

*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*

Frank Stajano Catherine Meadows  
Srdjan Capkun Tyler Moore (Eds.)

# Security and Privacy in Ad-hoc and Sensor Networks

4th European Workshop, ESAS 2007  
Cambridge, UK, July 2-3, 2007  
Proceedings

## Volume Editors

Frank Stajano  
Tyler Moore  
Computer Laboratory  
University of Cambridge  
Cambridge, UK  
E-mail: Frank.Stajano,Tyler.Moore@cl.cam.ac.uk

Catherine Meadows  
Center for High Assurance Computer Systems  
Naval Research Laboratory  
Washington, DC, USA  
E-mail: meadows@itd.nrl.navy.mil

Srdjan Capkun  
System Security Group  
ETH Zurich, Switzerland  
E-mail: capkuns@inf.ethz.ch

Library of Congress Control Number: 2007929079

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 3-540-73274-8 Springer Berlin Heidelberg New York  
ISBN-13 978-3-540-73274-7 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](http://springer.com)

© Springer-Verlag Berlin Heidelberg 2007  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper SPIN: 12082339 06/3180 5 4 3 2 1 0

# Preface

You hold in your hands the proceedings of ESAS 2007, the Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks. The workshop took place in Cambridge, UK, on the 2<sup>nd</sup> and 3<sup>rd</sup> of July 2007.

The workshop was European in name and location but it was definitely transatlantic in scope. We had a program chair from Europe and one from the USA, and membership of our program committee was almost evenly split between those two regions. When looking at participation, the workshop was even more global than that: the submitted papers came from 25 countries in 6 continents.

We received 87 submissions. After quick-rejecting 5 papers deemed to be out of scope, the remaining 82 papers were each reviewed by at least three PC members. The two program chairs, who did not submit any works, had sole authority to decide which papers to accept and reject, based only on the directive that quality had to be the primary criterion, in order to form a proceedings volume of high international relevance. The number of papers to be accepted was not set in advance: it was selected a posteriori so as to include only solid, innovative and insightful papers. The resulting acceptance rate of about 20%, very strict for a workshop, is a testimonial of how selective we chose to be in accepting only high quality papers. Congratulations to the authors published in this volume!

We arranged the accepted papers in the following sessions:

- Device Pairing
- Key Management
- Location Verification and Location Privacy
- Secure Routing and Forwarding
- Physical Security
- Detection of Compromise, and Revocation

As well as the 17 talks corresponding to the peer-reviewed papers, the workshop program also comprised a keynote talk by Paul Wilson and closed with a rump session in which attendees reported on late-breaking results. Since we went to press well ahead of the event, none of these additional talks are written up in this volume of workshop proceedings.

We are extremely grateful to many people and institutions who helped us make ESAS 2007 a reality. First and foremost, thank you to all the authors who submitted papers to the workshop and to everyone who attended, whether as a presenter or just a member of the audience. Special thanks to our keynote speaker Paul Wilson for giving us a wider perspective on the topics discussed at the workshop. Thanks to our sponsors, Microsoft Research, whose contribution allowed us among other things to endow some student bursaries. Thanks to

the program committee members and to the additional reviewers for providing insightful comments about all the submitted papers. On the organizational side, thanks to publicity chair João Girão for attracting so many submissions and for managing the workshop Web site, to Kasper Bonne Rasmussen for managing the submission server and to Carol Speed at Cambridge for helping with the back-end of the payment system.

In closing, we note that this fourth one in Cambridge was the last ESAS workshop under this name. If you share our feelings, you will have noticed that there are really too many security workshops and conferences nowadays: it's impossible to follow them all and it gets harder and harder to put together a quality program. So we encourage our community to take part in a global spring cleaning effort to reduce the number of events; from our side, we (or more precisely our steering committee) have merged ESAS with ACM SASN (Workshop on Security of Ad Hoc and Sensor Networks) and ACM WiSe (Workshop on Wireless Security) to become **WiSec**, the ACM Wireless Security Conference. Joining forces and avoiding duplication makes sense: having fewer but higher-profile events will raise the quality of the submitted papers by avoiding dilution and will make us all more likely to meet the key people in our community whenever we attend. WiSec will alternate between the US and Europe, starting in the US in 2008. See you there!

