to develop a strictly layered architecture with a small kernel that has a modular design. The kernel has only a small number of primitive abstractions from which all other operating system constructs can be built.

Using the layered architecture, a series of formal models are being developed, thus allowing

reusability of the models for future modifications to the system.

Timely Authentication in Distributed Systems

Kwok-Yan Lam and Thomas Beth, E.I.S.S., University Karlsruhe

In this talk we described a secure and usable scheme for distributed authentication. Our first objective is to give reasons for the provision of authentication protocols whose correctness depends on the correct generation of timestamps. Our second objective is to explain that this proposal is not as insecure as it first seems to be. The conclusion of this talk motivated our current effort of designing a secure clock synchronisation protocol as a part of our overall goal of building a secure distributed system.

Digital Distributed System Security Architecture

Morrie Gasser, Digital Equipment, Littleton, Mass., USA

Theory for the design of secure standalone systems is well understood, and many of the operating systems in production today are adequately secure for most commercial applications. However, today's style of computing is moving increasingly toward distributed heterogeneous systems, and unless there is a change in strategy the security of our systems will continue to deteriorate. DSSA attempts to raise the level of security of a distributed system to that of the best standalone systems in the areas of authentication, authorization (Access control), accountability (auditing), and secure channels (communication across the network). These capabilities are provided in an environment with no central point of control, decentralized trust, mutual suspicion between systems, and heterogeneous applications and operating systems.

A user of the distributed system ist registered by some certifying authority who signs a public key (X.509) certificate binding the user's X.500 name to his public key. The certificate is stored in the unsecure X.500 directory, freely available to servers that need to authenticate the user. The user logs in just once at some node, and signs a delegation certificate authorizing the login node to act on behalf of the user for a period of time. The login node may delegate this authority to subsequent nodes, and the final server will use the authenticated user and delegated node identities to enforce an access control decision. Access

control lists stored with objects contain principal names, groups, roles and delegations. Communications are secure with node-to-node symmetric encryption.

Towards a Security Architecture for BirliX

Hermann Härtig, GMD, Gesellschaft für Mathematik und Datenverarbeitung, St. Augustin

While many persistent object systems are built on top of conventional operating systems, the BirliX approach has followed the opposite direction: It has built a UNIX compatible OS by emulating the UNIX system interface on top of a persistent object system.

The BirliX kind is basically an abstract data type management system. Its basic services are the definition of abstract data types, their instantiation, their identification, and the communication between instances. All abstract data types share a common set of type independent attributes and methods inherited from the kernel-defined primary type as an infrastructure.

That structure leads to a security architecture, where application specific security policies are enforced by controlling the infrastructure for the BirliX objects and access control between objects. Access can be controlled using ACLs containing persons, times and instances and SRLs (subject restriction lists) as complementary mechanisms, infrastructure can be controlled using domains of confidence, that are based on authentication of nodes in secure booting techniques.

Logic of Authentication

Roger Needham, University of Cambridge

The talk mentioned some underlying concepts of the BAN logic, separating them out from the surrounding formalism. It then moved on to consider some limitations, and in particular the inability to deal with protocol-specific deductions. The idea of these was illustrated, and an extension discussed to the logic to deal with them.

