Lecture Notes in Computer Science 3313

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

Editorial Board

Claude Castelluccia Hannes Hartenstein
Christof Paar Dirk Westhoff (Eds.)

Security in Ad-hoc and Sensor Networks

First European Workshop, ESAS 2004
Heidelberg, Germany, August 6, 2004
Revised Selected Papers

Springer

Volume Editors

Claude Castelluccia
INRIA, Unité de Recherche Rhône-Alpes, France
E-mail: ccastell@ics.uci.edu

Hannes Hartenstein
Universität Karlsruhe (TH), Computing Center and Institute of Telematics
E-mail: hartenstein@rz.uni-karlsruhe.de

Christof Paar
Ruhr-Universität Bochum, Communication Security
44780 Bochum, Germany
E-mail: cpaar@crypto.rub.de

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: 2004117659

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

ISSN 0302-9743
ISBN 3-540-24396-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11377689 06/3142 5 4 3 2 1 0

Claude Castelluccia, Hannes Hartenstein, Christof Paar,
Dirk Westhoff (Eds.)

Security in Ad Hoc and Sensor Networks

First European Workshop, ESAS 2004
Heidelberg, Germany, August 6-6, 2004

Preface

Ad hoc and sensor networks are making their way from research to real-world deployments. Body and personal-area networks, intelligent homes, environmental monitoring or intervehicle communications: there is almost nothing left that is not going to be "smart" and "networked." While a great amount of research has been devoted to the pure networking aspects, ad hoc and sensor networks will not be successfully deployed if security, dependability and privacy issues are not addressed adequately. These issues are very important because ad hoc and sensor networks are usually used for very critical applications. Furthermore, they are very vulnerable because they are, most of the time, deployed in open and unprotected environments.

At ESAS 2004, researchers with interests in both networking and security came together to present and discuss the latest ideas and concepts in the design of secure, dependable and privacy-preserving ad hoc and sensor networks. In the keynote speeches, Jean-Pierre Hubaux (EPFL, Switzerland) discussed the challenges of ad hoc network security, and Antonis Galetsas (European Commission, DG Information Society) presented the current and future activities of the European Commission on these topics.

Out of 55 high-quality submissions, the program committee selected 17 papers for publication. The program covered the full spectrum of security-related issues, including key distribution and management, authentication, energy-aware cryptographic primitives, anonymity/pseudonymity, secure diffusion, secure P2P overlays and RFIDs.

We would like to thank all authors, referees, supporters and workshop participants for making this workshop a successful event. Special thanks to the program committee and further reviewers for their great work and for reviewing the papers in less than 4 weeks. We hope that you will enjoy the ESAS proceedings and your research work will be stimulated.

September 2004

Claude Castelluccia
Hannes Hartenstein
Christof Paar
Dirk Westhoff

Committees

Program Co-chairs

Claude Castelluccia, INRIA, France
Christof Paar, University of Bochum, Germany
Hannes Hartenstein, University of Karlsruhe, Germany
Dirk Westhoff, NEC Europe Ltd., Germany

Program Committee

Nadarajah Asokan, Nokia, Finland
Levente Buttyan, BME-HIT, Hungary
Sonja Buchegger, EPFL, Switzerland
Claudia Eckert, TU Darmstadt, Germany
Stefan Lucks, University of Mannheim, Germany
Refik Molva, Eurécom, France
Gabriel Montenegro, SunLabs, France
Pekka Nikander, Ericsson, Finland
Panagiotis Papadimitratos, Cornell University, USA
Ahmad-Reza Sadeghi, University of Bochum, Germany
Frank Stajano, University of Cambridge, UK
Gene Tsudik, UC Irvine, USA
Andre Weimerskirch, University of Bochum, Germany
Nathalie Weiler, ETH Zuerich, Switzerland
Susanne Wetzel, Stevens Institute of Technology, USA
Manel Guerrero Zapata, University Pompeu Fabra, Barcelona, Spain

Table of Contents