Lecture Notes in Computer Science 1007
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Advisory Board: W. Brauer D. Gries J. Stoer

Antoon Bosselaers Bart Preneel (Eds.)

Integrity Primitives for Secure Information Systems

Final Report of
RACE Integrity Primitives Evaluation
RIPE-RACE 1040

Springer

Series Editors

Gerhard Goos
Universität Karlsruhe
Vincenz-Priessnitz-Straße 3, D-76128 Karlsruhe, Germany

Juris Hartmanis
Department of Computer Science, Cornell University
4130 Upson Hall, Ithaca, NY 14853, USA

Jan van Leeuwen
Department of Computer Science,Utrecht University
Padualaan 14, 3584 CH Utrecht, The Netherlands

Volume Editors

Antoon Bosselaers
Bart Preneel
Department Elektrotechniek - ESAT, Katholieke Universiteit Leuven
Kardinaal Mercierlaan 94, B-3001 Heverlee, Belgium

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Integrity primitives for secure information systems : final RIPE report of RACE integrity primitives evaluation (R1040) / Antoon Bosselaers ; Bart Preneel (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 1995
(Lecture notes in computer science ; Vol. 1007)
ISBN 3-540-60640-8
NE: Bosselaers, Antoon [Hrsg.]; GT

CR Subject Classification (1991): D.4.6, E.3, K.6.5

ISBN 3-540-60640-8 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10487165 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

RIPE Integrity Primitives

Final report of RACE Integrity Primitives Evaluation (R1040)

A. Berendschot, *PTT Research, Leidschendam (NL)*
B. den Boer, *Philips Crypto B.V., Eindhoven (NL)*
J.P. Boly, *PTT Research, Leidschendam (NL)*
A. Bosselaers, *ESAT Lab, K.U. Leuven (B)*
J. Brandt, *Aarhus Universitet, Århus (DK)*
D. Chaum (chairman), *CWI/Digicash, Amsterdam (NL)*
I. Damgård, *Aarhus Universitet, Århus (DK)*
M. Dichtl, *Siemens AG, München (D)*
W. Fumy, *Siemens AG, München (D)*
M. van der Ham, *CWI, Amsterdam (NL)*
C.J.A. Jansen, *Philips Crypto B.V., Eindhoven (NL)*
P. Landrock, *Aarhus Universitet, Århus (DK)*
B. Preneel, *ESAT Lab, K.U. Leuven (B)*
G. Roelofsen, *PTT Research, Leidschendam (NL)*
P. de Rooij, *PTT Research, Leidschendam (NL)*
J. Vandewalle, *ESAT Lab, K.U. Leuven (B)*

Abstract

This is a manual intended for those seeking to secure information systems by applying modern cryptography. It represents the successful attainment of goals by RIPE (RACE Integrity Primitives evaluation), a 350 man-month project funded in part by the Commission of the European Communities. The recommended portfolio of integrity primitives, which is the main product of the project, forms the heart of this volume.

By integrity, we mean the kinds of security that can be achieved through cryptography, apart from concealment. Thus included are ways to ensure that stored or communicated data is not illicitly modified, that parties exchanging messages are actually present, and that "signed" electronic messages can be recognised as authentic by anyone.

Of particular concern to the project were the high-speed requirements of broadband communication. But the project also aimed for completeness in its recommendations. As a result, the portfolio contains primitives, i.e., building blocks, that can meet most of today's perceived needs for integrity.

AMS Subject Classification (1991): 94A60
CR Subject Classification (1991): D.4.6
Keywords & Phrases: Integrity Primitives, Security Services, Integrity Mechanisms, Data Origin Authentication, Entity Authentication, Access Control, Data Integrity, Non-repudiation, Signature, Key Exchange.
Note: The work described in this report is the result of a research project carried out during the period 1 November 1988 to 30 June 1992. While the project received support under the EC RACE programme, the results should not be interpreted as a given view on the Community policy in this area.

Table of Contents