

Editor-in-Chief

A. Joe Turner, Seneca, SC, USA

Editorial Board

Foundations of Computer Science

Mike Hinchey, Lero, Limerick, Ireland

Software: Theory and Practice

Michael Goedicke, University of Duisburg-Essen, Germany

Education

Arthur Tatnall, Victoria University, Melbourne, Australia

Information Technology Applications

Ronald Waxman, EDA Standards Consulting, Beachwood, OH, USA

Communication Systems

Guy Leduc, Université de Liège, Belgium

System Modeling and Optimization

Jacques Henry, Université de Bordeaux, France

Information Systems

Jan Pries-Heje, Roskilde University, Denmark

ICT and Society

Jackie Phahlamohlaka, CSIR, Pretoria, South Africa

Computer Systems Technology

Paolo Prinetto, Politecnico di Torino, Italy

Security and Privacy Protection in Information Processing Systems

Kai Rannenberg, Goethe University Frankfurt, Germany

Artificial Intelligence

Tharam Dillon, Curtin University, Bentley, Australia

Human-Computer Interaction

Annelise Mark Pejtersen, Center of Cognitive Systems Engineering, Denmark

Entertainment Computing

Ryohei Nakatsu, National University of Singapore

IFIP – The International Federation for Information Processing

IFIP was founded in 1960 under the auspices of UNESCO, following the First World Computer Congress held in Paris the previous year. An umbrella organization for societies working in information processing, IFIP's aim is two-fold: to support information processing within its member countries and to encourage technology transfer to developing nations. As its mission statement clearly states,

IFIP's mission is to be the leading, truly international, apolitical organization which encourages and assists in the development, exploitation and application of information technology for the benefit of all people.

IFIP is a non-profitmaking organization, run almost solely by 2500 volunteers. It operates through a number of technical committees, which organize events and publications. IFIP's events range from an international congress to local seminars, but the most important are:

- The IFIP World Computer Congress, held every second year;
- Open conferences;
- Working conferences.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is small and by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is less rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

Any national society whose primary activity is in information may apply to become a full member of IFIP, although full membership is restricted to one society per country. Full members are entitled to vote at the annual General Assembly. National societies preferring a less committed involvement may apply for associate or corresponding membership. Associate members enjoy the same benefits as full members, but without voting rights. Corresponding members are not represented in IFIP bodies. Affiliated membership is open to non-national societies, and individual and honorary membership schemes are also offered.

Dimitris Gritzalis Steven Furnell
Marianthi Theoharidou (Eds.)

Information Security and Privacy Research

27th IFIP TC 11 Information Security
and Privacy Conference, SEC 2012
Heraklion, Crete, Greece, June 4-6, 2012
Proceedings

Volume Editors

Dimitris Gritzalis

Marianthi Theoharidou

Athens University of Economics and Business, Department of Informatics
Information Security and Critical Infrastructure Protection Research Group
76 Patisision Ave., 10434 Athens, Greece

E-mail: {dgrit,mtheohar}@aueb.gr

Steven Furnell

University of Plymouth

School of Computing Communications and Electronics

A310, Portland Square, Drake Circus, Plymouth, PL4 8AA, UK

E-mail: s.furnell@plymouth.ac.uk

ISSN 1868-4238

ISBN 978-3-642-30435-4

DOI 10.1007/978-3-642-30436-1

Springer Heidelberg Dordrecht London New York

e-ISSN 1868-422X

e-ISBN 978-3-642-30436-1

Library of Congress Control Number: 2012937786

CR Subject Classification (1998): C.2, K.6.5, D.4.6, E.3, H.4, J.1

© IFIP International Federation for Information Processing 2012

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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

It was an honor and a privilege to chair the 27th IFIP International Information Security Conference (SEC 2012), a 29-year old event that has already become a tradition for information security professionals around the world. SEC 2012 was organized by Technical Committee 11 (TC-11) of IFIP and this year took place on the Greek island of Crete, during June 4–6, 2012. As Program Committee Chairs, we were extremely pleased to serve a conference in a location with such natural beauty, and where the hospitality and friendliness of the people have been going together, hand-in-hand, with its very long history.