Remarks on the DSS

Thomas Beth, University Karlsruhe

We give a report on the comments made upon the proposed Digital Signature Standard DSS of the U.S. NIST. These comments address the topics availability, export control, patent issues, trapdoors, size of parameters, security performance, fields of applications, improvements and new results from algebra. To achieve international acceptance of this important standard, its harmonized version, DSSH, was presented. For this the underlying El-Gamal scheme has been adapted to European needs by choosing a cyclic finite group EG of order $q = e \cdot d$ with generator w and an easy subgroup of order e. The sender, who possesses a secret personal number $p \in \mathbf{Z}_q$, sends his message $m \in \mathbf{Z}_q$ together with his userid $u = w^p$; which is the public one way result of her secret p, in short $p \dashv\!\triangleright\!\vdash u$. The sender also chose a random number i = "independente" (according to italian statistical tables) and oneways it to a, $i \dashv\!\triangleright\!\vdash a$, which suffices the french requirements for being "aléatoire". The sender also solves the equation $m = l \cdot i + p \cdot a \mod$ in the "Lösung" l (following the nomenclature of DIN).
In order to overcome computational and statistical asymmetries in the protocol the receiver challenged the sender with a test $t \in \mathbf{Z}_q$ after transforming it into a nonce $n = \omega^t$. The sender in turn will generate a so called "Schnorr multiplier" s, which by $n \dashv\!\triangleright\!\vdash n^s$ produces a Diffie-Hellmann stamp in the easy subgroup of G. The signature sent consists of the string (l, a, n^s) which by the receiver is verified by computing $\omega^m =^? u^d \cdot a^l \cdot (n^s)^q$ which in the case of correctness has to read

$$\omega^m = \omega^{ap+il} \quad 1^{st}.$$

Standardising Authentication Protocols based on Public Key Techniques

Chris Mitchell & Andy Thomas, Royal Holloway and Bedford New College,
London University

ISO has been working on a multi-part authentication standard for some years. Part I (ISO/IEC 9798-1) has recently been published and Parts 2 & 3 (9798-2 & 9798-3), covering

authentication mechanisms based on symmetric and asymmetric cryptography respectively, are now moving toward DIS (Draft International Standard) status. This paper contrasts two important authentication mechanisms from X.509-1988 and the latest draft of 9798-3, and briefly illustrates certain known attacks against this type of mechanism. A new potential security problem is described to which many published authentication protocols appear to be prone. Possible solutions to this problem are discussed together with potential ramifications on existing standards activities.

FFT II Hashing

Claus-Peter Schnorr, University of Frankfurt/Main

We present a design concept for cryptographic hash functions that uses as basic tools polynominal transformation over finite fields and the fast Fourier transform (FFT). We also present a particular example of an efficient hash algorithm that hashes messages of arbitrary bit length into an 128 bit hash value. The algorithm is designed to make the production of a pair of colliding messages computationally infeasible.
FFT II-Hashing is an improved version of FFT I-Hashing where the known weaknesses have been eliminated.

Algebraic Laws of Non-interference

John Graham-Cumming, Oxford University, Computing Laboratory, jgc@prg.ox.ac.uk

Existing formal methods for the specification and preservation of the functional properties of a system are inadequate when considering a specification with security properties. That fact is illustrated by an example of a system in CSP which is separable by giving a refinement (in traces) that loses the separability property.

The security policy non-interference is defined in the algebra of CSP and related to the original definition by Goguen & Meseguer. Using CSP abstracts from input and output and this definition is able to capture communicaton from "outputs" to "inputs" by considering communication caused by synchronisation. A number of laws for the development of non-interfering systems are given for a few CSP operators including prefiscing, concurrency and recursion.

The laws are used to illustrate the development of a multi-level secure system and show that it satisfies a non-interference property.

All proofs of laws are given in the algebra of CSP.

Tools for proving zero knowledge

J. Biehl, J. Buchmann, B. Meyer, Ch. Thiel, Ch. Tiel, Universität des Saarlandes, buchmann@cs.uni-sb.de

We develop general techniques that can be used to prove the zero knowledge property of most of the known zero knowledge protocols. Those techniques consist in reducing the circuit indistinguishability of the output distributions of two probabilistic turing machines to the indistinguishability of the output distributions of certain subroutines.

The login problem: An update

Jean-Jacques Quisquater, University of Louvain, jjq@fai.ucl.ac.be

Using the new attack of Biham-Shamir (chosen plaintext attack, Dec. 1991), we show there is a problem in a very common protocol. The identity based version of the protocol is also sensible to the same attack. We show how to repair such protocols using commitment. The resulting protocol is similar to well-known zero-knowledge protocols (without having the property!).

