Lecture Notes in Computer Science 7886

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

Lorenzo Cavallaro Dieter Gollmann (Eds.)

Information Security Theory and Practice.

Security of Mobile and Cyber-Physical Systems

7th IFIP WG 11.2 International Workshop, WISTP 2013
Heraklion, Greece, May 28-30, 2013
Proceedings

Springer

Volume Editors

Lorenzo Cavallaro
Royal Holloway, University of London
Information Security Group
Egham Hill, Egham TW20 0EX, UK
E-mail: lorenzo.cavallaro@rhul.ac.uk

Dieter Gollmann
University of Technology
Institutes of the TU Hamburg-Harburg
Security in Distributed Applications
Harburger Schlossstrasse 20
21079 Hamburg, Germany
E-mail: diego@tuhh.de

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-38529-2 e-ISBN 978-3-642-38530-8
DOI 10.1007/978-3-642-38530-8
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2013938410

CR Subject Classification (1998): E.3, K.6.5, C.5.3, C.3, C.2.0, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

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

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Current developments in IT are characterized by an increasing use of personal mobile devices and a growing reliance on IT for supporting industrial applications in the physical world. A new perspective on socio-technical and cyber-physical systems is required that sees in IT more than just an infrastructure but focuses on the ever closer integration between social and technical processes.

Application markets, such as Google Play and Apple App Store, drive a mobile ecosystem, offering new business models with high turnovers and new opportunities, but at the same time attracting cybercriminals and raising new privacy concerns as well.

In the area of cyber-physical systems, research has to go beyond securing the IT infrastructure to consider attacks launched by combining manipulations in physical space and cyber space.

This seventh edition of WISTP featured a lower number of submissions than previous years, with nine out of 19 papers accepted for inclusion in the workshop and proceedings. Submissions were reviewed by at least three reviewers, in some cases by four. This long and rigorous process was only possible thanks to the hard work of the Program Committee members and additional reviewers, listed on the following pages. In addition, we are pleased that Corrado Leita (Symantec Research Labs) and Lejla Batina (Radboud University Nijmegen) accepted our invitation to speak on challenges and opportunities in securing critical infrastructures and near-field communication privacy threats, respectively.

We wish to thank all the people who invested time and energy to make WISTP 2013 a success: first and foremost come all the authors who submitted papers to WISTP and presented them at the workshop. The members of the Program Committee together with all the external reviewers worked hard in evaluating the submissions. The WISTP Steering Committee helped us graciously in all critical decisions. Thanks also go to the 2013 General Chairs Ioannis Askoxylakis and Louis Marinos, the local organizer Nikolaos Petroulakis and their respective teams for handling the local arrangements, to Symantec Research Labs for co-sponsoring WISTP 2013, to Damien Sauveron for maintaining the conference website, and to Claudio Agostino Ardagna and Mauro Conti for their efforts as Publicity Chairs.

May 2013

Lorenzo Cavallaro
Dieter Gollmann

Organization

WISTP 2013 is organized by FORTH-ICS in cooperation with ENISA.

General Chairs

Ioannis G. Askoxylakis	FORTH-ICS, Greece
Louis Marinos	ENISA, EU

Local Organizer

Nikolaos Petroulakis	FORTH-ICS, Greece

Workshop/Panel/Tutorial Chair

Damien Sauveron	XLIM, University of Limoges, France

Publicity Chairs

Claudio A. Ardagna	Università degli Studi di Milano, Italy
Mauro Conti	University of Padua, Italy

Steering Committee

Ioannis G. Askoxylakis	FORTH-ICS, Greece
Angelos Bilas	FORTH-ICS and University of Crete, Greece
Konstantinos Markantonakis	ISG-SCC, Royal Holloway University of London, UK
Joachim Posegga	Institute of IT-Security and Security Law, Germany
Jean-Jacques Quisquater	DICE, Catholic University of Louvain, Belgium
Damien Sauveron	XLIM, University of Limoges, France

Program Chairs

Lorenzo Cavallaro	Royal Holloway, University of London, UK
Dieter Gollmann	Hamburg University of Technology, Germany

