Lecture Notes in Computer Science 4572

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

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^{nd} and 3^{rd} 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

Organization

ESAS 2007 was hosted by the Security Group of the Computer Laboratory of the University of Cambridge and took place in Sidney Sussex College, Cambridge.

General Chair

Frank Stajano	University of Cambridge, UK

Program Co-chairs

Catherine Meadows	Naval Research Laboratory, USA
Srdjan Capkun	ETH Zurich, Switzerland

Local Arrangements Chair

Tyler Moore	University of Cambridge, UK

Publicity Chair

João Girão	NEC Europe Network Lab, Germany

Steering Committee

Levente Buttyán	Budapest University of Technology and Economics, Hungary
Claude Castelluccia	INRIA, France
Dirk Westhoff	NEC Europe Network Lab, Germany

Webmasters

João Girão	NEC Europe Network Lab, Germany
Kasper Bonne Rasmussen	ETH Zurich, Switzerland
Tyler Moore	University of Cambridge, UK

Program Committee

Imad Aad	DoCoMo Lab Europe, Germany
Tansu Alpcan	Deutsche Telekom Laboratories/TU Berlin, Germany
Farooq Anjum	Telcordia Research, USA
N. Asokan	Nokia, Finland
Gildas Avoine	MIT, USA

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 Ganeriwal	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

Physical Security

Detection of Compromise, and Revocation