A simple authentication scheme

Bert den Boer, Philips CRYPTO b.v., The Netherlands

The question which answer produced the to be presented scheme was to find an authentication scheme where the probability of successful impersonation or substitution was below an acceptable low number, where we assume that the attacker has infinite computing

power and finally where the key space is essentially smaller than the message space.

In most known schemes having this above mentioned unconditional security, in other words a system that does not rely on computational difficulty but on pure lack of information, the key space is larger or as big as the message space.
Only recently D. Stinson presented in CRYPTO '91 a scheme where the key space is smaller than the message space. Our scheme needs for a fixed message space and a fixed safety parameter a smaller key space. The difference of the schemes is that the probability of succesful substitution is not a constant in our scheme but bounded above by a small number fixed by the safety parameter.

Cryptographic Hash Functions

Fritz Bauspieß, Universität Karlsruhe

I gave a 20 minutes overview of the E.I.S.S.-workshop on Cryptographic Hash Functions that was held in Oberwolfach the week before. It is hard to review all the intense discussions that took place, so I tried to present at least the essential ideas of what has been worked out and to give a short overview over the papers presented.

The papers given were:

G. Brassard:	"Privacy Amplification by Hashing"
E. Biham:	"On the Applicability of Differential Cryptoanalysis to Hash Functions"
F. Bauspieß/F. Damm:	"Requirements for Cryptographic Hash Functions"
A. Jung:	"Random Numbers in Hash Functions"
T. Matsumoto:	"Constructing One-Way Hash Functions and Relatives"
B. Preneel:	"Collision Resistant Hash Functions based on Block Cipher Algorithms"
M. Girault:	"FFT-Hashing (first version) is not collision-free"
C.P. Schnorr:	"FFT II Hashing"
P. Camion:	"A Probabilistic Algorithm which Breaks a Knapsack Hash Function"
J. J. Quisquater:	"Collisions"
M. Yung:	"Interactive Hashing: A Tool for Protocol Design"

Future Problems of System Security

Whitfield Diffie, SUN Microsystems, USA

Many problems in the development of secure systems with complex functionality can be solved by incorporating a tamper resistant module with several essential functions :

- it has a private key that cannot be altered without remanufacturing the equipment.
- it has a public key presented by a *makers mark* certificate, signed by the equipment manufacturer.
- it has a public key representing its owner with which it authenticates its owner's orders.
- it can also perform public and private key encryptions, sign and check signatures, etc.

What other capabilities such a module should have and where it should be placed in a larger information system in order, for example, to prevent virus infection or control the execution of software, presents a number of open questions.

A broader problem for system security is the mechanism by which an individual develops trust in the security mechanisms. It has been the view in the public community that each user could, in principle, audit the design and implementation of the security system, just as a mathematician can devote whatever amount of effort is needed to become thoroughly certain of any individual theorem. In practice, this is too complex a task even for an individual expert and user's must rely on faith in the organizations the have produced or acquired security equipment. The problem is made more difficult in principal by the assertion of a right of trade secrecy on the part of equipment manufacturers. One of the major challenges to information security is to develop a certification methodology that minimizes the degree to which the users of security equipment must rely on trust in the equipment suppliers.

A more technical issue is that of certificational cryptanalysis. Differential cryptanalysis is the first sign of a general method that can be used to judge and compare cryptographic algorithms and took the public cryptographic community by surprise. The paradigm of developing a formal theory in which cryptosystems can be proven secure shows no signs of yielding the needed results in the near future and a systematic, if less formal means must be found. The challenge is to develop an adequate certificational cryptanalysis that is not the outgrowth of practicing offensive cryptanalysis. A public community, after all, can never successfully practice offensive cryptanalysis as publication of results is incompatible with success in this field.