This volume contains the papers selected for presentation at SEC 2012, which proved to be a really competitive forum. After a first check by the PC chairs on meeting the submission criteria, scope and quality, 115 of the 167 initially submitted papers were then sent out for review by the conference Program Committee. All of these 115 papers were evaluated on the basis of their novelty and technical quality, and reviewed by at least two members of the program committee. Of these 115 papers, finally 42 were accepted as full papers. A further 11 submissions were accepted as short papers.

It is thanks to the commitment of several people that international conferences are able to happen. This holds true also for SEC 2012. The full list of individuals that volunteered their time and energy to help is really long, and we would like to express our sincere appreciation to the members of the Program Committee, to the external reviewers, and to the authors, who trusted their work in our hands. Many thanks go, also, to all conference attendees.

In particular, we would like to thank our distinguished keynote speaker, Udo Helmbrecht (ENISA) for accepting our invitation and honoring the conference with his presence and inspired talk. We also thank the local organizers and hosts, first among them being the Organizing Committee Chairs Marianthi Theoharidou and Nickolas Kyrloglou, as well as the Publicity Chair Sara Foresti, who took care of every detail to ensure that SEC 2012 would become a successful and memorable event. Our further appreciation also goes to Marianthi for strongly supporting us in the preparation and editing of this conference proceedings volume.

Finally, let us express a personal note. We would like to thank all TC-11 members for giving us the opportunity to serve SEC 2012 as Program Committee Chairs. It was the first time this opportunity is given to Steven Furnell. It was the fourth time, following events in Samos (SEC 1996), Athens (SEC 2003) and Pafos (SEC 2009), that this opportunity was given to Dimitris Gritzalis, who has thus further extended his record as a SEC conference chairing “dinosaur”.

Dimitris Gritzalis
Steven Furnell

Organization

Committees

General Chair

Sokratis Katsikas University of Piraeus, Greece

Program Chairs

Dimitris Gritzalis Athens University of Economics and Business,
Greece
Steven Furnell Plymouth University, (UK)

Organizing Committee Chairs

Marianthi Theoharidou Athens University of Economics and Business,
Greece
Nikolaos Kyrloglou Athens Chamber of Commerce and Industry,
Greece

Publicity Chair

Sara Foresti Università degli studi di Milano, Italy

Program Committee

Vijay Atluri Rutgers University, USA
Joachim Biskup University of Dortmund, Germany
Jan Camenisch IBM Research, Switzerland
Sabrina De Capitani
 di Vimercati Università degli studi di Milano, Italy
Nathan Clarke Plymouth University, UK
Jeff Crume IBM, USA
Frederic Cuppens TELECOM Bretagne, France
Nora Cuppens UEB, France
Bart De Decker K.U. Leuven, Belgium
Gurpreet Dhillon Virginia C/wealth University, USA
Theo Dimitrakos BT, UK
Ronald Dodge US Military Academy, USA
Simone Fischer-Huebner Karlstadt University, Sweden
Dieter Gollmann Hamburg University of Technology, Germany

