

# Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering

42

## Editorial Board

Ozgur Akan

*Middle East Technical University, Ankara, Turkey*

Paolo Bellavista

*University of Bologna, Italy*

Jiannong Cao

*Hong Kong Polytechnic University, Hong Kong*

Falko Dressler

*University of Erlangen, Germany*

Domenico Ferrari

*Università Cattolica Piacenza, Italy*

Mario Gerla

*UCLA, USA*

Hisashi Kobayashi

*Princeton University, USA*

Sergio Palazzo

*University of Catania, Italy*

Sartaj Sahni

*University of Florida, USA*

Xuemin (Sherman) Shen

*University of Waterloo, Canada*

Mircea Stan

*University of Virginia, USA*

Jia Xiaohua

*City University of Hong Kong, Hong Kong*

Albert Zomaya

*University of Sydney, Australia*

Geoffrey Coulson

*Lancaster University, UK*

Qijun Gu Wanyu Zang Meng Yu (Eds.)

# Security in Emerging Wireless Communication and Networking Systems

First International ICST Workshop, SEWCN 2009  
Athens, Greece, September 14, 2009  
Revised Selected Papers

## Volume Editors

Qijun Gu  
Texas State University-San Marcos  
Department of Computer Science  
601 University Drive  
San Marcos, TX 78666, USA  
E-mail: qijun@txstate.edu

Wanyu Zang  
Meng Yu  
Western Illinois University  
Department of Computer Science  
1 University Circle  
Macomb, IL 61455, USA  
E-mail: {w-zang; m-yu2}@wiu.edu

Library of Congress Control Number: 2009942991

CR Subject Classification (1998): C.2, D.4.6, K.6.5, E.3, G.2, I.1

|         |                                                       |
|---------|-------------------------------------------------------|
| ISSN    | 1867-8211                                             |
| ISBN-10 | 3-642-11525-X Springer Berlin Heidelberg New York     |
| ISBN-13 | 978-3-642-11525-7 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.com

© ICST Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering 2010  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper      SPIN: 12830046      06/3180      5 4 3 2 1 0

# Preface

The First ICST International Workshop on Security in Emerging Wireless Communication and Networking Systems (SEWCN 2009) was held in Athens, Greece, September 14, in conjunction with SecureComm 2009. SEWCN 2009 was sponsored by the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (ICST). The Workshop Chairs were Qijun Gu from Texas State University-San Marcos, USA, and Wanyu Zang from Western Illinois University, USA.

The workshop invited 20 researchers from academia and industry around the world in the areas of networking and security to form the Program Committee. The workshop received nine submissions and each submission received two or three double-blind reviews. The review process started on July 6 and ended on July 27. In all, 21 reviews were received. Based on the review scores and comments, seven papers with average score 0 or better were accepted for presentation and inclusion in the workshop proceedings.

The workshop emphasized new ideas for secure architectures and protocols to enhance the emerging wireless systems. The accepted papers cover topics on applied cryptography, key management, vulnerability analysis, privacy, authentication, and intrusion detection for emerging wireless systems. The papers were presented in two sessions, chaired by Nikolaos Preve from the National Technical University of Athens, Greece, and Theofilos Chrysikos from the University of Patras, Greece.

For the success of SEWCN 2009, we would like to thank the Program Committee and the authors for their work and contributions. We would like to thank the technical sponsors CREATE-NET and ICST for their support and organization. We would also like to thank all the people involved in the organization of the workshop, in particular, the main Conference Chair Peng Liu, the conference coordinators Gergely Nagy, Eszter Hajdu and Effie Makri, and the general Workshop Chair Reza Curtmola.

# Organization

## Workshop Chairs

|            |                                        |
|------------|----------------------------------------|
| Qijun Gu   | Texas State University-San Marcos, USA |
| Wanyu Zang | Western Illinois University, USA       |

## Technical Program Committee

|                       |                                                 |
|-----------------------|-------------------------------------------------|
| Abderrahim Benslimane | University of Avignon, France                   |
| Raheem Beyah          | Georgia State University, USA                   |
| Ioannis Broustis      | University of California, Riverside, USA        |
| Timothy Brown         | University of Colorado at Boulder, USA          |
| Alvaro Cárdenas       | University of California, Berkeley, USA         |
| Hakima Chaouchi       | Institut Telecom, France                        |
| Charles Clancy        | Laboratory for Telecommunications Sciences, USA |
| Sghaier Guizani       | Qatar University, Qatar                         |
| Wolfgang Hommel       | Leibniz Supercomputing Centre, Germany          |
| Jiankun Hu            | RMIT University, Australia                      |
| Salil Kanhere         | University of New South Wales, Australia        |
| Frank Kargl           | Ulm University, Germany                         |
| Costas Lambrinoudakis | University of the Aegean, Greece                |
| Timothy Newman        | Virginia Tech, USA                              |
| Raphael Phan          | Loughborough University, UK                     |
| Elmar Schoch          | Ulm University, Germany                         |
| Gritzalis Stefanos    | University of the Aegean, Greece                |
| Jay-Evan Tevis        | LeTourneau University, USA                      |
| Yang Xiang            | Central Queensland University, Australia        |
| Meng Yu               | Western Illinois University, USA                |

# Table of Contents

## Session 1 - Session Chair: Nikolaos Preve

|                                                                                                                         |    |
|-------------------------------------------------------------------------------------------------------------------------|----|
| A Closed-Form Expression for Outage Secrecy Capacity in Wireless Information-Theoretic Security .....                   | 3  |
| <i>Theofilos Chrysikos, Tasos Dagiuklas, and Stavros Kotsopoulos</i>                                                    |    |
| Enhanced Access Polynomial Based Self-healing Key Distribution .....                                                    | 13 |
| <i>Ratna Dutta, Sourav Mukhopadhyay, and Tom Dowling</i>                                                                |    |
| Security Flaws in an Efficient Pseudo-Random Number Generator for Low-Power Environments .....                          | 25 |
| <i>Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M.E. Tapiador, Enrique San Millán, and Jan C.A. van der Lubbe</i> |    |

## Session 2 - Session Chair: Theofilos Chrysikos

|                                                                                                                                                  |    |
|--------------------------------------------------------------------------------------------------------------------------------------------------|----|
| RSSI-Based User Centric Anonymization for Location Privacy in Vehicular Networks .....                                                           | 39 |
| <i>Yu-Chih Wei, Yi-Ming Chen, and Hwai-Ling Shan</i>                                                                                             |    |
| Integrating Wireless Sensor Networks with Computational Grids .....                                                                              | 53 |
| <i>Nikolaos Preve</i>                                                                                                                            |    |
| Security for Heterogeneous and Ubiquitous Environments Consisting of Resource-Limited Devices: An Approach to Authorization Using Kerberos ..... | 65 |
| <i>Jasone Astorga, Jon Matias, Purificacion Saiz, and Eduardo Jacob</i>                                                                          |    |
| Signalprint-Based Intrusion Detection in Wireless Networks .....                                                                                 | 77 |
| <i>Rob Mitchell, Ing-Ray Chen, and Mohamed Eltoweissy</i>                                                                                        |    |
| Author Index .....                                                                                                                               | 89 |