Also inherent in the use of cryptography for applications other than communication is the long term key management problem presented by encrypted data. When cryptographic methods are used to protect storage, the keys are not only secret but valuable, since the loss of a key represents the loss of data encrypted with that key. Techniques of shared secrecy and shared control must be developed to guarantee that data are neither disclosed nor lost accidentally.

The final question that must be asked is whether security problems are truly amenable to solution or whether an eternal 'arms race' is inevitable. Such implementation problems as emanations security and covert signal modulation suggest that even if the mathematics predict security, a less expensive implementation may always yield to an opponent with greater ressources.

Formal, informal and constructive Methods in Development of Secure Systems

Hermann Strack, E.I.S.S., University Karlsruhe

The "classical" approach to achieve security in system development is a top-down approach from the level of formal security model to the level of security specification and then to implementation. Verifying of the lower levels against the higher ones is the "classical" suggestion to ensure security.

It was shown by examples and principle, that this refinement approach preserves only certain security properties based on assumptions about "atomic" structures of the lower levels and takes not into account the existence of additional threats, which are not visible at higher specification levels. Additionally, using partial proofs only (for complexity reasons) reduces the meaning of the method to an informal one.

As a consequence, different additional techniques to ensure security in system development resp. refinement were suggested:

- feedback functionality from lower level specifications to security model, based on threat analysis at lower level specificatons (multilayered modelling and threat analysis)
- "multilevel" security primitives to support system development
- additional modelling of application scenario structures and of system / architecture structures

- avoiding unnecessary low level functionality and unnecessary user interactions (compared with high level spec.) through deleting or linking them together (semantic links / labels).
- a pointer was set to identify security requirements as second order requirements in requirements engineering related to certain threats and to detect them by threat analysis based on "security views".

List of Participants

Dipl.-Inform. Fritz Bauspieß
Universität Karlsruhe
Europäisches Institut für Systemsicherheit
Am Fasanengarten 5
W-7500 Karlsruhe 1
Germany
bauspies@ira.uka.de

Prof. Dr. Thomas Beth
Universität Karlsruhe
Europäisches Institut für Systemsicherheit
Am Fasanengarten 5
W-7500 Karlsruhe 1
Germany

Dr. Bert den Boer
Philips Crypto bv
P.O. Box 218
NL-5600 MD Eindhoven
The Netherlands

Prof. Dr. Johannes Buchmann
Universität des Saarlandes
Fachbereich 14 - Informatik
Im Stadtwald 15
W-6600 Saarbrücken 11
Germany
buchmann@cs.uni-sb.de

Dipl.-Math. Frank Damm
Universität Karlsruhe
Europäisches Institut für Systemsicherheit
Am Fasanengarten 5
W-7500 Karlsruhe 1
Germany
damm@ira.uka.de

Dipl. Inform. Richard De Moliner
Swiss Federal Institute of Technology
ETH Zentrum
Sternwart Straße 7
CH-8092 Zürich
Switzerland
demoliner@isi.ethz.ch

Dr. Whitfield Diffie
Sun Microsystems
MTV 01-40
2550 Garcia Avenue
Mountain View CA 94043
USA

Dr. Walter Fumy
Siemens AG
AUT 961 A
Günther-Scharowsky-Str. 1
W-8520 Erlangen
Germany

Morrie Gasser
Digital Equipment Corporation
LKG 1-2/A19
550 King Street
Littleton MA 01460
USA
gasser@grotto.enet.dec.com

Dipl.-Inform. Rainer Glaschick
Siemens-Nixdorf Informationssysteme
Putzbrunner Str. 71
W-8000 München 83
Germany

Dr. Dieter Gollmann
Royal Holloway and Bedford New College
Department of Computer Science
Egham Hill
Egham TW20 0EX
Great Britain
dieter@cs.rhbnc.ac.uk

John Graham-Cumming
Oxford University
Computing Laboratory
Programming Research Group
11 Keble Road
Oxford OX1 3QD
Great Britain
jgc@prg.ox.ac.uk