Program Committee

Raja Naeem Akram	Edinburgh Napier University, UK
Claudio A. Ardagna	Università degli Studi di Milano, Italy
Ioannis G. Askoxylakis	FORTH-ICS, Greece
Lejla Batina	Radboud University Nijmegen, The Netherlands
Danilo Bruschi	Università degli Studi di Milano, Italy
Mauro Conti	University of Padua, Italy
Marco Cova	University of Birmingham, UK
Manuel Egele	Carnegie Mellon University, USA
Jaap-Henk Hoepman	Radboud University Nijmegen, The Netherlands
Andrea Lanzi	Insitut Eurecom, France
Corrado Leita	Symantec Research Labs, EU
Federico Maggi	Politecnico di Milano, Italy
Evangelos Markatos	FORTH-ICS, Greece
Lorenzo Martignoni	Google, Switzerland
Sjouke Mauw	University of Luxembourg, Luxembourg
Aikaterini Mitrokotsa	EPFL, Switzerland
Igor Muttik	McAfee Labs, UK
Flemming Nielson	Danish Technical University, Denmark
Wolter Pieters	TU Delft, The Netherlands
Christina Pöpper	ETH Zürich, Switzerland
Joachim Posegga	Institute of IT-Security and Security Law, Germany
Jean-Jacques Quisquater	DICE, Catholic University of Louvain, Belgium
William Robertson	Northeastern University, USA
Pierangela Samarati	Università degli Studi di Milano, Italy
Asia Slowinska	Vrije Universiteit Amsterdam, The Netherlands
Stefano Zanero	Politecnico di Milano, Italy
Jianying Zhou	Institute for Infocomm Research, Singapore

Additional Reviewers

Alessandro Barenghi	Istvan Haller	Maryna Krotofil
Bastian Braun	Jin Han	Mario Leone
Baris Ege	Wafa Ben Jaballah	Henrich C. Pöhls
Sara Foresti	Roman Kochanek	

Scientific Support

IFIP WG 11.2 Pervasive Systems Security

Main Sponsors

Since the early stages of inception of the workshop, organizers received positive feedback from a number of high-profile organizations. With the development of a strong Program and Organizing Committee, this was further capitalized into direct financial support. This enabled the workshop organizers to strengthen significantly their main objective for a high-standard academic workshop. The support helped significantly to keep the workshop registration costs as low as possible and at the same time offer a number of best paper awards.

We are wholeheartedly thankful to our Silver Sponsor Symantec Research Labs for supporting WISTP 2013.

Securing Critical Infrastructures: Challenges and Opportunities

Corrado Leita

Symantec Research Labs

Abstract. The threat landscape is continuously evolving. Large, wide spread worm infections are leaving more and more space to more stealthy attacks targeting highly valuable targets. Industrial control systems (ICS) are rapidly becoming a new major target of cyber-criminals: industrial control systems have converged with standard IT technologies and have brought powerful capabilities into the critical infrastructure environments, along with new and yet undiscovered threats. This was pointed out in multiple occasions over these last years and was confirmed by the discovery of highly sophisticated threats such as Stuxnet, that underlined a completely different threat model when compared to traditional malware witnessed in the wild in previous years. This talk will dive into the challenges and the opportunities associated to ICS security research, and on the tools at our disposal to improve our ability to protect such critical environments.

Near-Field Privacy

Lejla Batina

Radboud University Nijmegen

Abstract. With the expansion of versatile privacy-sensitive RFID applications a clear need for new identification schemes has been established. In particular, new attribute-based authentication schemes as reminiscences of Microsofts U-Prove technology were proposed. We survey related works and discuss a recent scheme for selective disclosure of attributes providing the designation of verification. A scenario of mobile payments is also considered and the use of NFC-enabled phones for proving credentials.

Table of Contents

Cryptography and Cryptanalysis

Multiplicative Homomorphic E-Auction with Formally Provable Security 1
Kun Peng and Matt Henricksen

Malleable Signatures for Resource Constrained Platforms 18
Henrich C. Pöhls, Stefan Peters, Kai Samelin, Joachim Posegga, and Hermann de Meer

Cryptographic Key Exchange in IPv6-Based Low Power, Lossy Networks 34
Panagiotis Ilia, George Oikonomou, and Theo Tryfonas

Mobile Security

URANOS: User-Guided Rewriting for Plugin-Enabled ANdroid ApplicatiOn Security 50
Daniel Schreckling, Stephan Huber, Focke Höhne, and Joachim Posegga

Online Banking with NFC-Enabled Bank Card and NFC-Enabled Smartphone 66
Max Günther and Bernd Borchert

Smart Cards and Embedded Devices

A Defensive Virtual Machine Layer to Counteract Fault Attacks on Java Cards 82
Michael Lackner, Reinhard Berlach, Wolfgang Raschke, Reinhold Weiss, and Christian Steger

A Forward Privacy Model for RFID Authentication Protocols 98
Daisuke Moriyama, Miyako Ohkubo, and Shin'ichiro Matsuo

On Secure Embedded Token Design: Quasi-looped Yao Circuits and Bounded Leakage 112
Simon Hoerder, Kimmo Järvinen, and Daniel Page

Lightweight Authentication Protocol for Low-Cost RFID Tags 129
Pierre Dusart and Sinaly Traoré

Author Index 145