VIII Organization

Jaap-Henk Hoepman	TNO and Radboud University Nijmegen, The Netherlands
Thorsten Holz	Ruhr University Bochum, Germany
Sotiris Ioannidis	FORTH, Greece
Bart Jacobs	Radboud University Nijmegen, The Netherlands
Sushil Jajodia	George Mason University, USA
Lech Janczewski	University of Auckland, New Zealand
Tom Karygiannis	NIST, USA
Vasilios Katos	University of Thrace, Greece
Panagiotis Katsaros	University of Thessaloniki, Greece
Stefan Katzenbeisser	T.U. Darmstadt, Germany
Dogan Kesdogan	University of Siegen, Germany
Costas Lambrinouidakis	University of Piraeus, Greece
Carl Landwehr	University of Maryland, USA
Ronald Leenes	Tilburg University, The Netherlands
Javier Lopez	University of Malaga, Spain
Evangelos Markatos	FORTH and University of Crete, Greece
Stephen Marsh	Communications Research Center, Canada
Ioannis Mavridis	University of Macedonia, Greece
Natalia Miloslavskaya	National Nuclear Research University, Russia
Yuko Murayama	Iwate Prefectural University, Japan
Eiji Okamoto	University of Tsukuba, Japan
Martin Olivier	University of Pretoria, South Africa
Evangelos Ouzounis	ENISA, (EU)
Jakob Illeborg Pagter	Alexandra Instituttet, Denmark
Maria Papadaki	Plymouth University, UK
Philippos Peleties	USB Bank, Cyprus
Sihan Qing	Chinese Academy of Sciences, China
Muttukrishnan Rajarajan	City University, UK
Kai Rannenber	Goethe University Frankfurt, Germany
Carlos Rieder	HSW Luzern, Switzerland
Pierangela Samarati	Università degli studi di Milano, Italy
Ryoichi Sasaki	Tokyo Denki University, Japan
Ingrid Schaumüller-Bichl	UAS Hagenberg, Austria
Anne Karen Seip	Finanstilsynet, Norway
Rossouw Von Solms	NMMU, South Africa
Theo Tryfonas	University of Bristol, UK
Craig Valli	Edith Cowan University, Australia
Jozef Vyskoc	VaF, Slovakia
Christian Weber	WebITsec, Germany
Tatjana Welzer	University of Maribor, Slovenia
Dirk Westhoff	HAW Hamburg, Germany
Louise Yngstrom	University of Stockholm, Sweden
Moti Yung	Google, USA

Additional Reviewers

Stelios Dritsas
Carmen Fernandez
Gerardo Fernandez
Antonios Gouglidis
Christian Kahl
Ella Kolkowska
Antonis Krithinakis
Meixing Le
Andreas Leicher
Dimitra Liveri
Milica Milutinovic
Wojciech Mostowski
Konstantinos Moulinos

David Nuñez
Antonis Papadagiannakis
Thanasis Petsas
Ahmad Sabouri
Bill Tsoumas
Fabian van den Broek
Giorgos Vasiliadis
Sicco Verwer
Fatbardh Veseli
Pim Vullers
Philipp Winter
Ge Zhang
Lei Zhang

Table of Contents

Attacks and Malicious Code

Relay Attacks on Secure Element-Enabled Mobile Devices: Virtual Pickpocketing Revisited	1
<i>Michael Roland, Josef Langer, and Josef Scharinger</i>	
Would You Mind Forking This Process? A Denial of Service Attack on Android (and Some Countermeasures)	13
<i>Alessandro Armando, Alessio Merlo, Mauro Migliardi, and Luca Verderame</i>	
An Approach to Detecting Inter-Session Data Flow Induced by Object Pooling	25
<i>Bernhard J. Berger and Karsten Sohr</i>	
Embedded Eavesdropping on Java Card	37
<i>Guillaume Barbu, Christophe Giraud, and Vincent Guerin</i>	

Security Architectures

Authenticated Key Exchange (AKE) in Delay Tolerant Networks	49
<i>Sofia Anna Menesidou and Vasilios Katos</i>	
OFELIA – A Secure Mobile Attribute Aggregation Infrastructure for User-Centric Identity Management	61
<i>Alexandre B. Augusto and Manuel Eduardo Correia</i>	
Smart OpenID: A Smart Card Based OpenID Protocol	75
<i>Andreas Leicher, Andreas U. Schmidt, and Yogendra Shah</i>	
Peer to Peer Botnet Detection Based on Flow Intervals	87
<i>David Zhao, Issa Traore, Ali Ghorbani, Bassam Sayed, Sherif Saad, and Wei Lu</i>	

