

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

University of California, Los Angeles, CA, 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

Levente Buttyán Virgil Gligor
Dirk Westhoff (Eds.)

Security and Privacy in Ad-Hoc and Sensor Networks

Third European Workshop, ESAS 2006
Hamburg, Germany, September 20-21, 2006
Revised Selected Papers

Volume Editors

Levente Buttyán

Budapest University of Technology and Economics

BME-HIT, PO Box 91, 1521 Budapest, Hungary

E-mail: buttyan@crysys.hu

Virgil Gligor

University of Maryland

Electrical and Computer Engineering Department

College Park, Maryland 20741, USA

E-mail: gligor@umd.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: Applied for

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

LNCS Sublibrary: SL 5 – Computer Communication Networks
and Telecommunications

ISSN 0302-9743

ISBN-10 3-540-69172-3 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-69172-3 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 2006

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 11964254 06/3142 5 4 3 2 1 0

Preface

These proceedings contain the papers of the 3rd European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS 2006), which was held in Hamburg, Germany, September 20–21, 2006, in conjunction with the 11th European Symposium on Research in Computer Security (ESORICS 2006).

This year, a total of 44 full papers were submitted to ESAS. Each submitted paper was reviewed by at least three expert referees. After a short period of discussion and deliberation, the Program Committee selected 14 papers for presentation and subsequent publication in the workshop proceedings. This corresponds to an acceptance rate of 32% – a respectable rate by any measure.

In addition to the presented papers, this year’s workshop also featured two keynote speeches and seven project presentations. In the first keynote, Jean-Pierre Hubaux (EPFL) gave an overview of “Security and Cooperation in Wireless Networks”. The second keynote was given by Pim Tuyls (Philips) on the interesting topic of “Grey-Box Cryptography: Physical Unclonable Functions”. The project presentations covered the following European Projects: S3MS, SeVeCom, BIONETS, CASCADAS, MOBIUS, EYES and UbiSecSens. Unfortunately, the extended abstracts of these presentations could not be included in the proceedings.

As the Chairs of ESAS 2006, we are very happy with the outcome of the workshop that clearly demonstrates the continued importance, popularity, and timeliness of the topic: Security and Privacy in Ad Hoc and Sensor Networks.

Many people contributed to the success of ESAS 2006. First of all, we are thankful to the authors of the submitted papers for their confidence in this venue. We are also grateful to the members of the Program Committee for reviewing the submitted papers and for putting together the workshop program. The following external experts helped the work of the Program Committee in the reviewing process: Asmaa Adnane, Frederik Armknecht, Jared Cordasco, Stefano Crosta, Laszlo Csik, Ari Juels, Jerome Lebeque, Jin Wook Lee, Marcin Poturski, Maxim Raya, and Liu Yang; we appreciate their contribution very much.

We are also thankful to the participants of the workshop in particular, to the keynote speakers, the session chairs, and to those who presented their papers or their projects. Many thanks go to the organizers of ESORICS for accommodating ESAS and taking care of the logistics. We are thankful to Claude Castelluccia and Susanne Wetzel for serving as Publicity Chairs, and to Gergely Acs for maintaining the Web site of ESAS 2006 (www.crysys.hu/ESAS2006). Finally, we are grateful to NEC Europe for sponsoring the workshop and to Springer for publishing the proceedings.

Levente Buttyan (Program Co-chair)
Virgil Gligor (Program Co-chair)
Dirk Westhoff (General Chair)

