Lecture Notes in Computer Science 2140
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

Isabelle Attali Thomas Jensen (Eds.)

Smart Card Programming and Security

International Conference
on Research in Smart Cards, E-smart 2001
Cannes, France, September 19-21, 2001
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Isabelle Attali
INRIA Sophia Antipolis
BP 93, 06902 Sophia Antipolis Cedex, France
E-mail: Isabelle.Attali@inria.fr

Thomas Jensen
IRISA/CNRS
Campus de Beaulieu
35042 Rennes, France
E-mail: Thomas.Jensen@irisa.fr

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Smart card programming and security ; proceedings / International
Conference on Research in Smart Cards, E-Smart 2001, Cannes, France,
September 19 - 21, 2001. Isabell Attali ; Thomas Jensen (ed.). - Berlin ;
Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ;
Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2140)
ISBN 3-540-42610-8

CR Subject Classification (1998): C.3, C.2, D.3.2, D.4.6, E.3, F.3, K.6.5, K.4.4

ISSN 0302-9743
ISBN 3-540-42610-8 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

© Springer-Verlag Berlin Heidelberg 2001
Printed in Germany

Typesetting: Camera-ready by author, data conversion by DA TeX Gerd Blumenstein
Printed on acid-free paper SPIN 10840169 06/3142 5 4 3 2 1 0

Foreword

The E-smart 2001 international conference on research in smart cards was held in Cannes, France on 19–21 September. The conference was jointly organized by the Java Card Forum, Eurosmart and INRIA, and received helpful financial support from the Conseil Régional Provence-Alpes-Côte d'Azur.

The intention with E-smart is to provide a forum for discussion and exchange of results on smart card development, security, and applications. This year's program was established by an international program committee that examined 38 papers submitted and selected 20 of these for presentation. The list of topics of this year's presentations includes biometrics, cryptography and electronic signatures on smart cards, hardware and software solution for smart card security, formal methods for smart card evaluation and certification, architectures for multi-applications and secure open platforms, middleware for smart cards and novel applications of smart cards. The conference also featured an invited talk by Simon Moore from the University of Cambridge.

Isabelle Attali
Thomas Jensen
E-smart 2001 program committee co-chairs.

Organization

Program Committee

Isabelle Attali, INRIA
Dominique Bolignano, Trusted Logic
Bertrand du Castel, Schlumberger
Wolfgang Effing, Giesecke & Devrient
Christian Goire, Bull CP8
Pieter Hartel, University of Twente
Peter Honeyman, University of Michigan
Thomas Jensen, IRISA / CNRS
Pierre Paradinas, Gemplus
Joachim Posegga, SAP AG
Peter Ryan, CERT
Jean-Paul Thomasson, ST Microelectronics
Yasuyoshi Uemura, ECSEC

Thanks are due to the following people for their help with the refereeing of papers: Thomas Genet, Valerie Viet Triem Tong, Stefan Friedich, Harald Vogt, Jaap-Henk Hoepman, Neil Henderson, Adam Field, and Jordan Chong.

Table of Contents

Invited Talk

Protecting Consumer Security Devices (The Next 10 Years) 1
Simon Moore

Contributed Papers

Jakarta: A Toolset for Reasoning about JavaCard 2
G. Barthe, G. Dufay, M. Huisman, and S. Melo de Sousa

Mechanising a Protocol for Smart Cards 19
Giampaolo Bella

JCCM: Flexible Certificates for Smartcards with Java Card 34
Celeste Campo, Andrés Marm, Arturo García, Ignacio Díaz,
Peter T. Breuer, Carlos Delgado, and Carlos García

Context Inference for Static Analysis of Java Card Object Sharing 43
Denis Caromel, Ludovic Henrio, and Bernard Serpette

Automated Test and Oracle Generation for Smart-Card Applications 58
Duncan Clarke, Thierry Jéron, Vlad Rusu, and Elena Zinovieva

An Internet Authorization Scheme
Using Smart-Card-Based Security Kernels 71
Yves Deswarte, Noreddine Abghour, Vincent Nicomette,
and David Powell

Turning Multi-applications Smart Cards Services Available
from Anywhere at Anytime: A SOAP/MOM Approach
in the Context of Java Cards 83
Didier Donsez, Sébastien Jean, Sylvain Lecomte, and Olivier Thomas

An Operational Semantics of the Java Card Firewall 95
Marc Éluard, Thomas Jensen, and Ewen Denne

CardS4: Modal Theorem Proving on Java Smartcards 111
Rajeev Prabhakar Goré and Phuong Thê Nguyên

iButton Enrolment and Verification Requirements
for the Pressure Sequence Smartcard Biometric 124
Neil J. Henderson, Neil M. White, and Pieter H. Hartel

SIMspeak – Towards an Open and Secure Application Platform
for GSM SIMs 135
Roger Kehr and Hendrik Mieves

On-Card Bytecode Verification for Java Card 150
Xavier Leroy

Towards a Full Formal Specification of the JavaCard API 165
Hans Meijer and Erik Poll

Protection Profiles and Generic Security Targets
for Smart Cards as Secure Signature Creation Devices –
Existing Solutions for the Payment Sector 179
Gisela Meister and Michael Vogel

A Flexible Invocation Framework for Java Card 188
Michael Montgomery and Ksheerabdhi Krishna

ElectroMagnetic Analysis (EMA):
Measures and Counter-Measures for Smart Cards 200
Jean-Jacques Quisquater and David Samyde

Information Leakage Attacks against Smart Card Implementations
of the Elliptic Curve Digital Signature Algorithm 211
Tanja Römer and Jean-Pierre Seifert

Use of Biometrics for User Verification
in Electronic Signature Smartcards 220
Bruno Struif

Programming Internet Smartcard with XML Scripts 228
Pascal Urien

Public-Key-Based High-Speed Payment (Electronic Money) System
Using Contact-Less Smart Cards 242
*Hideo Yamamoto, Tetsutaro Kobayashi, Masahiro Morita,
and Ryuji Yamada*

Author Index 255