System Security

Towards a Universal Data Provenance Framework Using Dynamic Instrumentation	103
<i>Eleni Gessiou, Vasilis Pappas, Elias Athanasopoulos, Angelos D. Keromytis, and Sotiris Ioannidis</i>	
Improving Flask Implementation Using Hardware Assisted In-VM Isolation	115
<i>Baozeng Ding, Fufeng Yao, Yanjun Wu, and Yeping He</i>	

HyperForce: Hypervisor-enForced Execution of Security-Critical Code 126
Francesco Gadaleta, Nick Nikiforakis, Jan Tobias Mühlberg, and Wouter Joosen

RandHyp: Preventing Attacks via Xen Hypercall Interface 138
Feifei Wang, Ping Chen, Bing Mao, and Li Xie

Access Control

Role Mining under Role-Usage Cardinality Constraint 150
John C. John, Shamik Sural, Vijayalakshmi Atluri, and Jaideep S. Vaidya

HIDE_DHCP: Covert Communications through Network Configuration Messages 162
Ruben Rios, Jose A. Onieva, and Javier Lopez

Handling Stateful Firewall Anomalies 174
Frédéric Cuppens, Nora Cuppens-Boulahia, Joaquín García-Alfaro, Tarik Moataz, and Xavier Rimasson

A Framework for Threat Assessment in Access Control Systems 187
Hemanth Khambhammettu, Sofiene Boulares, Kamel Adi, and Luigi Logrippo

Database Security

Support for Write Privileges on Outsourced Data 199
Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati

Malicious Users’ Transactions: Tackling Insider Threat 211
Weihan Li, Brajendra Panda, and Qussai Yaseen

Privacy Attitudes and Properties

Privacy-Preserving Television Audience Measurement Using Smart TVs 223
George Drosatos, Aimilia Tasidou, and Pavlos S. Efrimidis

Tracking Users on the Internet with Behavioral Patterns: Evaluation of Its Practical Feasibility 235
Christian Banse, Dominik Herrmann, and Hannes Federrath

Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition	249
<i>Alexios Mylonas, Vasilis Meletiadis, Bill Tsoumas, Lilian Mitrou, and Dimitris Gritzalis</i>	

Social Networks and Social Engineering

Modeling Social Engineering Botnet Dynamics across Multiple Social Networks	261
<i>Shuhao Li, Xiaochun Yun, Zhiyu Hao, Yongzheng Zhang, Xiang Cui, and Yipeng Wang</i>	
Layered Analysis of Security Ceremonies	273
<i>Giampaolo Bella and Lizzie Coles-Kemp</i>	

Applied Cryptography, Anonymity and Trust

A Small Depth-16 Circuit for the AES S-Box	287
<i>Joan Boyar and René Peralta</i>	
Formal Verification of the mERA-Based eServices with Trusted Third Party Protocol	299
<i>Maria Christofi and Aline Gouget</i>	

Usable Security

My Authentication Album: Adaptive Images-Based Login Mechanism	315
<i>Amir Herzberg and Ronen Margulies</i>	
Balancing Security and Usability of Local Security Mechanisms for Mobile Devices	327
<i>Shuzhe Yang and Gökhan Bal</i>	
Analyzing Value Conflicts for a Work-Friendly ISS Policy Implementation	339
<i>Ella Kolkowska and Bart De Decker</i>	
When Convenience Trumps Security: Defining Objectives for Security and Usability of Systems	352
<i>Gurpreet Dhillon, Tiago Oliveira, Santa Susarapu, and Mário Caldeira</i>	

Security and Trust Models

Security-by-Contract for the OSGi Platform	364
<i>Olga Gadyatskaya, Fabio Massacci, and Anton Philippov</i>	

