Lecture Notes in Computer Science 578

Th. Beth M. Frisch G. J. Simmons (Eds.)

Public-Key Cryptography: State of the Art and Future Directions

E.I. S. S. Workshop
Oberwolfach, Germany, July 3–6, 1991
Final Report

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Volume Editors

Thomas Beth
Markus Frisch
European Institute for System Security (E.I.S.S.), Universität Karlsruhe
Am Fasanengarten 5, W-7500 Karlsruhe, FRG

Gustavus J. Simmons
National Security Studies, SANDIA National Laboratories
P. O. Box 5800, Org. 700, Albuquerque, NM 87185, USA

CR Subject Classification (1991): E.3, F.2.1

ISBN 3-540-55215-4 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-55215-4 Springer-Verlag New York Berlin Heidelberg

Typesetting: Camera ready by author
Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
45/3140-543210 - Printed on acid-free paper

Preface

The "European Institute for System Security (E.I.S.S.)" was founded on February 29, 1988 by cabinet resolution of the state government Baden-Württemberg. It is headed by Professor Thomas Beth and is affiliated with the Institute for Algorithms and Cognitive Systems (IAKS) of the Faculty for Computer Science at the University of Karlsruhe (TH). From November 1, 1988 to November 30, 1990, the institute was situated in the rooms of the building Kaiserstrasse 8 (title picture annual report 1988/89) on the campus of the University of Karlsruhe. Even back then, the E.I.S.S. was provided with a seminar and conference room, laboratory and computer rooms as well as a separate administration office and a library, apart from rooms for the permanently employed staff and visiting scientists.

Since December 1, 1990, the E.I.S.S. is situated together with the Institute for Algorithms and Cognitive Systems in the new building of the Faculty for Computer Science, Am Fasanengarten 5.

In accordance with the cabinet resolution, the basic task setting for the E.I.S.S. is scientific research and knowledge transfer in the field of security in telecommunications, computer and information systems. These tasks are dealt with in the scope of European projects and in cooperation with other private and public research institutions.

Among the E.I.S.S. tasks are mainly

- Research and development projects in the field of data security technology for open networks,
- Research and development projects in the field of data security technology in information and computer systems,
- Procurement and evaluation of up-to-date research and project information within the competence of the E.I.S.S.,
- Vocational and advanced training measures in the fields of data security and security of open networks as well as of information and computer systems.

With the installation of the E.I.S.S. a centre, where the sufficient concentration of personnel, expertise and equipment is available permanently, will be dedicated in Europe to the key sector of system security, which is important for the future of information technology. Thus the core for an attractive institute has been created, where research and development, as well as knowledge transfer between science, economy and administration in Europe can be advanced.

E.I.S.S. Karlsruhe Thomas Beth
December 1991

What Is Achieved Through this Report?

In accordance with its main task, the E.I.S.S. has convened assessment workshops on central questions of system security such as

- Open and secure information systems,
- Block cipher technology,
- Stream cipher technology and
- Security for object-oriented systems / databases.

In this suite the most recent one addressed the topic of public-key cryptography and will be followed by a workshop on state of the art of hash functions in early 1992. This report on the state of the art and future direction of public-key cryptography is made public in accordance with the terms of reference of the E.I.S.S. The publication through the Lecture Notes in Computer Science series has been chosen as a fast and cost-effective way of disseminating the results of this workshop and the know-how compiled by the invited experts to all members of the general computer science community: systems developers, researchers, decision makers, standardization committees, patent offices, and, last but not least, users and customers of secure computer systems.

Contents