

# Lecture Notes in Computer Science

1361

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Bruce Christianson Bruno Crispo  
Mark Lomas Michael Roe (Eds.)

# Security Protocols

5th International Workshop  
Paris, France, April 7-9, 1997  
Proceedings



Springer

## Volume Editors

**Bruce Christianson**

Computer Science Department, University of Hertfordshire  
Hatfield, AL10 9AB, UK  
E-mail: b.christianson@herts.ac.uk

**Bruno Crispo**

University of Cambridge, Computer Laboratory  
New Museums Site, Pembroke Street, Cambridge, CB2 3QG, UK  
and University of Turin, Department of Computer Science  
Corso Svizzera 185, I-10149 Torino, Italy  
E-mail: bruno.crispo@cl.cam.ac.uk

**Mark Lomas**

Information Security Department, Goldman Sachs International  
Peterborough Court, 133 Fleet Street, London EC4A 2BB, UK  
E-mail: mark.lomas@gs.com

**Michael Roe**

University of Cambridge, Computer Laboratory  
New Museums Site, Pembroke Street, Cambridge, CB2 3QG, UK  
E-mail: michael.roe@cl.cam.ac.uk

Cataloging-in-Publication data applied for

## Die Deutsche Bibliothek - CIP-Einheitsaufnahme

**Security protocols : 5th international workshop, Paris, France, April 7 - 9, 1997 ; proceedings / Mark Lomas et al. (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1998**

(Lecture notes in computer science ; Vol. 1361)

ISBN 3-540-64040-1

CR Subject Classification (1991): E.3, F.2.1-2, C.2, K.6.5, J.1

ISSN 0302-9743

ISBN 3-540-64040-1 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 1998  
Printed in Germany

Typesetting: Camera-ready by author  
SPIN 10631798 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

## Preface

Welcome to the proceedings of the fifth International Workshop on Security Protocols. These workshops grew from a series of informal meetings held at the University of Cambridge Computer Laboratory. Our aim has been to assemble researchers in an environment where they could discuss the limitations and omissions of current work in computer security, and the implications of these for future directions in security protocol research.

Since the publications in 1978 of the seminal paper on authentication by Roger Needham and Michael Schroeder, it has become abundantly clear that the properties which cryptographic protocols actually possess are extraordinarily fragile. One reason for this is the complex nature of the interactions between the algorithmic mechanisms used to realise the protocols on the one hand, and the high-level behaviour of the applications which the protocols are intended to support on the other. Experience also shows that it is difficult to abstract from these interactions successfully, and to describe them in a way which allows them to be reasoned about correctly.

Consequently, security failures often occur as a result of an unnoticed mismatch between the use an application makes of a security protocol and the properties which the realisation of the protocol provides. The insights provided by these subtle constraints, and by breaking them, form the theme of this year's workshop. We hope these proceedings will enable you to share some of these insights.

We would like to thank Serge Vaudenay for the exemplary local arrangements at the Ecole Normale Supérieure during the workshop.

October 1997  
(Brumaire 206)

Mark Lomas  
Bruce Christianson  
Bruno Crispo  
Michael Roe

# Contents

Secure Books: Protecting the Distribution of Knowledge <i>Ross J. Anderson, Václav Matyáš Jr., Fabien A. Petitcolas Iain E. Buchan and Rudolf Hanka</i> .....	1
Protocols Using Anonymous Connections: Mobile Applications <i>Michael G. Reed, Paul F. Syverson and David M. Goldschlag</i> .....	13
Receipt-Free Electronic Voting Schemes for Large Scale Elections <i>Tatsuaki Okamoto</i> .....	25
Flexible Internet Secure Transactions Based on Collaborative Domains <i>Eduardo Solana, Jürgen Harms</i> .....	37
How to Build Evidence in a Public-Key Infrastructure for Multi-domain Environments <i>Bruno Crispo</i> .....	53
On Signature Schemes with Threshold Verification Detecting Malicious Verifiers <i>Holger Petersen, Markus Michels</i> .....	67
Open Key Exchange: How to Defeat Dictionary Attacks Without Encrypting Public Keys <i>Stefan Lucks</i> .....	79
Protocol Interactions and the Chosen Protocol Attack <i>John Kelsey, Bruce Schneier and David Wagner</i> .....	91
Binding Bit Patterns to Real World Entities <i>Bruce Christianson, James A. Malcolm</i> .....	105
Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient Faults <i>Feng Bao, Robert H. Deng, Yong F. Han, Albert B.R. Jeng, Arcot D. Narasimhalu and Teow H. Ngair</i> .....	115
Low Cost Attacks on Tamper Resistant Devices <i>Ross J. Anderson, Markus Kuhn</i> .....	125
Entity Authentication and Authenticated Key Transport Protocols Employing Asymmetric Techniques <i>Simon Blake-Wilson, Alfred Menezes</i> .....	137

SG Logic - A Formal Analysis Technique for Authentication Protocols <i>Sigrid Gürgens</i> .....	159
How to Convert any Digital Signature Scheme into a Group Signature Scheme <i>Holger Petersen</i> .....	177
Threshold Key-Recovery Systems for RSA <i>Tatsuaki Okamoto</i> .....	191
A Weakness of the Menezes-Vanstone Cryptosystem <i>Klaus Kiefer</i> .....	201
On Ideal Non-perfect Secret Sharing Schemes <i>Pascal Paillier</i> .....	207
<b>Author Index</b> .....	<b>217</b>