Dr. Hermann Härtig
GMD/IS
Schloß Birlinghoven
Postfach 12 40
W-5205 St. Augustin 1
Germany
haertig@gmdzi.gmd.de

Priv.-Doz. Dr. Franz-Peter Heider
CAP debis GEI
Oxfordstr. 12-16
W-5300 Bonn 1
Germany
heider@geibn.uucp

Priv.-Doz. Dr. Patrick Horster
Universität Karlsruhe
Europäisches Institut für Systemsicherheit
Am Fasanengarten 5
W-7500 Karlsruhe 1
Germany

Dr. Jeremy Lawrence Jacob
Oxford University Computing Laboratory
Programming Research Group
11 Keble Road
Oxford OX1 3QD
Great Britain
Jeremy.Jacob@comlab.oxford.ac.uk

Dipl.-Inform. Hans-Joachim Knobloch
Universität Karlsruhe
Europäisches Institut für Systemsicherheit
Am Fasanengarten 5
W-7500 Karlsruhe 1
Germany
knobloch@ira.uka.de

Dr. Kwok-yan Lam
Royal Holloway and Bedford New College
Department of Computer Science
Egham Hill
Egham TW20 0EX
Great Britain
kyl@cs.rhbnc.ac.uk

Mrs. Jaisook Landauer
Trusted Information Systems Inc.
3060 Washington Road
Glenwood MD 21738
USA
jrl@la.tis.com

Prof. Dr. Ueli Maurer
ETH Zürich
Department of Computer Science
ETH-Zentrum
CH-8092 Zürich
Switzerland
maurer@inf.wthz.ch

Prof. Chris Mitchell
Royal Holloway and Bedford New College
Department of Computer Science
Egham Hill
Egham TW20 0EX
Great Britain
cjm@cs.rhbnc.ac.uk

Prof. Dr. Sape J. Mullender
Universieit Twente
Faculteit der Informatica
Postbus 217
NL-7500 AE Enschede
The Netherlands
sape@cs.utwente.nl

Prof. Dr. Roger Needham
Cambridge University
Computer Laboratory
Pembroke Street
Cambridge CB2 3QG
Great Britain
Roger.Needham@cl.cam.ac.uk

Dr. Valtteri Niemi
University of Turku
Dept. of Mathematics
20500 Turku 50
Finland
vniemi@kontu.utu.fi

Dr. Kaisa Nyberg
Im Etzental 19
W-5300 Bonn 2
Germany

Dr. Jean-Jacques Quisquater
Universit'e de Louvain
FAI - Dept. of Electrical Engineering
Place du Levant 3
B-1348 Louvain-la-Neuve
Belgium
jjd@fai.ucl.ac.be

Dr. Manfred Reitenspieß
Siemens Nixdorf Informationssysteme AG
STO XS 23
Otto-Hahn-Ring 6
W-8000 München 83
Germany
sinix@unido.euunet

Dr. Ingrid Schaumüller-Bichl
GENESIS
Hardware-Software-Consulting GmbH
Lannerweg 9
A-9291 Krumpendorf
Austria

Prof. Dr. Claus P. Schnorr
Universität Frankfurt
Fachbereich Mathematik
Robert-Mayer-Str. 6-10
W-6000 Frankfurt 11
Germany
schnorr@informatik.uni-frankfurt.de

Prof. Andrea Sgarro
Universit'a degli Studi di Trieste
Dipt. di Science Matematiche
I-34100 Trieste
Italy
dsma@univ.trieste.it

Dipl.-Math. Hermann Strack
Universität Karlsruhe
Europäisches Institut für Systemsicherheit
Am Fasanengarten 5
W-7500 Karlsruhe 1
Germany
strack@ira.uka.de

Prof. Dr. Brigitte Vall'ee
ISMRA
Boulevard du Marechal Juin
F-14050 Caen Cedex
France
valee@geocub.greco-prog.fr