Organization

General Chair

Dirk Westhoff, NEC Europe Network Lab, Germany

Program Chairs

Levente Buttyán, BME, CrySyS Lab, Hungary

Virgil Gligor, University of Maryland, USA

Publicity Chairs

Claude Castelluccia, INRIA, France

Susanne Wetzels, Stevens Institute of Technology, USA

Program Committee

Imad Aad, DoCoMo Lab Europe, Germany

N. Asokan, Nokia, Finland

Sonja Buchegger, University of California, Berkeley, USA

Srdjan Capkun, Technical University of Denmark, Denmark

Claude Castelluccia, INRIA, France

Xuhua Ding, Singapore Management University, Singapore

Roberto Di Pietro, Università “di Roma La Sapienza”, Italy

Hannes Hartenstein, University of Karlsruhe, Germany

Yih-Chun Hu, University of Illinois UC, USA

Markus Jakobsson, Indiana University, Bloomington, USA

Frank Kargl, University of Ulm, Germany

Yongdae Kim, University of Minnesota, Minneapolis, USA

Breno de Medeiros, Florida State University, USA

Ludovic Me, Supelec, France

Pietro Michiardi, Eurecom, France

Gabriel Montenegro, Microsoft, USA

Cristina Nita-Rotaru, Purdue University, USA

Guevara Noubir, Northeastern University, USA

Kaisa Nyberg, Helsinki University of Technology, Finland

Panagiotis Papadimitratos, EPFL, Switzerland

Adrian Perrig, Carnegie Mellon University, USA

Radha Poovendran, University of Washington, USA

Frank Stajano, Cambridge University, UK

VIII Organization

Andre Weimerskirch, escrypt GmbH - Embedded Security, Germany
Dirk Westhoff, NEC Europe Network Lab, Germany
Susanne Wetzel, Stevens Institute of Technology, USA
Jeong Hyun Yi, Samsung Advanced Institute of Technology, Korea
Imad Aad, DoCoMo Lab Europe, Germany

Table of Contents

Abstracts of Invited Talks

Security and Cooperation in Wireless Networks	1
<i>Jean-Pierre Hubaux</i>	
Grey-Box Cryptography: Physical Unclonable Functions	3
<i>Pim Tuyls</i>	

Regular Papers

Low-Cost Elliptic Curve Cryptography for Wireless Sensor Networks . . .	6
<i>Lejla Batina, Nele Mentens, Kazuo Sakiyama, Bart Preneel,</i> <i>and Ingrid Verbauwhede</i>	
Re-visited: Denial of Service Resilient Access Control for Wireless Sensor Networks	18
<i>Frederik Armknecht, Joao Girao, Marc Stoecklin,</i> <i>and Dirk Westhoff</i>	
Tiny 3-TLS: A Trust Delegation Protocol for Wireless Sensor Networks	32
<i>Sepideh Fouladgar, Bastien Mainaud, Khaled Masmoudi,</i> <i>and Hossam Afifi</i>	
Impact of Pseudonym Changes on Geographic Routing in VANETs	43
<i>Elmar Schoch, Frank Kargl, Tim Leinmüller, Stefan Schlott,</i> <i>and Panos Papadimitratos</i>	
Identification in Infrastructureless Networks	58
<i>Gina Kounqa and Thomas Walter</i>	
Two's Company, Three Is a Crowd: A Group-Admission Protocol for WSNs	70
<i>Joao Girao and Miquel Martin</i>	
So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks	83
<i>Jolyon Clulow, Gerhard P. Hancke, Markus G. Kuhn,</i> <i>and Tyler Moore</i>	
Dynamics of Learning Algorithms for the On-Demand Secure Byzantine Routing Protocol	98
<i>Baruch Awerbuch, Robert G. Cole, Reza Curtmola, David Holmer,</i> <i>and Herbert Rubens</i>	

On the Wiretap Channel Induced by Noisy Tags	113
<i>Julien Bringer and Hervé Chabanne</i>	
On Optimality of Key Pre-distribution Schemes for Distributed Sensor Networks	121
<i>Subhas Kumar Ghosh</i>	
Cryptographic Protocol to Establish Trusted History of Interactions	136
<i>Samuel Galice, Marine Minier, John Mullins, and Stéphane Ubéda</i>	
Ad Hoc Security Associations for Groups	150
<i>Jukka Valkonen, N. Asokan, and Kaisa Nyberg</i>	
Verifiable Agreement: Limits of Non-repudiation in Mobile Peer-to-Peer Ad Hoc Networks	165
<i>Zinaida Benenson, Felix C. Freiling, Birgit Pfitzmann, Christian Rohner, and Michael Waidner</i>	
Using Radio Device Fingerprinting for the Detection of Impersonation and Sybil Attacks in Wireless Networks	179
<i>Bartłomiej Sieka</i>	
Author Index	193