Cyber Weather Forecasting: Forecasting Unknown Internet Worms Using Randomness Analysis	376
<i>Hyundo Park, Sung-Oh David Jung, Heejo Lee, and Hoh Peter In</i>	
Incentive Compatible Moving Target Defense against VM-Colocation Attacks in Clouds	388
<i>Yulong Zhang, Min Li, Kun Bai, Meng Yu, and Wanyu Zang</i>	
Give Rookies a Chance: A Trust-Based Institutional Online Supplier Recommendation Framework	400
<i>Han Jiao, Jixue Liu, Jiuyong Li, and Chengfei Liu</i>	

Security Economics

A Game-Theoretic Formulation of Security Investment Decisions under Ex-ante Regulation	412
<i>Giuseppe D’Acquisto, Marta Flamini, and Maurizio Naldi</i>	
Optimizing Network Patching Policy Decisions	424
<i>Yolanta Beres and Jonathan Griffin</i>	
A Risk Assessment Method for Smartphones	443
<i>Marianthi Theoharidou, Alexios Mylonas, and Dimitris Gritzalis</i>	
Empirical Benefits of Training to Phishing Susceptibility	457
<i>Ronald Dodge, Kathryn Coronges, and Ericka Rovira</i>	

Authentication and Delegation

Multi-modal Behavioural Biometric Authentication for Mobile Devices	465
<i>Hataichanok Saevanee, Nathan L. Clarke, and Steven M. Furnell</i>	
Analysis and Modeling of False Synchronizations in 3G-WLAN Integrated Networks	475
<i>Christoforos Ntantogian, Christos Xenakis, and Ioannis Stavrakakis</i>	
Password Protected Smart Card and Memory Stick Authentication against Off-Line Dictionary Attacks	489
<i>Yongge Wang</i>	
Distributed Path Authentication for Dynamic RFID-Enabled Supply Chains	501
<i>Shaoying Cai, Yingjiu Li, and Yunlei Zhao</i>	
Enhanced Dictionary Based Rainbow Table	513
<i>Vrizlynn L.L. Thing and Hwei-Ming Ying</i>	

Short Papers

Authorization Policies for Materialized Views	525
<i>Sarah Nait-Bahloul, Emmanuel Coquery, and Mohand-Saïd Hacid</i>	
Enhancing the Security of On-line Transactions with CAPTCHA Keyboard	531
<i>Yongdong Wu and Zhigang Zhao</i>	
Fighting Pollution Attack in Peer-to-Peer Streaming Networks: A Trust Management Approach	537
<i>Xin Kang and Yongdong Wu</i>	
A Framework for Anonymizing GSM Calls over a Smartphone VoIP Network	543
<i>Ioannis Psaroudakis, Vasilios Katos, and Pavlos S. Efraimidis</i>	
A Browser-Based Distributed System for the Detection of HTTPS Stripping Attacks against Web Pages	549
<i>Marco Prandini and Marco Ramilli</i>	
Privacy-Preserving Mechanisms for Organizing Tasks in a Pervasive eHealth System	555
<i>Milica Milutinovic, Vincent Naessens, and Bart De Decker</i>	
Web Services Security Assessment: An Authentication-Focused Approach	561
<i>Yannis Soupionis and Miltiadis Kandias</i>	
Open Issues and Proposals in the IT Security Management of Commercial Ports: The S-PORT National Case	567
<i>Nineta Polemi and Theodoros Ntouskas</i>	
A Response Strategy Model for Intrusion Response Systems	573
<i>Nor Badrul Anuar, Maria Papadaki, Steven Furnell, and Nathan Clarke</i>	
Intrusion Tolerance of Stealth DoS Attacks to Web Services	579
<i>Massimo Ficco and Massimiliano Rak</i>	
Towards Use-Based Usage Control	585
<i>Christos Grompanopoulos and Ioannis Mavridis</i>	
Author Index	591