Zuletzt erschienene und geplante Titel:

G. Farin, H. Hagen, H. Noltemeier (editors):
Geometric Modelling, Dagstuhl-Seminar-Report; 17, 1.-5.7.1991 (9127)

A. Karshmer, J. Nehmer (editors):
Operating Systems of the 90s and Beyond, Dagstuhl-Seminar-Report; 18, 8.-12.7.1991 (9128)

H. Hagen, H. Müller, G.M. Nielson (editors):
Scientific Visualization, Dagstuhl-Seminar-Report; 19, 26.8.-30.8.91 (9135)

T. Lengauer, R. Möhring, B. Preas (editors):
Theory and Practice of Physical Design of VLSI Systems, Dagstuhl-Seminar-Report; 20, 2.9.-6.9.91 (9136)

F. Bancilhon, P. Lockemann, D. Tsichritzis (editors):
Directions of Future Database Research, Dagstuhl-Seminar-Report; 21, 9.9.-12.9.91 (9137)

H. Alt , B. Chazelle, E. Welzl (editors):
Computational Geometry, Dagstuhl-Seminar-Report; 22, 07.10.-11.10.91 (9141)

F.J. Brandenburg , J. Berstel, D. Wotschke (editors):
Trends and Applications in Formal Language Theory, Dagstuhl-Seminar-Report; 23, 14.10.-18.10.91 (9142)

H. Comon , H. Ganzinger, C. Kirchner, H. Kirchner, J.-L. Lassez , G. Smolka (editors):
Theorem Proving and Logic Programming with Constraints, Dagstuhl-Seminar-Report; 24, 21.10.-25.10.91 (9143)

H. Noltemeier, T. Ottmann, D. Wood (editors):
Data Structures, Dagstuhl-Seminar-Report; 25, 4.11.-8.11.91 (9145)

A. Dress, M. Karpinski, M. Singer(editors):
Efficient Interpolation Algorithms, Dagstuhl-Seminar-Report; 26, 2.-6.12.91 (9149)

B. Buchberger, J. Davenport, F. Schwarz (editors):
Algorithms of Computeralgebra, Dagstuhl-Seminar-Report; 27, 16.-20.12.91 (9151)

K. Compton, J.E. Pin , W. Thomas (editors):
Automata Theory: Infinite Computations, Dagstuhl-Seminar-Report; 28, 6.-10.1.92 (9202)

H. Langmaack, E. Neuhold, M. Paul (editors):
Software Construction - Foundation and Application, Dagstuhl-Seminar-Report; 29, 13..-17.1.92 (9203)

K. Ambos-Spies, S. Homer, U. Schöning (editors):
Structure and Complexity Theory, Dagstuhl-Seminar-Report; 30, 3.-7.02.92 (9206)

B. Booß, W. Coy, J.-M. Pflüger (editors):
Limits of Modelling with Programmed Machines, Dagstuhl-Seminar-Report; 31, 10.-14.2.92 (9207)

K. Compton, J.E. Pin , W. Thomas (editors):
Automata Theory: Infinite Computations, Dagstuhl-Seminar-Report; 28, 6.-10.1.92 (9202)

H. Langmaack, E. Neuhold, M. Paul (editors):
Software Construction - Foundation and Application, Dagstuhl-Seminar-Report; 29, 13.-17.1.92 (9203)

K. Ambos-Spies, S. Homer, U. Schöning (editors):
Structure and Complexity Theory, Dagstuhl-Seminar-Report; 30, 3.-7.2.92 (9206)

B. Booß, W. Coy, J.-M. Pflüger (editors):
Limits of Information-technological Models, Dagstuhl-Seminar-Report; 31, 10.-14.2.92 (9207)

N. Habermann, W.F. Tichy (editors):
Future Directions in Software Engineering, Dagstuhl-Seminar-Report; 32; 17.2.-21.2.92 (9208)