April 2007

Frank Stajano  
Cathy Meadows  
Srdjan Capkun  
Tyler Moore



Lejla Batina	ESAT SCD/COSIC, Belgium
Levente Buttyán	Budapest University of Technology and Economics, Hungary
Mario Cagalj	University of Split, Croatia
Claude Castelluccia	INRIA, France
Xuhua Ding	Singapore Management University, Singapore
Saurabh Ganerival	Google, USA
Virgil Gligor	University of Maryland, College Park, USA
Christian D. Jensen	Technical University of Denmark, Denmark
Markus Kuhn	University of Cambridge, UK
Loukas Lazos	University of Washington, USA
Wenke Lee	Georgia Institute of Technology, USA
Mingyan Li	Boeing, USA
Donggang Liu	University of Texas at Arlington, USA
Refik Molva	Institute Eurocom, France
Peng Ning	NC State, USA
Kaisa Nyberg	Helsinki University of Technology, Finland
Radha Poovendran	University of Washington, USA
Michael Roe	Microsoft Research, Cambridge, UK
Mani Srivastava	UCLA, USA
Dirk Westhoff	NEC Europe Network Lab, Germany
Susanne Wetzel	Stevens Institute of Technology, USA

## Additional Referees

Gergely Ács	Aurélien Francillon	Dave Singelée
Frederik Armknecht	Alban Hessler	Claudio Soriente
Farshad Bahari	Maarit Hietalahti	Gelareh Taban
Aldar Chan	Tamás Holczer	Patrick Tague
Jared Cordasco	Sotiris Ioannidis	Slim Trabelsi
László Csik	Frank Kargl	Liu Yang
Christophe De Cannière	Nitesh Saxena	Yanjiang Yang
Qi Dong	Stefaan Seys	Fan Zhang
László Dóra	Abdullatif Shikfa	

## Sponsoring Institutions

### Gold Sponsor

Microsoft Research Cambridge, UK

# Table of Contents

## Device Pairing

The Candidate Key Protocol for Generating Secret Shared Keys from Similar Sensor Data Streams . . . . .	1
<i>Rene Mayrhofer</i>	
The Martini Synch: Joint Fuzzy Hashing Via Error Correction . . . . .	16
<i>Darko Kirovski, Michael Sinclair, and David Wilson</i>	
Private Handshakes . . . . .	31
<i>Jaap-Henk Hoepman</i>	
Security Associations in Personal Networks: A Comparative Analysis . . .	43
<i>Jani Suomalainen, Jukka Valkonen, and N. Asokan</i>	

## Key Management

Key Establishment in Heterogeneous Self-organized Networks . . . . .	58
<i>Gelareh Taban and Rei Safavi-Naini</i>	
Enabling Full-Size Public-Key Algorithms on 8-bit Sensor Nodes . . . . .	73
<i>Leif Uhsadel, Axel Poschmann, and Christof Paar</i>	
Key Distribution in Mobile Ad Hoc Networks Based on Message Relaying . . . . .	87
<i>Johann van der Merwe, Dawoud Dawoud, and Stephen McDonald</i>	

## Location Verification and Location Privacy

Distance Bounding in Noisy Environments . . . . .	101
<i>Dave Singelée and Bart Preneel</i>	
Multiple Target Localisation in Sensor Networks with Location Privacy . . . . .	116
<i>Matthew Roughan and Jon Arnold</i>	
On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs . . . . .	129
<i>Levente Buttyán, Tamás Holczer, and István Vajda</i>	

## Secure Routing and Forwarding

“End-by-Hop” Data Integrity . . . . .	142
<i>Stephen Farrell and Christian D. Jensen</i>	



Authenticating DSR Using a Novel Multisignature Scheme Based on Cubic LFSR Sequences ..... 156  
*Saikat Chakrabarti, Santosh Chandrasekhar, Mukesh Singhal, and Kenneth L. Calvert*

**Physical Security**

Security for Mobile Low Power Nodes in a Personal Area Network by Means of Trusted Platform Modules ..... 172  
*Ulrich Grossmann, Enrik Berkhan, Luciana C. Jatoba, Joerg Ottenbacher, Wilhelm Stork, and Klaus D. Mueller-Glaser*

ALGSICS — Combining Physics and Cryptography to Enhance Security and Privacy in RFID Systems ..... 187  
*Neil Bird, Claudine Conrado, Jorge Guajardo, Stefan Maubach, Geert-Jan Schrijen, Boris Skoric, Anton M.H. Tombreur, Peter Thueringer, and Pim Tuyls*

**Detection of Compromise, and Revocation**

Detecting Node Compromise in Hybrid Wireless Sensor Networks Using Attestation Techniques ..... 203  
*Christoph Krauß, Frederic Stumpf, and Claudia Eckert*

Direct Anonymous Attestation (DAA): Ensuring Privacy with Corrupt Administrators ..... 218  
*Ben Smyth, Mark Ryan, and Liqun Chen*

New Strategies for Revocation in Ad-Hoc Networks ..... 232  
*Tyler Moore, Jolyon Clulow, Shishir Nagaraja, and Ross Anderson*

**Author Index** ..... 247