

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Refik Molva Gene Tsudik
Dirk Westhoff (Eds.)

Security and Privacy in Ad-hoc and Sensor Networks

Second European Workshop, ESAS 2005
Visegrad, Hungary, July 13-14, 2005
Revised Selected Papers



Springer

Volume Editors

Refik Molva
Institut Eurécom
2229 Route des Crêtes
06560 Valbonne Sophia Antipolis, France
E-mail: molva@eurecom.fr

Gene Tsudik
University of California, Irvine
Computer Science Department
Irvine CA 92697-3425, USA
E-mail: gts@ics.uci.edu

Dirk Westhoff
NEC Europe Ltd., Network Laboratories
Kurfürsten-Anlage 36
69115 Heidelberg, Germany
E-mail: dirk.westhoff@netlab.nec.de

Library of Congress Control Number: 2005937512

CR Subject Classification (1998): E.3, C.2, F.2, H.4, D.4.6, K.6.5

ISSN 0302-9743
ISBN-10 3-540-30912-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-30912-3 Springer 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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2005
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11601494 06/3142 5 4 3 2 1 0

Preface

It was a pleasure to take part in the 2005 European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS 2005), held on July 13–14 in Visegrad (Hungary) in conjunction with the First International Conference on Wireless Internet (WICON) <<http://www.wicon.org/>>.

As Program Co-chairs, we are very happy with the outcome of this year's ESAS workshop. It clearly demonstrates the continued importance, popularity and timeliness of the workshop's topic: security and privacy in ad hoc and sensor networks. A total of 51 full papers were submitted. Each submission was reviewed by at least three expert referees. After a short period of intense discussions and deliberations, the Program Committee selected 17 papers for presentation and subsequent publication in the workshop proceedings. This corresponds to an acceptance rate of 33% — a respectable rate by any measure.

First and foremost, we thank the authors of ALL submitted papers. Your confidence in this venue is much appreciated. We hope that you will continue patronizing ESAS as authors and attendees. We are also very grateful to our colleagues in the research community who served on the ESAS Program Committee. Your selfless dedication is what makes the workshop a success.

Finally, we are very grateful to the ESAS Steering Group: Levente Buttyan, Claude Castelluccia, Dirk Westhoff and Susanne Wetzel. They had the vision and the drive to create this workshop in the first place; they also provided many insights and lots of help with this year's event. We especially acknowledge and appreciate the work of Levente Buttyan whose dedication (as Steering Committee member, PC member and Local Arrangements Chair) played a very important role in the success of the workshop.

September 2005

Refik Molva
Gene Tsudik

Organization

Program Chairs

Refik Molva, Eurecom, France

Gene Tsudik, UC Irvine, USA

Program Committee

Imad Aad, EPFL, Switzerland

N. Asokan, Nokia, Finland

Sonja Buchegger, UC Berkeley, USA

Laurent Bussard, Microsoft, Germany

Levente Buttyán, BUTE, CrySyS Lab, Hungary

Srdjan Capkun, UCLA, USA

Claude Castelluccia, INRIA, France

Hannes Hartenstein, University of Karlsruhe, Germany

Yih-Chun Hu, UC Berkeley, USA

Markus Jakobsson, Indiana University, Bloomington, USA

Yongdae Kim, University of Minnesota, Minneapolis, USA

Stefan Lucks, University of Mannheim, Germany

Breno de Medeiros, Florida State University, USA

Ludovic M, Supelec, France

Gabriel Montenegro, SunLabs, USA

Cristina Nita-Rotaru, Purdue University, USA

Guevara Noubir, Northeastern University, USA

Kaisa Nyberg, Nokia, Finland

Christof Paar, University of Bochum, Germany

Panagiotis Papadimitratos, Cornell University, USA

Andre Weimerskirch, University of Bochum, Germany

Dirk Westhoff, NEC Europe Network Lab., Germany

Susanne Wetzel, Stevens Institute of Technology, USA

Workshop Organizers

Levente Buttyán, Budapest University of Technology and Economics, Hungary
(buttyan@crysys.hu)

Claude Castelluccia, INRIA, France (Claude.Castelluccia@inrialpes.fr)

Dirk Westhoff, NEC Europe Network Lab., Heidelberg, Germany
(Dirk.Westhoff@netlab.nec.de)

Susanne Wetzel, Stevens Institute of Technology, USA (swetzel@cs.stevens.edu)

Table of Contents

Efficient Verifiable Ring Encryption for Ad Hoc Groups <i>Joseph K. Liu, Patrick P. Tsang, Duncan S. Wong</i>	1
SKiMPy: A Simple Key Management Protocol for MANETs in Emergency and Rescue Operations <i>Matija Pužar, Jon Andersson, Thomas Plagemann, Yves Roudier</i> . . .	14
Remote Software-Based Attestation for Wireless Sensors <i>Mark Shaneck, Karthikeyan Mahadevan, Vishal Kher, Yongdae Kim</i>	27
Spontaneous Cooperation in Multi-domain Sensor Networks <i>Levente Buttyán, Tamás Holczer, Péter Schaffer</i>	42
Authenticated Queries in Sensor Networks <i>Zinaida Benenson</i>	54
Improving Sensor Network Security with Information Quality <i>Qiang Qiu, Tieyan Li, Jit Biswas</i>	68
One-Time Sensors: A Novel Concept to Mitigate Node-Capture Attacks <i>Kemal Bicakci, Chandana Gamage, Bruno Crispo, Andrew S. Tanenbaum</i>	80
Randomized Grid Based Scheme for Wireless Sensor Network <i>Mohammed Golam Sadi, Jong Sou Park, Dong Seong Kim</i>	91
Influence of Falsified Position Data on Geographic Ad-Hoc Routing <i>Tim Leinmüller, Elmar Schoch, Frank Kargl, Christian Maihöfer</i> . . .	102
Provable Security of On-Demand Distance Vector Routing in Wireless Ad Hoc Networks <i>Gergely Ács, Levente Buttyán, István Vajda</i>	113
Statistical Wormhole Detection in Sensor Networks <i>Levente Buttyán, László Dóra, István Vajda</i>	128
RFID System with Fairness Within the Framework of Security and Privacy <i>Jin Kwak, Keunwoo Rhee, Soohyun oh, Seungjoo Kim, Dongho Won</i>	142

Scalable and Flexible Privacy Protection Scheme for RFID Systems <i>Sang-Soo Yeo, Sung Kwon Kim</i>	153
RFID Authentication Protocol with Strong Resistance Against Traceability and Denial of Service Attacks <i>Jeonil Kang, DaeHun Nyang</i>	164
Location Privacy in Bluetooth <i>Ford-Long Wong, Frank Stajano</i>	176
An Advanced Method for Joint Scalar Multiplications on Memory Constraint Devices <i>Erik Dahmen, Katsuyuki Okeya, Tsuyoshi Takagi</i>	189
Side Channel Attacks on Message Authentication Codes <i>Katsuyuki Okeya, Tetsu Iwata</i>	205
Author Index	219