R. Cole, E.W. Mayr, F. Meyer auf der Heide (editors):
Parallel and Distributed Algorithms; Dagstuhl-Seminar-Report; 33; 2.3.-6.3.92 (9210)

P. Klint, T. Reps, G. Snelting (editors):
Programming Environments; Dagstuhl-Seminar-Report; 34; 9.3.-13.3.92 (9211)

H.-D. Ehrich, J.A. Goguen, A. Sernadas (editors):
Foundations of Information Systems Specification and Design; Dagstuhl-Seminar-Report; 35; 16.3.-19.3.9 (9212)

W. Damm, Ch. Hankin, J. Hughes (editors):
Functional Languages:
Compiler Technology and Parallelism; Dagstuhl-Seminar-Report; 36; 23.3.-27.3.92 (9213)

Th. Beth, W. Diffie, G.J. Simmons (editors):
System Security; Dagstuhl-Seminar-Report; 37; 30.3.-3.4.92 (9214)

C.A. Ellis, M. Jarke (editors):
Distributed Cooperation in Integrated Information Systems; Dagstuhl-Seminar-Report; 38; 5.4.-9.4.92 (9215)

J. Buchmann, H. Niederreiter, A.M. Odlyzko, H.G. Zimmer (editors):
Algorithms and Number Theory, Dagstuhl-Seminar-Report; 39; 22.06.-26.06.92 (9226)

E. Börger, Y. Gurevich, H. Kleine-Büning, M.M. Richter (editors):
Computer Science Logic, Dagstuhl-Seminar-Report; 40; 13.07.-17.07.92 (9229)

J. von zur Gathen, M. Karpinski, D. Kozen (editors):
Algebraic Complexity and Parallelism, Dagstuhl-Seminar-Report; 41; 20.07.-24.07.92 (9230)

F. Baader, J. Siekmann, W. Snyder (editors):
6th International Workshop on Unification, Dagstuhl-Seminar-Report; 42; 29.07.-31.07.92 (9231)

J.W. Davenport, F. Krückeberg, R.E. Moore, S. Rump (editors):
Symbolic, algebraic and validated numerical Computation, Dagstuhl-Seminar-Report; 43; 03.08.-07.08.92 (9232)

R. Cohen, W. Wahlster (editors):
3rd International Workshop on User Modeling, Dagstuhl-Seminar-Report; 44; 10.-14.8.92 (9233)

R. Reischuk, D. Uhlig (editors):
Complexity and Realization of Boolean Functions, Dagstuhl-Seminar-Report; 45; 24.08.-28.08.92 (9235)

Th. Lengauer, D. Schomburg, M.S. Waterman (editors):
Molecular Bioinformatics, Dagstuhl-Seminar-Report; 46; 07.09.-11.09.92 (9237)

V.R. Basili, H.D. Rombach, R.W. Selby (editors):
Experimental Software Engineering Issues, Dagstuhl-Seminar-Report; 47; 14.-18.09.92 (9238)

Y. Dittrich, H. Hastedt, P. Schefe (editors):
Computer Science and Philosophy, Dagstuhl-Seminar-Report; 48; 21.09.-25.09.92 (9239)

R.P. Daley, U. Furbach, K.P. Jantke (editors):
Analogical and Inductive Inference 1992 , Dagstuhl-Seminar-Report; 49; 05.10.-09.10.92 (9241)

E. Novak, St. Smale, J.F. Traub (editors):
Algorithms and Complexity of Continuous Problems, Dagstuhl-Seminar-Report; 50; 12.10.-16.10.92 (9242)

J. Encarnação, J. Foley (editors):
Multimedia - System Architectures and Applications, Dagstuhl-Seminar-Report; 51; 02.11.-06.11.92 (9245)

F.J. Rammig, J. Staunstrup, G. Zimmermann (editors):
Self-Timed Design, Dagstuhl-Seminar-Report; 52; 30.11.-04.12.92 (9249)