Lecture Notes in Computer Science 3362

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Gilles Barthe Lilian Burdy
Marieke Huisman Jean-Louis Lanet
Traian Muntean (Eds.)

Construction and Analysis of Safe, Secure, and Interoperable Smart Devices

International Workshop, CASSIS 2004
Marseille, France, March 10-14, 2004
Revised Selected Papers

Springer

Volume Editors

Gilles Barthe
Lilian Burdy
Marieke Huisman
Jean-Louis Lanet
INRIA Sophia-Antipolis
2004 Route des Lucioles, BP 93, 06902 Sophia Antipolis, France
E-mail:{Gilles.Barthe, Marieke.Huisman, Jean-Louis.Lanet}@inria.fr
Lilian.Burdy@sophia.inria.fr

Traian Muntean
Université de la Méditerranée
Ecole Supérieure D'Ingénieurs de Luminy
Case 925 - ESIL Parc Scientifique, 13288 Marseille, France
E-mail: Traian.Muntean@esil.univ-mrs.fr

Library of Congress Control Number: 2004117384

CR Subject Classification (1998): D.2, C.3, D.1, D.3, D.4, F.3, E.3

ISSN 0302-9743
ISBN 3-540-24287-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 11375197 06/3142 5 4 3 2 1 0

Preface

This volume contains a selection of refereed papers from participants of the workshop "Construction and Analysis of Safe, Secure and Interoperable Smart Devices" (CASSIS), held from the 10th to the 13th March 2004 in Marseille, France:

`http://www-sop.inria.fr/everest/events/cassis04/`

The workshop was organized by INRIA (Institut National de Recherche en Informatique et en Automatique), France and the University de la Méditerranée, Marseille, France. The workshop was attended by nearly 100 participants, who were invited for their contributions to relevant areas of computer science.

The aim of the workshop was to bring together experts from the smart devices industry and academic researchers, with a view to stimulate research on formal methods and security, and to encourage the smart device industry to adopt innovative solutions drawn from academic research.

The next generation of smart devices holds the promise of providing the required infrastructure for the secure provision of multiple and personalized services. In order to deliver their promise, the smart device technology must however pursue the radical evolution that was initiated with the adoption of multi-application smartcards. Typical needs include:

- The possibility for smart devices to feature extensible computational infrastructures that may be enhanced to support increasingly complex applications that may be installed post-issuance, and may require operating system functionalities that were not pre-installed. Such additional flexibility must however not compromise security.
- The possibility for smart devices to achieve a better integration with larger computer systems, through improved connectivity, genericity, as well as interoperability.
- The possibility for smart devices to protect themselves and the applications they host from hostile applications, by subjecting incoming applications to analyses that bring strong guarantees in terms of confidentiality or resource control.
- The possibility for application developers to establish through formal verification based on logical methods the correctness of their applications. In addition, application developers should be offered the means to convey to end-users or some trusted third party some verifiable evidence of the correctness of their applications.
- The possibility for smart devices to be modeled and proved correct formally, in order to achieve security evaluations such as Common Criteria at the highest levels.

In order to address the different issues raised by the evolution of smart devices, the workshop consisted of seven sessions featuring one keynote speaker and three or four invited speakers:

1. Trends in smart card research
2. Operating systems and virtual machine technologies
3. Secure platforms
4. Security
5. Application validation
6. Verification
7. Formal modeling

The keynote speakers for this edition were: Eric Vétillard (Trusted Logic), Ksheerabdhi Krishna (Axalto), Xavier Leroy (INRIA), Pieter Hartel (U. of Twente), K. Rustan M. Leino (Microsoft Research), Jan Tretmans (U. of Nijmegen), and J. Strother Moore (U. of Texas at Austin).

In addition, a panel chaired by Pierre Paradinas (CNAM), and further consisting of Jean-Claude Huot (Oberthur Card Systems), Gilles Kahn (INRIA), Ksheerabdhi Krishna (Axalto), Erik Poll (U. of Nijmegen), Jean-Jacques Quisquater (U. of Louvain), and Alain Sigaud (Gemplus), examined the opportunities and difficulties in adapting open source software for smart devices execution platforms.

We wish to thank the speakers and participants who made the workshop such a stimulating event, and the reviewers for their thorough evaluations of submissions. Furthermore, we gratefully acknowledge financial support from Conseil Général des Bouches-du-Rhône, Axalto, France Télécom R&D, Gemplus International, Microsoft Research and Oberthur Card Systems.

November 2004

Gilles Barthe
Lilian Burdy
Marieke Huisman
Jean-Louis Lanet
Traian Muntean

Organizing Committee

Gilles Barthe	INRIA Sophia Antipolis, France
Lilian Burdy	INRIA Sophia Antipolis, France
Marieke Huisman	INRIA Sophia Antipolis, France
Jean-Louis Lanet	INRIA DirDRI, France
Traian Muntean	University de la Méditerranée, Marseille, France

Reviewers

Cuihtlauac Alvarado	Rajeev Joshi	Judi Romijn
John Boyland	Florian Kammüller	Vlad Rusu
Michael Butler	Laurent Lagosanto	Peter Ryan
Koen Claessen	Yassine Lakhnech	David Sands
Alessandro Coglio	Xavier Leroy	Gerardo Schneider
Adriana Compagnoni	Gerald Lüttgen	Ulrik Pagh Schultz
Pierre Crégut	Anil Madhavapeddy	David Scott
Jean-Michel Douin	Claude Marché	Robert de Simone
Hubert Garavel	Ricardo Medel	Christian Skalka
Nikolaos Georgantas	Greg Morisett	Oscar Slotosch
Mike Gordon	Laurent Mounier	Kim Sunesen
Chris Hankin	Christophe Muller	Sabrina Tarento
Rene Rydhof Hansen	Alan Mycroft	Hendrik Tews
Klaus Havelund	Brian Nielsen	Mark Utting
Lex Heerink	David von Oheimb	Eric Vétillard
Ludovic Henrio	Arnd Poetzsch-Hefftner	Willem Visser
Charuwalee Huadmai	Erik Poll	Olivier Zendra
Thierry Jéron	Christophe Rippert	Elena Zucca

Table of Contents